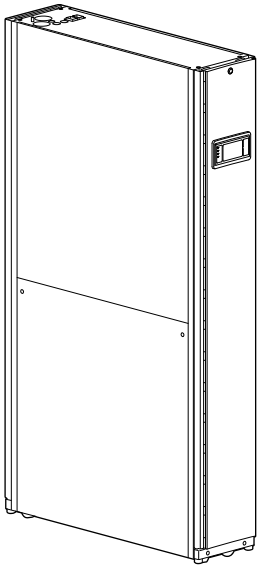
Uniflair™ Chilled-Water InRow Cooling

ACRC300 Series

Online Guide

990-2022726B-001
Release Date: 09/2025



www.schneider-electric.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this document are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owner.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.
This manual contains general information, safety instructions, and guidance. Updates may be published from time to time and are available upon request. This manual is not a substitute for the user conducting a detailed operational and site-specific development plan.
This product is for industrial use only. It should only be used for the functions for which it has been designed as set out in this manual. User must evaluate and take adequate precautions to address risks associated with use of this product in environments and/or processes not specifically addressed in this manual (e.g. heavy industry, medical, marine environments, railway, etc.).

This product should be installed, configured, used, serviced, maintained, replaced or have similar work carried out on it only by suitably qualified, trained, experienced and competent personnel who hold any necessary authorizations (e.g. licenses, permits or certifications) to perform such work. User must ensure that all work is carried out in compliance with the manufacturer’s instructions (including the product labels/ markings, technical specification manual, installation manual, and operation and maintenance manual) and with all applicable laws, regulations, standards and guidance (including standards and guidance applicable to the installation location).

All work must be carried out in a way that does not give rise to danger and using appropriate personal protective equipment (PPE).
Schneider Electric shall not be responsible for any works carried out by anyone other than Schneider Electric; or for integration or use of the product with other products (including spare parts and software) that are neither approved nor provided by Schneider Electric for such purposes; or for any non-Schneider Electric software, firmware, information or memory data contained in, stored on, or integrated with this product.

To the maximum extent permitted by applicable law, neither Schneider Electric nor any of its affiliates shall be liable for any claims, costs, losses, damages, death or injuries arising out of the improper use of this product or any failure to comply with any of the above requirements.Schneider Electric’s quality management system is ISO 9001 certified and the products are marked

Table of Contents

Introduction

Product Description

Unit Overview

The cooling units are Web-based, IPv6–ready products. They can manage supported devices using multiple open standards such as the following:

- Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)
- Secure SHell (SSH)
- Secure Copy (SCP)
- Lightweight Directory Access Protocol (LDAP) - v3.1.x and higher
- Terminal Access Controller Access-Control System Plus (TACACS+) - v3.0.x and higher
- Extensible Authentication Protocol (EAP) over LAN (EAPoL)
- Simple Network Management Protocol versions 1 .2 and 3 (SNMPv1, SNMPv2, SNMPv3)
- Building Automation and Control Networks Protocol (BACnet)
- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Telnet
- Syslog
- RADIUS
- Modbus TCP/IP

Features

- Provides data and event logs.
- Enables you to set up notifications through event logging, e-mail, Syslog and SNMP traps.
- Supports using a Dynamic Host Configuration Protocol (DHCP) or BOOTstrap Protocol (BOOTP) server to provide the network (TCP/IP) address of the unit.
- Supports using the Remote Monitoring Service (RMS).
- Provides the ability to export a user configuration (.ini) file from a configured unit to one or more unconfigured units.
- Provides a selection of security protocols for authentication and encryption.
- Communicates with Struxureware Data Center Expert or Ecostruxure™ IT gateway.
- Provides one USB host port to support firmware upgrades in addition to the retrieval of event, data log, and configuration files.

IPv4 Initial Setup

You must define three TCP/IP settings for the unit before it can operate on the network.

- The IP address of the unit
- The subnet mask of the unit
- The IP address of the default gateway (only needed if you are going off segment)

NOTE: Do not use the loopback address (127.0.0.1) as the default gateway. Doing so disables the card. You must then log on using a serial connection and reset TCP/IP settings to their defaults.

For detailed information on how to use a DHCP server to configure the TCP/IP settings for a unit, see DHCP Response Options, page 41.

IPv6 Initial Setup

IPv6 network configuration provides flexibility to accommodate your requirements. IPv6 can be used anywhere an IP address is entered on this interface. You can configure manually, automatically, or using DHCP.

See TCP/IP Settings for IPv6, page 40.

Network Management with Other Applications

These applications and utilities work with the unit:

- PowerNet® Management Information Base (MIB) with a standard MIB browser — Perform SNMP SETs and GETs and receive SNMP traps.
- Struxureware Data Center Expert or Ecostruxure™ IT gateway — Collects, organizes, and distributes critical alerts and key information, providing a unified view of complex physical infrastructure environments from anywhere on the network.
- Device IP Configuration Utility — Configure the basic settings of one or more units over the network.
- Security Wizard CLI — Assists in creating or importing Transport Layer Security (TLS) server certificates and Secure SHell (SSH) host keys, which help to protect the integrity and confidentiality of communication with the unit.

Internal Management Features

Overview

Use the Web user interface (UI) or the command line interface (CLI).

Access Priority for Logging On

You can enable more than one user to log on at the same time, where each user has equal access.

See Session Management, page 28.

Types of User Accounts

The unit has various levels of access— Super User, Administrator, Device User, Read-Only User, and Network-Only User — and these are protected by user name and password requirements.

- A Super User can use all of the menus in the UI and all of the commands in the command line interface. The Super User can also define additional user accounts, and set variables for the additional users. The default user name is `device`, and a password must be set before the user account can be enabled. You will be prompted to enter a new password after you log in.

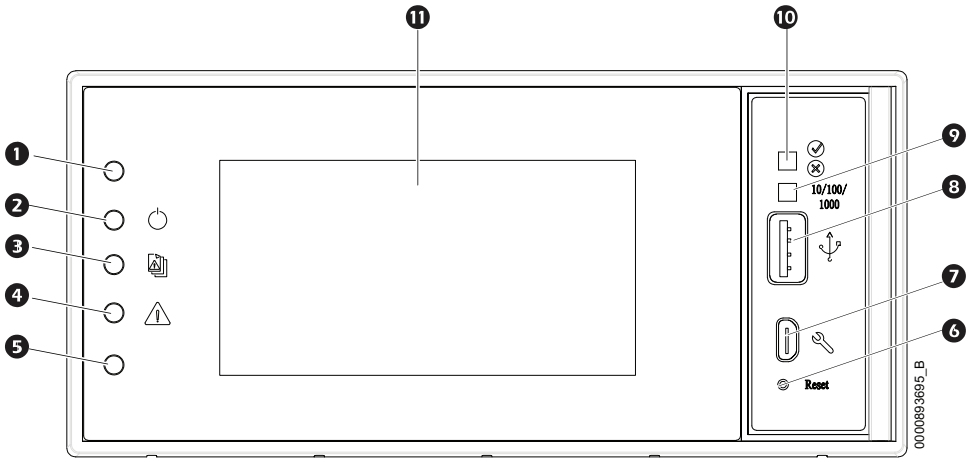
  NOTE: The Super User cannot be renamed or deleted, but it can be disabled. It is recommended that the Super User account is disabled once any additional Administrator accounts are created. Make sure that there is at least one Administrator account enabled before the Super User account is disabled.

- An Administrator can use all of the menus in the UI and all of the commands in the command line interface. In v3.0.x and higher, there is no default name and password.
- A Device User has read and write access to device-related screens. Administrative functions like **Session Management** under the **Configuration > Security** menu and **Firewall** under **Logs** are grayed out.
  - The default user name is `device`, and a password must be set before the user account can be enabled.
- A Read-Only User has the following restricted access:
  - Access through the Web UI and command line interface (CLI) only.
  - Access to the same menus as a Device User above but without the capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but disabled. (The Event and Data Logs display no button for this user to clear the log.)
  - The default user name is `readonly`, and a password must be set before the user account can be enabled.
- A Network-Only User can only log on using the Web user interface (UI) and CLI (through telnet/SSH not serial port). A Network-Only user has Read-Write access to the Network-Related menus only. There is no default name and password.

  NOTE: The Administrator, Device User, Read-Only User, and Network-Only user accounts are disabled by default, and cannot be enabled until the Super User default password (apc) is changed.

To set User Name and Password values for the top three account types, see Local Users, page 28.

Display Interface



Item	Description	Function
❶	Not used	
❷	Power LED	The cooling unit is powered when the LED is illuminated. Unit firmware is updating when LED is blinking.
❸	Check log LED	When this LED is illuminated, a new entry has been made to the event log.
❹	Alarm LED	Displays current alarm condition of unit.
❺	Not used	
❻	Display reset button	Resets the display microprocessor. This has no effect on the air conditioner controller.
❼	Micro USB	• Used as serial configuration port. Connect the display interface with a local computer to configure initial network settings or to access the command line interface (CLI). • Used as service port.
❽	USB-A port	Supports firmware upgrades.
❾	Link-RX/TX (10/100/1000) LED	Displays current network link status.
❿	Status LED	Displays current network management card status.
⓫	LCD display	4.3 in. touch-screen color display.

Alarm LED

This LED indicates active alarms on the display.

Condition	Description
Off	No alarm
Solid yellow	Warning alarm
Solid red	Critical alarm

Status LED

This LED displays current network management card status and display status.

Condition	Description
Off	One of the following situations exist: • The display is not receiving input power. • The display is not operating properly. It may need to be repaired or replaced. Please contact Schneider ElectricTrane Customer Support.
Solid green	The display has valid TCP/IP settings.
Solid orange	A hardware malfunction has been detected in the display. Please contact Schneider ElectricTrane Customer Support.
Flashing green	The display does not have valid TCP/IP settings.
Flashing orange	The display is making BOOTP requests.
Alternately flashing green and orange	If the LED is flashing slowly, the display is making DHCP requests. If the LED is flashing rapidly, the display is starting up.

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

This LED indicates the network status of the display.

Condition	Description
Off	One or more of the following situations are occurring: • The display is not receiving input power. • The cable or device that connects the cooling unit to the network is disconnected or not functioning properly. • The display itself is not operating properly. It may need to be repaired or replaced. Contact Schneider ElectricTrane Customer Support.
Solid green	The display is connected to a network operating at 10 megabits per second (Mbps).
Solid orange	The display is connected to a network operating at 100/1000 Mbps.
Flashing green	The display is receiving or transmitting at 10 Mbps.
Flashing orange	The display is receiving data packets at 100/1000 Mbps.

How to Recover from a Lost Password

You can use a local computer that connects to the display through the serial port to access the command line interface.

1. Select a serial port on the local computer, and disable any service that uses that port.
2. Connect the provided serial cable to the selected port on the computer and to the configuration port on the display.
3. Run a terminal program (such as HyperTerminal®) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press **Enter**, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
   - The serial port is not in use by another application.
   - The terminal settings are correct as specified in step 3.
   - The correct cable is being used as specified in step 2.
5. Press the **Reset** button. The **Status** LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.
6. Press **Enter**, repeatedly if necessary, to display the **User Name** prompt again, then use the default, `apc`, for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is re-displayed, you must repeat step 5 and log on again.)
7. At the command line interface, use the following commands to change the **Password** setting, which is `apc` at this stage:

   `user -n <user name> -pw <user password>`

   For example, to change the Super User password to XYZ, type:

   `user -n apc -pw XYZ`
8. Type `quit` or `exit` to log off, reconnect any serial cable you disconnected from the computer, and restart any service you disabled on the unit.

Watchdog Features

Overview

To detect internal problems and recover from unanticipated input, the display uses internal, system-wide watchdog mechanisms. When it restarts to recover from an internal problem, a System: Network Interface Restarted event is recorded in the event log.

Network Interface Watchdog Mechanism

The display implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the display unit does not receive any network traffic for 9.5 minutes (either direct traffic, such as SNMP, or broadcast traffic, such as an Address Resolution Protocol [ARP] request), it assumes that there is a problem with its network interface and restarts.

Resetting the Network Timer

To ensure that the display does not restart if the network is quiet for 9.5 minutes, the display unit attempts to contact the default gateway every 4.5 minutes. If the

gateway is present, it responds to the display, and that response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network and is on the same subnet. The network traffic of that computer will restart the 9.5-minute timer frequently enough to prevent the display from restarting.

Automatic Logout

By default, users will be automatically logged out of the NMC Web and CLI interfaces after 3 minutes of inactivity. The default logout time for each user can be adjusted through the web interface:
Configuration > Security > Local Users > Management.

- Click the hyperlink of the user name for the account you want to change.
- Under Session timeout, modify the number of minutes.

Automatic Logout	Duration (min)
Default	3
Minimum	1
Maximum	60 (1 hr)

Web User Interface

Introduction

Overview

The Web User Interface (UI) provides options to manage the unit and to view the status of the unit.

See Web Access, page 44 for information on how to select, enable, and disable the protocols that control access to the UI and to define the Web-server ports for the protocols.

Supported Web Browsers

The latest version of the following web browsers are supported to access the unit through its UI.

- Microsoft® Edge
- Firefox®
- Google Chrome®

Other commonly available browsers might work but have not been fully tested.

The unit cannot work with a proxy server. Before you can use a browser to access the UI of the unit, you must do one of the following:

- Configure the browser to disable the use of a proxy server for the unit.
- Configure the proxy server so that it does not proxy the specific IP address of the unit.

How to Log On

Overview

You can use the DNS name or the System IP address of the unit for the URL address of the UI. Use your case-sensitive user name and password to log on. In v3.0.x and higher, the password is not shown as it is entered, the default user name can be used and differs by account type:

- **apc** for Administrator or for Super User
- **device** for a Device User
- **readonly** for a Read-Only User

The default password is **apc** for these three account types. There is no default for a Network-only account type.

NOTE: Before logging to the device/read-only account, log in as an administrator and go to the User Management Configuration page, select the device and enable the device/read-only account.
Path: Configuration > Security > Local Users > Management

See also Types of User Accounts, page 11.

You can set your UI language as you log on by choosing a language from the **Language** drop-down box.

When HTTPS is enabled, the NMC generates its own certificate. This certificate negotiates encryption methods with your browser. Refer to the Security Handbook for more details.

First Log In

When you log in to the NMC for the first time, you will be prompted to change the default Super User account password (`apc`). You will then be directed to the Configuration Summary Overview screen. This screen is an overview of all system protocols, and their current values (e.g. enabled/disabled). You can access this screen at any time afterwards by following the path: **Configuration > Network > Summary**.

URL Address Format

Type the DNS name or IP address of the unit in the Web browser URL address field and press Enter.

Common Browser Error Messages at Log-On		
Error Message	**Browser**	**Cause of the Error**
”DNS error”	edge	Web access is disabled, or the URL was not correct.
”Unable to connect.”	Firefox, Chrome	

URL Format Examples	
Example and Access Mode	**URI Format**
DNS name of `Web1`	
HTTP	`http://Web1`
HTTPS	`https://Web1`
System IP address of `139.225.6.133` and a default Web server port (80)	
HTTP	`http://139.225.6.133`
HTTPS	`https://139.225.6.133`
System IP address of `139.225.6.133` and a non-default Web server port (5000)	
HTTP	`http://139.225.6.133:5000`
HTTPS	`https://139.225.6.133:5000`
System IPv6 address of `2001:db8:1::2c0:b7ff:fe00:1100` and a non-default Web server port (5000)	
HTTP	`http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000`

Home Screen

Overview

Home: On the **Home** screen of the Web user interface, you can view the device name and location, temperature readings, active alarms, and the most recent events recorded in the **Event Log**. To view the entire **Event Log**, click **More Events** in the bottom-right of the **Recent Device Events** list.

One or more icons and accompanying text indicate the current operating status of the unit.

Symbol	Description
	**No Alarm:** No alarms are present.
	**Informational:** Provides details on any alarms that are not a warning or critical.
	**Warning:** An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
	**Critical:** A critical alarm exists that requires immediate action.

In the upper-right corner of every screen, the same icons report the unit status. If any Critical or Warning alarms exist, the number of active alarms also displays.

Icons and links: To make any screen the “home” screen (i.e., the screen that displays first when you log on), go to that screen, and click  in the top-right corner.

Click  to revert to displaying the **Home** screen when you log on.

At the lower-left on each screen of the interface, there are three configurable links to useful Web sites. By default, the links access the URLs for these Web pages:

- Link 1: Knowledge Base
- Link 2: Schneider Electric Product Center
- Link 3: Schneider Electric Downloads

To re-configure the links, see Configure the Links Screen, page 59.

Monitoring the Status

Unit Status

Path: Main > Status > Unit

View information specific to this unit.

The unit and network can be configured using the **Configuration** menu options. See Configuring Your Settings, page 25.

Overview

- **Operating Mode:** The unit is in one of the following modes:
  - **On:** The unit is cooling.
  - **Standby:** The unit is receiving power but not enabled for cooling.
  - **Idle:** The unit is not operating in normal mode due to active alarms.
- **Rack Inlet Temperature 1–4:** The average air temperature entering the racks.
- **Unit Maximum Rack Inlet Temperature:**The recorded maximum temperature at the rack inlet temperature sensors connected to the unit.
- **Supply Air Temperature:** The temperature of the air leaving the unit.
- **Return Air Temperature:** The temperature of the air entering the unit.
- **Dew Point Temperature:** The dew point of the environment (ACRC301H only).
- **Airflow:** The velocity at which air flows into or out of the unit.
- **Fan Speed:** The speed of the fans that regulate the airflow through the cooling unit.
- **Cool Output:** The actual cooling output of the unit.
- **Cool Demand:** The amount of cooling that the heat load currently requires.
- **Unit Energy:** The electrical energy consumed by the unit since the last Reset Unit Energy command (**Path: Main > Configuration > Unit > Configuration**).
- **Unit Power:** The average revolutions per minute (RPM) of all condenser fans, given as percentage of the maximum fan speed.
- **Unit Maximum Rack Inlet Temperature:** The unit maximum air temperature entering the racks.

Detailed Status

- **Chilled Water Valve Position:**The position (percent open) of the valve that controls how much chilled water enters the cooling unit.
- **Chilled Water Flow:** The amount of chilled water flows through the cooling unit.
- **Entering Chilled Water Temperature:** The temperature of the chilled water as it enters the cooling unit.
- **Leaving Chilled Water Temperature:**The temperature of the chilled water as it leaves the cooling unit.
- **Coil Chilled Water Temperature:** The temperature of chilled water entering the coil (ACRC301H only).
- **Standby Input State:** The current state of the input. If the input is in an abnormal state, an alarm will occur and the unit will stop cooling.

- **Output 1-4 State:** The current state of the four output relays.
- **Filter Differential Pressure:** The differential pressure of the air filter.
- **Leak Detector 1–4:** The state of the leak detector rope sensor.
- **Active Power Source:** The power source being used by the unit. The unit supports a redundant power input.

Unit Run Hours

The cooling unit records the number of hours each of its components has been in operation.

- **Unit**
- **Condensate Pump (ACRC301S only)**
- **Circulation Pump (optional for ACRC301H only)**
- **Fan Power Supply 1-2**
- **Air Filter**

  NOTE: When the air filter is replaced, use the **Air Filter Serviced** button to reset the maintenance alarm.
- **Fan 1-8 (Fan 1 is the bottom fan; Fan 8 is the top fan)**

Group Status

View information related to the cooling group.

You can configure your unit and network using the **Configuration > Group** menu options. See Group Configuration, page 26.

Overview

This screen displays the status of the group of cooling units connected by A-Link.

- **Cool Output:** The combined output of the cooling group.
- **Cool Demand:** The cooling output required to meet the current heat load of the conditioned space.
- **Cool Setpoint:** The temperature set to maintain the room environment.
- **Airflow:** The combined airflow output of the units in the cooling group.
- **Maximum Rack Inlet Temperature:** The highest return temperature reported by any cooling unit in the cooling group.
- **Minimum Rack Inlet Temperature:** The lowest return temperature reported by any cooling unit in the cooling group.

Network Status

Path: Main > Status > Network

The **Network** screen displays information about your network.

Current IPv4 Settings

- **System IP:** The IP address of the cooling unit.
- **Subnet Mask:** The subnet mask for the sub-network.
- **Default Gateway:** The default gateway address used by the network.
- **MAC Address:** The MAC address of the cooling unit.
- **Mode:** How the IPv4 settings are assigned: **Manual**, **DHCP**, or **BOOTP**.
- **DHCP Server:** The IP address of the DHCP server. This is only displayed if **Mode** is DHCP.
- **Lease Acquired:** The date/time that the IP address was accepted from the DHCP server.
- **Lease Expires:** The date/time that the IP address accepted from the DHCP server expires and will need to be renewed.

Current IPv6 Settings

- **Type:** How the IPv6 settings are assigned.
- **IP Address:** The IP address of the unit.
- **Prefix Length:** The range of addresses for the sub-network.

Domain Name System Status

- **Active Primary DNS Server:** The IP address of the primary DNS server.
- **Active Secondary DNS Server:** The IP address of the secondary DNS server.
- **Active Host Name:** The host name of the active DNS server.
- **Active Domain Name (IPv4/IPv6):** The IPv4/IPv6 domain name that is currently in use.
- **Active Domain Name (IPv6):** The IPv6 domain name that is currently in use.

Port Speed

- **Current Speed:** The current speed assigned to the Ethernet port.

Security and Network Control

The **Control** menu options enable you to take immediate actions affecting active user management and the security of your network.

Manage User Sessions

Path: Main > Control > Security > Session Management

The screens gives details about users who are logged on, the interface they are using (e.g. the Web user interface, the CLI), their IP address, and how long they have been logged on. If you have sufficient rights, click on the name to see what means of authentication were used to validate the user. You can then also use the **Terminate Session** button to log off a user.

Network on Control Menu

Web CLI

Path: Main > Control > Network > Web CLI

Provides a web-based command line interface (CLI) for the currently logged in user.

Reset/Reboot

Path: Main > Control > Network > Reset/Reboot

This menu gives you the option to reset and reboot various components of the network interface. Users have the option to **Reboot Management Interface**, **Reset All** (option to exclude TCP/IP), or **Reset Only** (**TCP/IP** or **Event Configuration**).

- **Reboot Management Interface:** Restarts the network interface of the device without turning off and restarting the device itself.
- **Reset All:**
  - If **Exclude TCP/IP** is not selected, all configured values and settings are reset to their default values, including the setting that determines how this device must obtain its TCP/IP configuration values and the EAPoL configuration. The default for TCP/IP configuration setting is DHCP and that EAPoL access is disabled.
  - If **Exclude TCP/IP** is selected, all configured values and settings except the setting that determines how this device must obtain its TCP/IP and the EAPoL configuration values are reset to their default values.
- **Reset Only:**
  - **TCP/IP:** Resets only the setting that determines how this device must obtain its TCP/IP configuration values including the EAPoL configuration which is reset to disabled. The default for TCP/IP configuration setting is DHCP and that for EAPoL access is disabled.
  - **Event Configuration:** Resets events to their default configuration. Any specially configured event or group will also revert to the default value.

Configuring Your Settings

With the **Configuration** menu options, you can set fundamental operational values for your unit.

Unit Configuration

NOTE: Displayed settings will vary based on unit configuration.

Thresholds

Path: Main > Configuration > Unit > Thresholds

This menu displays various unit thresholds, their sensor value, and the editable threshold setting. After making changes to a given threshold temperature, click **Apply** to confirm changes, or **Cancel** to revert to previous settings. An example of this would be if the water temperature exceeds the temperature defined by the corresponding **Temperature Threshold**, an alarm will occur..

- **Rack Inlet High Temperature Threshold:** An alarm condition exists when the temperature of the air entering the rack at the rack inlet sensor exceeds the threshold.
- **Supply Air High Temperature Threshold:** An alarm condition exists when the temperature of the air output from the cooling unit exceeds the threshold.
- **Return Air High Temperature Threshold:** An alarm condition exists when the temperature of the air entering the cooling unit at the temperature sensor exceeds the threshold.
- **Entering Chilled Water High Temperature Threshold:**The chilled water entering the cooling unit.

Unit Configuration

Path: Main > Configuration > Unit Configuration

This menu provides a variety of configurable standard unit options for the user. After making any changes, click **Apply** to confirm changes, or **Cancel** to revert to previous settings.

- **Startup Delay:** The delay begins when the cooling unit is started and initialized. The cooling unit cannot begin operation until this delay expires. Use the start-up delay to restart equipment sequentially in your room after a scheduled downtime.
- **Idle On Leak Detect:** When set to **Yes**, the cooling unit will enter idle mode if a **Water Detection Error** activates. Set to **No** to disable the cooling unit from entering idle mode if a leak is detected.
- **Idle on Cool Fail** : When set to **Yes**, the cooling unit will enter idle mode if the cooling unit is unable to supply conditioned air. Set to **No** to disable the cooling unit from entering idle mode if a cooling failure is detected.
- **Bypass Valve Position** : Reflects the position of the manual bypass valve. This setting must match the physical setting of the valve. When the bypass valve is closed, the maximum chilled water flow is limited via the **Maximum Chilled Water Flow** setting.
- **Air Filter** : The number of hours the air filter has been in operation.
- **Air Filter Serviced** : Select this check box to reset an **Air Filter Run Hours Violation** or air filter status after the physical air filter is cleaned or replaced.
- **Air Filter Service Alarm Enable** : **Enable** or **Disable** the air filter service alarm.

- **Air Filter Service Interval** : Enter the number of weeks between air filter service alarms.
- **Air Filter Type** : The type of air filter installed in the cooling unit: **Standard** or **Pleated**.
- **Maximum Chilled Water Flow** : Restricts the maximum chilled water flow rate of the unit. This setting is only used when the bypass valve is closed. The input range is 0-100 gallons per minute (0-379 liters per minute). Only qualified service personnel can make changes to this setting.
- **Chilled Water Valve Control** : The setting used to determine chilled water flow. When Automatic is selected, the unit operates based on measured demand. Only qualified service personnel can make changes to this setting.
- **Power Source** : Indicates the number of power sources connected to the cooling unit. Select Single when using one power connection. Select **Dual** when using two power connections.
- **Number of Rack Inlet Temp Sensors in Unit** : The number of expected rack inlet sensors for the unit. The maximum number of rack inlet temperature sensors is four.
- **Number of Leak Detectors in Unit** : The number of expected leak detectors in the unit. The maximum number of leak detectors is four.
- **Unit Service Alarm Enable:Enable** or **Disable** the unit service alarm. Only qualified service personnel can make changes to this setting.
- **Unit Service Alarm Interval:** Enter the number of weeks between unit service alarms. Only qualified service personnel can make changes to this setting.
- **Unit Energy:** The electrical energy consumed by the unit since the last time the **Unit Energy** has been reset or the cooling unit has been powered on.
- **Reset Unit Energy:** Select this check box to reset the **Unit Energy**.
- **Alarm on Standby:** When set to**Yes**, `Standby Due to User Action` alarm is triggered if the unit is in standby mode.

Input Contacts Configuration

Path: Main > Configuration > Unit > Input Contacts

Input Configuration displays the **Standby Input State** and lets you select the standby input normal state, **Open** or **Closed**. The unit will stop operation if the standby input is not in the normal state.

Output Relays

Path: Main > Configuration > Unit > Output Relays

Output Configuration displays the name and state (**Normal** or **Abnormal**) of each relay.

Under **Current Settings**, use the check boxes under each output name to specify whether the output will change that relay to the abnormal state when the selected alarm is active. More than one output can be selected for a specified alarm. No more than 20 alarms per output can be selected.

Group Configuration

Path: Main > Configuration > Group

The Group Configuration screen displays options pertaining to the cooling group.

Setpoints

A setpoint is the target value that a cooling group will maintain in the environment. The default setpoints are appropriate for most cooling applications.

- **Cool Setpoint**. Set the temperature that the cooling group should maintain. The setpoint must be within 18.0–35.0°C (64.4–95.0°F).

  NOTE: This is the temperature maintained at the rack inlets.

- **Supply Air Setpoint**. The setpoint must be within 15.0–30.2°C (59.0–86.4°F). The Supply Air Setpoint will be the required temperature of the air expelled into the surrounding environment.

  NOTE: The Supply Air Setpoint is defined by the field service representative when the cooling group is commissioned.

- **Delta-T Setpoint**. When the group is programmed for HACS or RACS mode and an AFC is not being used, this property specifies the desired temperature difference across the equipment from the following options.
  - 10°F/5.6°C
  - 15°F/8.3°C
  - 20°F/11.1°C
  - 25°F/13.9°C
  - 30°F/16.7°C
  - 35°F/19.4°C
  - 40°F/22.2°C

Group Configuration

- **Number of Units in Group:** The number of units indicates the number of cooling units in this cooling group. Up to twelve cooling units can be joined together to work as a single cooling group.
- **Configuration Type:** The airflow control strategy for the cooling units of this cooling group. Only qualified service personnel can make changes to this setting.
  - **In-Row:** Air flow is horizontal to allow in-row operation of the cooling. The loads share a common open cold aisle.
  - **HACS (Hot Aisle Containment System):** Air flow in the room is controlled by enclosing the hot air aisle. The loads share an enclosed common hot aisle. This is not a sealed system.
  - **RACS (Rack Air Containment System):** Air flow in the enclosure is controlled by a ducting system fitted to the enclosure. This is not a sealed system.
  - **CACS (Cold Aisle Containment System):** Air flow in the room is controlled by enclosing the cold air aisle. The loads share an enclosed common cold aisle. This is not a sealed system.
- **Percent Glycol:** This specifies the percentage of glycol by volume in the chilled water. This setting affects how cooling output is reported. Only qualified service personnel can make changes to this setting.
- **Maximum Fan Speed:** Defines the maximum speed at which the fans in the unit operate when in Auto mode.

  NOTE: Reducing the fan speed will affect the cooling capacity of the unit.

- **Number of Active Flow Controllers:** Sets number of AFC units in the group (0 to 5).
- **Airflow control:** When Automatic is selected, the cooling unit operates based on measured demand. When set to **60%, 70%, 80%, 90%, 100%**, the fans will operate at the selected output.

- **Cool Gain ‘P’:** The proportional multiplier (gain) for this mode or actuator. The proportional multiplier adjusts for the difference (error) between the measured temperature and the setpoint. The proportional multiplier is expressed in percent of output per unit error. Only qualified service personnel can make changes to this setting.
- **Cool Derivative ‘D’:**. The derivative multiplier (derivative) for this mode or actuator. The derivative multiplier adjusts the output for rapid changes in the error, correcting for the rate of change of the error over time. It is expressed in percent of output for each unit of error per minute (error divided by minutes). Only qualified service personnel can make changes to this setting.
- **Cool Reset Rate ‘I’:** The integral multiplier (reset rate) for this mode or actuator. The integral multiplier adjusts for error measurement and for the amount of time that the error has existed. The integral multiplier adds to or subtracts from the output in small increments to correct for the offset error caused by the proportional contribution. It is expressed in percent of output for each minute and unit of error (error multiplied by minutes). Only qualified service personnel can make changes to this setting.

Security Menu

Session Management

Path: Main > Configuration > Security > Session Management

Enable **Allow Concurrent Logins** Two or more users can log on at the same time. Each user has equal access and each interface (HTTP, FTP, telnet console, serial console (CLI), etc.) counts as a logged-in user. Allow Concurrent Logins allows a maximum of eight users logged into the web interface, five users logged into the CLI and one user logged into the serial console at the same time.

Remote Authentication Override: The unit supports remote authentication dial-in user service (RADIUS) storage of passwords on a server. However, if you enable this override, the unit will allow a user with **Serial Remote Authentication Override** enabled to log on using the password for local authentication.

See Local Users, page 28 and Remote Users Authentication, page 30.

NOTE: Remote Authentication Override only works for users logged-in through the LCD display or through the serial cable.

Ping Response

Path: Main > Configuration > Security > Ping Response

Enable the **IPv4 Ping Response** check box to allow the cooling unit to respond to network pings. This does not apply to IPv6.

Local Users

Use these menu options to view, and to set up access and individual preferences (like displayed date format), for the unit display interface. This applies to users as defined by their logon name.

Management

Path: Main > Configuration > Security > Local Users > Management

From this menu, an administrator or super user can view the users that are allowed access to the UI. Click on the user name to view details and to edit or delete a user.

Click **Add User** to add a user. On the resulting **User Configuration** screen, you can add a user and withhold access by clearing the **Access** check box. The maximum length for both the name and password is 64 characters, with less for multi-byte characters. You have to enter a password. A PIN of four to eight digits may also be designated.

To change an administrator/super user setting, you must supply the current password as a security measure.

Default Settings

Path: Main > Configuration > Security > Local Users > Management > Default Settings

Default User Settings

- **User Type**: There are four levels of access (Administrator, Device User, Read-Only User, and Network-Only User).
  - **An Administrator** can use all the menus in the Web interface and control console. The default user name and password are both **apc**.
  - **A Device User** can access only the following:
    - In the Web interface, the menus on the **Group** and **Unit** tabs and the event and data logs, accessible under the **Events** and **Data** headings on the left navigation menu of the **Logs** tab.
    - In the control console, the equivalent features and options. The default user name is device, and the default password is **apc**.
  - **A Read-Only User** has the following restricted access:
    - Access through the Web interface only. You must use the Web interface to configure values for the Read-Only User.
    - Access to the same tabs and menus as a Device User, but without the capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but disabled, and the event and data logs display no button to clear the log.

      The default user name is **readonly**, and the default password is **apc**.
  - **A Network-Only User** has the following restricted access:
    - Access through the Web interface only (UI) and CLI (telnet not serial). A network-only user has read-write access to the network-related menus only. There is no default name and password.
- **Touch Screen**: Use to configure whether or not this account can log in to the touch screen even when the NMC authentication is set to RADIUS.
- **User Description**: This is a general description of the user.
- **Session Timeout**: Use to configure the length of time that the various UIs wait before logging-out this user (three minutes by default). If you change this value, the user must log-off for the change to take effect.
- **Bad Login Attempts**: When a user attempts to log in but enters incorrect credentials, the system will record it as a bad login attempt.

User Preferences

Select options related to how users view information.

- **Event Log Color Coding:** Select the check box to enable color-coding of alarm text recorded in the event log based on severity. (System-event entries and configuration-change entries do not change color because they are considered informational events.)
- **Export Log Format:** Exported log files can be formatted using CSV (comma-separated values) or tab delimited.

See Event Log, page 63 for information on exporting logs.

- **Temperature Scale:** Select the temperature scale for measurements in this UI. **US Customary** corresponds to Fahrenheit, and **Metric** corresponds to Celsius.
- **Date Format:** Select the date form for the UI.
- **Language:** Select the default language for the UI. This can be set when you log on also. You can also specify different languages for e-mail recipients and SNMP trap receivers.

See E-Mail Notification Configuration, page 55 and SNMP Trap Receiver Configuration, page 56.

Password Requirements

- **Strong Passwords**: Strong passwords are passwords that are difficult to guess or crack, making them more secure than weak passwords.
- **Password Policy**: It is a security measure that requires users to change their passwords within a specified time.

Remote Users Authentication

Path: Main > Configuration > Security > Remote Users > Authentication

Authentication

Specify how you want users to be authenticated at logon.

For more information about local authentication (not using the centralized authentication of a RADIUS server), see Security Handbook.

The following authentication and authorization functions of LDAP (Lightweight Directory Access Protocolv3.1. x and higher), RADIUS (Remote Authentication Dial-In User Service), and TACACS+ (Terminal Access Controller Access Control System - v3.0.x and higher) are supported:

- When a user accesses the unit or other network-enabled device that has RADIUS or TACACS+ enabled, an authentication request is sent to the server to determine the user’s permission level.
- LDAP, RADIUS, and TACACS+ user names are limited to 64 characters with the NMC.

See the options below for authentication method:

Setting	Description
Local User Authentication	Specify if and when the local user database is checked: **First**: The local user database is always checked first. If the username is found, then the password is checked and the login either succeeds or fails. If the username is not found, then remote authentication, if enabled, is used. **Last**: The local user database is checked after attempting remote authentication if there is an error contacting the remote authentication server. When remote authentication is off, this behaves the same as First. **Off**: The local user database is never checked. **NOTE:** Setting this to **Off** is not recommended as it can result in being permanently locked out of the NMC if the remote authentication server goes down or is misconfigured on the NMC. If **Off** is used, it is strongly recommended to enable the Remote Authentication Override setting and to set the Serial Remote Authentication Override option for the super user or an administrator. **NOTE:** If both Local and Remote User Authentication settings are set to **Off**, then Local User Authentication will automatically be set to **First**.
Remote User Authentication	Specify which, if any, remote authentication protocol is used: **Off**: Do not use remote user authentication and always perform local user authentication. **RADIUS**: Remote user authentication will use RADIUS. Note: The message "No configured RADIUS servers have been added." indicates that you must add a properly configured RADIUS server so that RADIUS authentication can operate. **TACACS+**: Remote user authentication will use TACACS+. Note: The message "No configured TACACS+ servers have been added." indicates that you must add a properly configured TACACS+ server so that TACACS+ authentication can operate. **LDAP**: Remote user authentication will use LDAP. **NOTE:** The message "No configured LDAP servers have been added." indicates that you must properly configure LDAP so that LDAP authentication can operate.

IMPORTANT: If **Local Authentication** is set to **Off**, and the authentication servers are unavailable, improperly identified, or improperly configured, remote access is unavailable to all users. To regain access, you must use a serial connection to the command line interface and change the **access** setting to **local, radiusLocal** or **tacacs+Local**
For example, the command to change the access setting to **local** would be:
`userauth -a local`

For RADIUS server, see RADIUS screen below and Configuring the RADIUS Server. For TACACS+ server, see TACACS+ screen (v3.0.x and higher) below and Configuring the TACACS+ Server. For LDAP server, see LDAP screen (v3.1.x and higher) below and Configuring the LDAP Server.

LDAP screen (v3.1.x and higher)

Path: Main > Configuration > Security > Remote Users > LDAP
You can set up the device to use an LDAP server to authenticate remote users. Two common examples of this are Microsoft Active Directory and OpenLDAP. Authentication is always performed using a simple bind request over a TLS connection. Ensure that the LDAP server's CA certificate is installed in order for the TLS connection to the LDAP server to complete.

LDAP Setting	Description
Search User URI	An LDAP URI representing the location of a user object to initially bind to. This user object must have permission to search the LDAP database for users. During a user login attempt, the LDAP server in this URI is connected to and a bind to the DN is performed with the password provided in "Search User Password". If this bind is successful, the user attempting to login is then searched for. This LDAP URI must include a scheme of either "ldap" or "ldaps". When "ldaps" is used, then the TLS connection is implicit and the TCP connection defaults to using port 636. When "ldap" is used, then the TLS connection is initiated by sending a StartTLS request and the TCP connection defaults to using port 389. Use of "ldaps" is nonstandard and discouraged. This LDAP URI may include the address of the LDAP server and optionally the port number. The DN of the search user object follows. If the search user DN ends with DC components, then a DNS lookup of the SRV record for the LDAP service at this domain is performed. If the SRV record is found, then it is used instead of the host specified in the URI. If the SRV record is not found, then the host specified in the URI is used. The host component of the URI may be omitted if the SRV record for LDAP is known to exist. If the DN is omitted, then the host component must be present and an anonymous bind is performed. Examples: • **"ldap://ldap.domain.com/CN=searchuser,OU=users,DC=domain,DC=com** If DNS is available, a DNS lookup of the SRV record for the LDAP service at domain.com is performed. If it is found, then it is connected to. If it is not found, then "ldap.domain.com" at port 389 is connected to. TLS is then established after sending a StartTLS request, and then a bind to the object "CN=searchuser, OU=users,DC=domain,DC=com" with the password specified in Search User Password is performed. From here a search for the user logging in is performed. • **“ldap:///CN=searchuser,OU=users,DC=domain,DC=com** If DNS is available, a DNS lookup of the SRV record for the LDAP service at domain.com is performed. If it is found, then it is connected to. If it is not found, then no connection is made because the host component of the URI is omitted and LDAP authentication cannot proceed. If the connection is successful, then StartTLS, bind, and search are performed as described above. • **"ldaps://ldap.domain.com** "ldap.domain.com" at port 636 is connected to and a TLS handshake is immediately performed without sending a StartTLS request. If this succeeds, then an anonymous bind is performed. From here a search for the user logging in is performed. • **"ldap://ldap.domain.com:42/CN=searchuser,OU=users,DC=domain,DC=com** • This is the same as the first example except that if the SRV record is not found then "ldap.domain.com" at port 42 is connected to.
Search User Password	The password to use in the initial bind request to the search user as described above. If left blank, then either an anonymous or unauthenticated bind is performed depending on whether or not a search user DN is provided.
Reply Timeout	The timeout in seconds to use when connecting to and communicating with the LDAP server. The initial TCP connection must complete within this amount of time. If it does, then each LDAP response from the server must be received within this amount of time following each LDAP request. Because a single LDAP authentication can consist of multiple requests (and even to multiple servers if referrals are chased) the overall authentication time may end up being much longer than the timeout value specified here.
Users Base DN	This is the DN of the base object entry under which all users who login must exist.
Groups Base DN	This is the DN of the base object entry under which the user groups specified in the following settings must exist.
Admins Group Name	This is the common name (CN) of the LDAP group to which NMC Administrators are members of. If the user logging in is a member of this group, then the user is granted Administrator access.
Device Users Group Name	This is the common name (CN) of the LDAP group to which NMC Device Users are members of. If the user logging in is a member of this group, then the user is granted Device User access.
Network Users Group Name	This is the common name (CN) of the LDAP group to which NMC Network Users are members of. If the user logging in is a member of this group, then the user is granted Network User access.
Read Only Users Group Name	This is the common name (CN) of the LDAP group to which NMC Read Only Users are members of. If the user logging in is a member of this group, then the user is granted Read Only User access.
Active Directory Schema	If this is enabled, then LDAP directories containing users of the "User" class and groups of the "Group" class following the standard Active Directory schema will be supported.

LDAP Setting	Description
RFC2307 POSIX Schema	If this is enabled, then LDAP directories containing users of the "posixAccount" class and groups of the "posixGroup" class following the schema defined in RFC 2307 will be supported.
RFC4519 User Schema	If this is enabled, then LDAP directories containing users of the "uidObject" class and groups of either the "groupOfNames" class or the "groupOfUniqueNames" class following the schema defined in RFC 4519 will be supported.
RFC2798 inetOrgPer-son	If this is enabled, then LDAP directories containing users of the "inetOrgPerson" class as defined in RFC 2798 will be supported.
Custom User Class	If this is enabled, then LDAP directories containing users of classes that do not conform to any of the supported classes above can be supported. When this is enabled, the settings **Custom User Class Name** and **Custom User Username Attr** must be provided, and **Custom User Group Number Attr** may optionally be provided.
Custom Group Class	If this is enabled, then LDAP directories containing groups of classes that do not conform to any of the supported classes above can be supported. When this is enabled, the settings **Custom Group Class Name** and **Custom Group Member Attr** must be provided, and **Custom Group Number Attr** may optionally be provided. **Custom Group Member Type** must also be set correctly.
Custom User Class Name	This is the name of the object class that user entries belong to. It is only used when **Custom User Class** is enabled.
Custom User Username Attr	This is the name of the attribute that contains a user's username for the object class specified by **Custom User Class Name**. It is only used when Custom User Class is enabled.
Custom User Group Number Attr	This is the name of the attribute that contains the group number for a user's primary group for the object class specified by Custom User Class Name. This is optional, and only used when **Custom User Class** is enabled. It is used the same way as the "gidNumber" attribute in the "posixAccount" class.
Custom Group Class Name	This is the name of the object class that group entries belong to. It is only used when Custom Group Class is enabled.
Custom Group Group Member Attr	This is the name of the attribute that contains the members of the group for the object class specified by **Custom Group Class Name**. It is only used when **Custom Group Class** is enabled. When **Custom Group Member Type** is set to "DN", then the values in this attribute are DNs. When it is set to "User Name", then the values in this attribute are user names.
Custom Group Number Attr	This is the name of the attribute that contains the group number of the group for the object class specified by **Custom Group Class Name**. This is optional, and only used when **Custom Group Class** is enabled. It is used the same way as the "gidNumber" attribute in the "posixGroup" class.
Custom Group Member Type	This specifies how members of the group for the object class specified by **Custom Group Class Name** are specified. It can be set to either "DN" or "User Name".
Test Settings	Enter the username and password of any account on the server to test the newly configured settings before applying them. If the user successfully authenticates and is a member of at least one of the specified groups, then the settings are applied. Otherwise, they are not applied.
Skip Test and Apply	Applies the settings without first performing a test authentication.

See also Remote Users authentication above.

Configuring the LDAP Server

Configuration of an OpenLDAP, Active Directory, or other LDAP server is beyond the scope of this document. As mentioned in the Settings descriptions above, the most common schemas are supported by default, including Active Directory users and groups, the POSIX schema defined in RFC2307, the User Schema defined in RFC4519, and the inetOrgPerson user class defined in RFC2798. If configuring a new server, it is recommended that one of these schemas is chosen. Ensure that

groups are created for each NMC user type that you wish to support, and that users are added to them accordingly.

RADIUS Screen

Path: Main > Configuration > Security > Remote Users > RADIUS

You can use a RADIUS server to authenticate remote users. Use this option to do the following actions:

RADIUS Setting	Description
RADIUS Server	The server name or IP address of the primary or secondary RADIUS server.
Port	The port number of the primary or secondary RADIUS server. **NOTE:** RADIUS servers use port 1812 by default to authenticate users. The NMC supports ports 1 to 65535.
Secret	The shared secret between the RADIUS server and the NMC.
Require Message-Authenticator	Enabling this setting (disabled by default) will require the NMC to receive a valid Message-Authenticator attribute in the response from the RADIUS server.
Reply Timeout	The time in seconds that the NMC waits for a response from the RADIUS server.
Test Settings	Enter the Administrator user name and password in order to test the RADIUS server path that you have configured.
Skip Test and Apply	Do not test the RADIUS server path.

See also Remote Users authentication above and Configuring the RADIUS Server below.

Configuring the RADIUS Server

Summary of the configuration procedure.

You must configure your RADIUS server to work with the NMC, see the steps below.

For examples of the RADIUS users file with Vendor Specific Attributes (VSAs) and an example of an entry in the dictionary file on the RADIUS server, see the Security Handbook.

1. Add the IP address of the NMC to the RADIUS server client list (file).
2. Users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined. If no Service-Type attributes are configured, users will have read-only access (on the Web UI only). See your RADIUS server documentation for information about the RADIUS users file, and see the Security Handbook for an example.
3. VSAs can be used instead of the Service-Type attributes provided by the RADIUS server. VSAs require a dictionary entry and a RADIUS user's file. In the dictionary file, define the names for the ATTRIBUTE and VALUE keywords, but not for the numeric values. If you change numeric values, RADIUS authentication and authorization will not work. VSAs take precedence over standard RADIUS attributes.

Configuring a RADIUS Server on UNIX® with Shadow Passwords.
If UNIX shadow password files are used (/etc/passwd) with the RADIUS dictionary files, the following two methods can be used to authenticate users:

- If all UNIX users have administrative privileges, add the following to the RADIUS “user” file. To allow only Device Users, change the APC-Service-Type to `Device`.
  ```
  DEFAULT Auth-Type = System
  APC-Service-Type = Admin
  ```
- Add user names and attributes to the RADIUS “user” file, and verify the password against /etc/passwd. The following example is for users `bconners` and `thawk`:
  ```
  bconners Auth-Type = System
  APC-Service-Type = Admin
  ```

Supported RADIUS servers.
FreeRADIUS v1.x and v2.x, and Microsoft Server 2008 and 2012 Network policy Server (NPS) are supported. Other commonly available RADIUS applications may work, but may not have been fully tested.

TACACS+ screen (v3.0.x and higher)

Path: Main > Configuration > Security > Remote Users > TACACS+

You can use a TACACS+ server to authenticate remote users. Use this option to do the following:

- List the TACACS+ servers (a maximum of two) available to the NMC and the time-out period for each.
- Configure the authentication parameters for a new or existing TACACS+ server by clicking on a **TACACS+ Server** link.

TACACS+ Setting	Description
TACACS+ Server	The server name or IP address of the primary or secondary TACACS+ server.
Port	The port number of the primary or secondary TACACS+ server. **NOTE:** TACACS+ servers use port 49 by default to authenticate users. The NMC supports ports 1 to 65535.
Secret	The shared secret between the TACACS+ server and the NMC.
Reply Timeout	The time in seconds that the NMC waits for a response from the TACACS+ server.
Test Settings	Enter the Administrator user name and password in order to test the TACACS+ server path that you have configured.
Skip Test and Apply	Do not test the TACACS+ server path.

See also Remote Users authentication above and Configuring the TACACS+ Server below.

There are two global TACACS+ options that are applicable to all servers:

TACACS+ Setting	Description
Read-Only User Privilege Level	Specify a value between 0 and 15. If an authorized user's privilege level (priv-lvl authorization argument) is greater than or equal to the specified value, and less than the **Administrator Privilege Level**, then the user will be granted read-only access. This value must be less than the **Administrator Privilege Level**.
Administrator Privilege Level	Specify a value between 0 and 15. If an authorized user's privilege level (priv-lvl authorization argument) is greater than or equal to this then the user will be granted administrator access. This value must be greater than the **Read-Only User Privilege Level**.

Configuring the TACACS+ Server

Summary of the configuration procedure.

You must configure your TACACS+ server to work with the NMC.

See more information on configuring the TACACS+ server in the Security Handbook.

Firewall

Path: Main > Configuration > Security > Firewall > Configuration

Enable or disable the firewall functionality. The configured policy is listed by default. Select the Enable check box to enable the firewall. The check box is unchecked by default.

- Click **Apply** to confirm a firewall policy you have selected to enable. The **Firewall Confirmation** page will open.
  - The **Confirmation** page contains a recommendation to test the firewall before enabling. It is not mandatory.
  - The first hyperlink goes to the **Firewall Policy** page.
  - The second hyperlink goes to the **Firewall Test** page.
  - Click **Apply** to enable the firewall and return to the **Configuration** page.
  - Click **Cancel** to return to the **Configuration** page without enabling the **Firewall.**
- Click **Cancel**: No new selection will be enabled. You stay on the **Configuration** page.

Path: Main > Configuration > Security > Firewall > Active Policy

Select an active policy from the **Available Policies** drop-down list, and view the validity of that policy. The current active policy is displayed by default; you can select another from the list.

- Click **Apply** to enable your changes. If a different firewall was selected and enabled, the change is effective immediately. If a newly configured firewall policy has been selected, it is recommended that you test the new firewall before enabling it. (See **Configuration** above.)
- Click **Cancel** to restore the original active policy and stay on the **Active Policy** page.

Path: Main > Configuration > Security > Firewall > Active Policy

Select an active policy from the available firewall policies. The validity of the policy is also listed here.

Path: Main > Configuration > Security > Firewall > Active Rules

When a firewall is enabled, this read-only page lists the individual rules that are being enforced by a current active policy. See **Create/Edit Policy** section for descriptions of the fields (**Priority, Destination, Source, Protocol, Action**, and **Log**).

Path: Main > Configuration > Security > Firewall > Create/Edit Policy

Create a new policy; delete or edit an existing policy.

> **NOTE:** While deleting an active enabled firewall policy cannot be done, editing a running policy can be done but is not recommended as changes are applied immediately. Instead, disable the firewall, edit the policy, test it, and then re-enable the policy.

Create a new policy: Click **Add Policy**, and type in the file name for the new firewall file. The filename should have a .fwl file extension. If left without a file extension, .fwl will be appended to the name automatically.

- Click **Apply**: If the filename is legal, the empty file firewall policy file will be created. It will be located in the /fwl folder with the other policies on the system.
- Click **Cancel** to return to the previous page without creating a new firewall file.

1. Select the policy you want to edit from the **Policy Name** drop-down list, and click **Edit Policy**.
2. Click **Add Rule** or select the **Priority** of an existing rule to go to the **Edit Rule** page. From this page, you can change the rule settings or delete the selected rule.

You can change the rule settings or delete the selected rule.

- **Priority:** If 2 rules conflict, the rule with the higher priority will determine what happens. The highest priority is 1; the lowest is 250.
- Type:
  - **host:** In the IP/any field, you will enter a single IP address.
  - **subnet:** In the IP/any field, you will enter a subnet address.
  - **range:** In the IP/any field, you will enter a range of IP addresses.
- **IP/any:** Specify the IP address or range of addresses this rule applies to, or select one of the following:
  - **any:** The rule applies regardless of the IP address.
  - **anyipv4:** The rule applies for any IPv4 address.
  - **anyipv6:** The rule applies for any IPv6 address.
- **Port:** Specify a port the rule will apply to.
  - **None:** The rule will apply to any port.
  - **Common Configured ports:** Select a standard port.
  - **Other:** Specify a non-standard port number.
- **Protocol:** Specify which protocol the rule applies to.
  - **any:** any protocol.
  - **tcp:** used for reliable information transfer between applications.
  - **udp:** alternative to TCP using for faster, lower bandwidth information transfer. Though it has fewer delays, UDP is less reliable than TCP.
  - **icmp:** used to report errors for troubleshooting.
  - **icmpv6:** used to report errors for troubleshooting on applications using IPv6.
- **Action:**
  - **allow:** Allow the packet that matches this rule.
  - **discard:** Discard the packet that matches this rule.
- **Log:** If this rule applied to a packet, regardless of whether the packet is blocked or allowed, this will add an entry to the **Firewall Log**. See Firewall Log, page 68. It is recommended that you add one of the following as the lowest priority rule in your firewall policy:
- To use the firewall as an allowlist, add `250 Dest any / Source any / protocol any / discard`
- To use the firewall as a blocklist, add `250 Dest any / Source any / protocol any / allow`

Delete a policy:

- Select **Delete Policy** to open the Confirm Deletion page.
- Click **Apply** to confirm . The selected firewall file is removed from the file system.

Path: Main > Configuration > Security > Firewall > Load Policy

Load a policy (with .fwl suffix) from a source external to this device.

Path: Main > Configuration > Security > Firewall > Test

Temporarily enforce the rules of a chosen policy for a time that you specify.

802.1X Security

Path: Main > Configuration > Security > 802.1X Security
The NMC takes the role of a supplicant in an EAPoL (Extensible Authentication Protocol over LAN) architecture used in IEEE 802.1X port-based network access control. The NMC supports the EAP-TLS authentication method.
EAP-TLS performs mutual authentication in a TLS handshake so that the network can authenticate the NMC, and the NMC can authenticate the network. The NMC must have installed an end-entity certificate and its associated private key. This certificate is passed to the authenticator during the handshake. The authenticator's certificate is also passed to the NMC during the handshake. In order for the NMC to verify this certificate, it must also have installed the certificate for the CA that signed this certificate (or the root CA if a chain of trust is used). These certificates must be installed to the NMC's certificate store using the certificate loader. See SSL Certificate, page 38.
The Web UI offers the following options for EAPoL configuration:

NOTE: The options available differ between v2.5.x and v3.x.

The Web UI offers the following options for EAPoL configuration:

- **EAPoL Access:**Enables IEEE 802.1X authentication (EAPoL) using the EAP-TLS authentication method.

  NOTE: 802.1X security access is disabled by default. You can only enable access when a valid client certificate has been installed.

  See SSL Certificate, page 38.
- **Supplicant Identifier:** The identity of the EAP Supplicant to send to the authenticator (up to 32 characters including whitespace).

  NOTE: By default, the supplicant identifier is set to “NMC-Supplicant-xx:xx:xx:xx:xx:xx” where six octets of “xx” are the MAC ID of the NMC.
- **Client Certificate:** The NMC's client certificate to use in the EAP-TLS authentication handshake. A list of installed end-entity certificates is provided and one must be chosen. Client certificates can be installed on the SSL Certificate, page 38 page.

SSL Certificate

Path: Main > Configuration > Security > SSL Certificates

The NMC supports TLS (Transport Layer Security) and SSL (Secure Sockets Layer) which provide a layer of security on top of TCP by adding authentication and encryption to the connection. To support TLS/SSL connections, the NMC provides a certificate store to which both X.509 certificates and private keys can be uploaded. Both CA (Certificate Authority) certificates and end entity certificates may be uploaded. A list of all installed certificates is displayed on this page. Clicking on a certificate’s common name navigates to a certificate details page. The details page provides additional information about the certificate and allows for the file containing it to be uninstalled.

Upload CA Certificate:

- **Certificate File:** Provide the CA certificate. The supported file formats are PEM and DER encoded X.509. The file extension should be .crt, .cer, .pem, or .der. PEM files may contain a list of any number of CA certificates.

Upload Local Device Certificate:

- **Certificate File:** Provide the end entity certificate. The supported file formats are PEM and DER encoded X.509. The file extension should be .crt, .cer, .pem, or .der. PEM files may contain a certificate chain where the first certificate is the end entity certificate. The following certificates must be for intermediate CAs where each certificate directly certifies the one preceding.
- **Private Key File:** Provide the private key for the end entity certificate. The file can be encrypted or unencrypted and must be PEM or DER encoded with PKCS#8 format. The file extension must be .p8, .key, .pem, or .der.

  NOTE: All private keys are encrypted by the NMC prior to storage.

- **Private Key Passphrase:** Provide the passphrase to decrypt the encrypted private key. Allows up to 64 characters including whitespace. If the private key file is not encrypted, this field must be left blank.

Network Configuration

TCP/IP Settings for IPv4

Path: Main > Configuration > Network > TCP/IP > IPv4 Settings

The upper part of the screen displays any current IPv4 address, subnet mask, default gateway, MAC address, boot mode, DHCP server, and lease dates of the unit. Use the lower part of the screen to configure those settings, including disabling IPv4.

- **Manual:** Specify your IPv4 address, subnet mask, default gateway here.
- **BOOTP:** At 32-second intervals, the device requests network assignment from any BOOTP server:
  - If it receives a valid response, it starts the network services.
  - If previously configured network settings exist and it receives no valid response to five requests (the original and four retries), it uses the previously configured settings by default. This ensures that it remains accessible if a BOOTP server is no longer available.
  - If it finds a BOOTP server, but the request to that server does not work or times out, the device stops requesting network settings until it is restarted.
- **DHCP:** At 32-second intervals, the device requests network assignment from any DHCP server.
  - If a DHCP server is found, but the request to that server does not work or times out, it stops requesting network settings until it is restarted.
  - Optionally, you can set up the device with **Require vendor specific cookie to accept DHCP Address** in order to accept the lease and start the network services.
  - **Vendor Class:** This should be APC. This is only available if BOOTP or DHCP is selected.
  - **Client ID:** The MAC address of the device. If you change this value, the new value must be unique on the LAN. This is only available if BOOTP or DHCP is selected.
  - **User Class:** The name of the application firmware module. This is only available if BOOTP or DHCP is selected.

TCP/IP Settings for IPv6

Path: Main > Configuration > Network > TCP/IP > IPv6 Settings

The upper part of this screen displays any current IPv6 settings of the unit. Use the lower part of the screen to configure those settings, including disabling IPv6.

You have the option of using manual or automated IP addressing. It is possible to use them both concurrently. For **Manual**, select the check box and then enter the **System IPv6** address and the **Default Gateway**.

Select the **Auto Configuration** check box to enable the system to obtain addressing prefixes from the router (if available). It will use those prefixes to automatically configure IPv6 addresses.

IPv6 Possible Formats	Description
fe80:0000:0000:0000:0204:61ff:fe9d:f156	full form of IPv6
fe80:0:0:0:204:61ff:fe9d:f156	drop leading zeroes
fe80::204:61ff:fe9d:f156	collapse multiple zeroes to :: in the IPv6 address
fe80:0000:0000:0000:0204:61ff:254.157.241.86	IPv4 dotted quad at the end
fe80:0:0:0:0204:61ff:254.157.241.86	drop leading zeroes, IPv4 dotted quad at the end

IPv6 Possible Formats	Description
fe80::204:61ff:254.157.241.86	dotted quad at the end, multiple zeroes collapsed
::1	localhost
fe80::	link-local prefix
2001::	global unicast prefix

For **DHCPv6 Mode**, see the table below.

Option	Description
Router Controlled	When this radio box is selected, DHCPv6 is controlled by the **M** (Managed Address Configuration Flag) and **O** (Other Stateful Configuration Flag) flags received in IPv6 router advertisements. When a router advertisement is received, the unit checks whether the M and O flags are set. The unit interprets them as follows: • **Neither is set:** Indicates that the local network has no DHCPv6 infrastructure. The unit uses Router Advertisements and manual configuration to get non-link-local addresses and other settings. • **M, or M and O are set:** In this situation, full DHCPv6 address configuration occurs. DHCPv6 is used to obtain addresses AND other configuration settings. This is known as “DHCPv6 stateful.” Once the M flag has been received, the DHCPv6 address configuration stays in effect until the interface in question has been closed, even if subsequent Router Advertisement packets are received in which the M flag is not set. If an O flag is received first, then an M flag is received subsequently, the unit performs full address configuration upon receipt of the M flag. • **Only O is set:** In this situation, the unit sends a DHCPv6 Info-Request packet. DHCPv6 is used to configure “other” settings (such as location of DNS servers), but NOT to provide addresses. This is known as “DHCPv6 stateless.”
Address and Other Information	DHCPv6 is used to obtain addresses AND other configuration settings. This is known as “DHCPv6 stateful.”
Non-Address Information Only	DHCPv6 is used to configure “other” settings (such as location of DNS servers), but NOT to provide addresses. This is known as “DHCPv6 stateless.”
Never	DHCPv6 is NOT used for any configuration settings.

DHCP Response Options

Each valid DHCP response contains options that provide the TCP/IP settings that the unit needs in order to operate on a network. Each response also has other information that affects the operation of the unit.

For more information, refer to FA156110 on **FAQ**, under the **Support** tab at www.schneider-electric.com.

Vendor Specific Information (option 43)

The unit uses this option in a DHCP response to determine whether the DHCP response is valid. This option contains an option in a TAG/LEN/DATA format, called the APC Cookie. This is disabled by default.

- APC Cookie. Tag 1, Len 4, Data “1APC”

  Option 43 communicates to the unit that a DHCP server is configured to service devices.

  The following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie:

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

TCP/IP Options

The unit uses the following options within a valid DHCP response to define its TCP/IP settings. All of these options, except the first, are described in **RFC2132**.

- **IP Address** (from the **yiaddr** field of the DHCP response, described in **RFC2131**)**:** The IP address that the DHCP server is leasing to the unit.
- **Subnet Mask** (option 1)**:** The **Subnet Mask** value that the unit needs to operate on the network.
- **Router**, i.e., Default Gateway (option 3)**:** The default gateway address that the unit needs to operate on the network.
- **IP Address Lease Time** (option 51)**:** The time duration for the lease of the IP Address to the unit.
- **Renewal Time, T1** (option 58)**:** The time that the unit must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59)**:** The time that the unit must wait after an IP address lease is assigned before it can seek to rebind that lease.

Other Options

The unit also uses these options within a valid DHCP response. All of these options except the **Boot File Name** are described in RFC2132.

- **Network Time Protocol Servers** (option 42)**:** Up to two NTP servers (primary and secondary) that the unit can use.
- **Time Offset** (option 2)**:** The offset of the unit subnet, in seconds, from Coordinated Universal Time (UTC).
- **Domain Name Server** (option 6)**:** Up to two Domain Name System (DNS) servers (primary and secondary) that the unit can use.
- **Host Name** (option 12)**:** The host name that the unit will use (32-character maximum length).
- **Domain Name** (option 15)**:** The domain name that the unit will use (64-character maximum length).
- **Boot File Name** (from the file field of the DHCP response, described in RFC2131)**:** The fully qualified directory-path to a user configuration file (.ini file) to download. The **siaddr** field of the DHCP response specifies the IP address of the server from which the unit will download the .ini file. After the download, the unit uses the .ini file as a boot file to reconfigure its settings.

Port Speed

Path: Main > Configuration > Network > Port Speed

The port speed setting defines the communication speed of the Ethernet network port. Your current setting is displayed in **Current Speed**.

You can change the setting by choosing a radio button under **Port Speed**.

- For **Auto-negotiation** (the default), network devices negotiate to transmit at the highest possible speed, but if the supported speeds of two devices are not matched, the slower speed is used.
- Alternatively, you can select 10 Mbps or 100 Mbps, each with the following options:
  - Half-Duplex (communication in only one direction at a time)
  - Full-Duplex (communication in both directions on the same channel simultaneously)

DNS Configuration

Path: Main > Configuration > Network > DNS > Configuration

The values under **Domain Name System Status** list your current status and setup.

Use the options under **Manual Domain Name System Settings** to configure the Domain Name System (DNS).

- **Override Manual DNS Settings:** Enabling **Override Manual DNS Settings** means that configuration data from other sources like DHCP take precedence over the manual configurations here.
- **Primary DNS Server:** Specify the Primary DNS Server and, optionally, the Secondary DNS Server with IPv4 or IPv6 addresses. For the unit to send email, you must at least define the IP address of the primary DNS server.
  - The unit waits up to 15 seconds for a response from the primary DNS server or the secondary DNS server. If the unit does not receive a response within that time, email cannot be sent. Use DNS servers on the same segment as the unit or on a nearby segment, but not across a wide-area network (WAN).
  - After you define the IP addresses of the DNS servers, test it.
- **System Name Synchronization:** Enabling this synchronizes the DNS host name with the unit system name. Click on the **System Name** link to define it.
- **Host Name:** After you configure a host name here and a domain name in the **Domain Name** field, users can enter a host name in any field in the unit interface (except e-mail addresses) that accepts a domain name.
- **Domain Name (IPv4/IPv6):** For the display interface, you only need to configure the domain name here. In all other fields in this UI — except email addresses — that accept domain names, the unit defaults to adding this domain name when only a host name is entered.

  To override the expansion of a specified host name by the addition of a domain name, set this domain name field to its default, `somedomain.com` or to `0.0.0.0`.

  To override the expansion of a specific host name entry (for example, when defining a trap receiver), include a trailing period. The unit recognizes a host name with a trailing period (such as `mySnmpServer.`) as if it were a fully-qualified domain name and does not append the domain name.
- **Domain Name (IPv6):** Specify the IPv6 domain name here.

DNS Testing

Path: Main > Configuration > Network > DNS > Test

Use this option to send a DNS query that tests the setup of your DNS servers by looking up the IP address.

View the result of a test in the **Last Query Response** field.

- For **Query Type**, select the method to use for the DNS query, see the table below.
- For **Query Question**, specify the value to be used for the selected query type as explained in the table.

Query Type Selection	Query Question to Use
By Host	The host name, the URL
By FQDN	The fully-qualified domain name: `my_server.my_domain.com`
By IP	The IP address of the server
By MX	The mail exchange address

Web Access

Path: Main > Configuration > Network > Web > Access

Use this option to configure the access method for the Web interface. In order to activate any changes here, you must log off from the unit display interface.

- **HTTP:** Select this check box to enable access through HTTP. HTTP does not encrypt user names, passwords, and data during transmission.

  NOTE: HTTP is disabled by default.
- **HTTPS:** Select this check box to enable access through HTTPS. HTTPS encrypts user names, passwords, and data during transmission.

  NOTE: HTTPS is enabled by default.
- **HTTP Port:** The port used for HTTP connection. The port range is 5000–32768: default is 80.
- **HTTPS Port:** The port used for HTTPS connection. The port range is 5000–32768: default is 443.

  NOTE: You must use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114 enter `http(s)://152.214.12.114:5000`.
- **Minimum Protocol:** Select the minimum encryption protocol. There are four available.
  - TLS 1.1
  - TLS 1.2
  - TLS 1.3 (v3.1.x and higher)
- **Require Authentication Cookie:** If enabled, a session cookie will be used for authentication tracking within the browser. The cookie will be removed upon session end.
- **Limited Status Access:** Select whether or not to display a read-only, public Web page with basic device status. This feature is disabled by default and can be set via the **Use as default page** option to show as the default landing page when a user accesses the device with just the IP/hostname (no specific page listed).

Web SSL Certificate Configuration

Path: Main > Configuration > Network > Web > SSL Certificate

Add, replace, or remove a security certificate. SSL (Secure Socket Layer) is a protocol used to encrypt data between your browser and the Web server.

- **Status:** The **Status** can be one of the following:
  - **Valid certificate:** A valid certificate was installed or was generated by the unit. Click on this link to view the contents of the certificate.
  - **Certificate not installed:** A certificate is not installed or was installed by FTP or SCP to an incorrect location. Using **Add or Replace Certificate File** installs the certificate to the correct location: /ssl on the unit.
  - **Generating:** The unit is generating a certificate because no valid certificate was found.
  - **Loading:** A certificate is being activated on the unit.

    IMPORTANT: If you install an invalid certificate, or if no certificate is loaded while SSL is enabled, the unit generates a default certificate, a process which delays access to the interface for up to one minute. You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on.
- **Add or Replace Certificate File:** Browse to the certificate file created with the Security Wizard. See Creating and Installing Digital Certificates in the Security Handbook to see how to use digital certificates created by the Security Wizard or generated by the NMC.
- **Remove:** Delete the certificate. See screen text also.

Console Settings

Console Access

Path: Main > Configuration > Network > Console > Access

Console access enables use of the command line interface (CLI).

You can enable access to the CLI through either **Telnet** or **SSH/SCP** or through both, by using the **Enable** check boxes. Telnet does not encrypt user names, passwords, and data during transmission whereas SSH does. **Telnet** is disabled by default; **SSH/SCP** is enabled by default.

For the ports to be used to communicate with the unit, you can change the setting to any unused port from 5000 to 32768 for additional security.

- **Telnet Port:** This is 23 by default. You must then use a colon (:) or a space to specify the non-default port, as required by your Telnet client program.

  For example, for port 5000 and an IP address of 152.214.12.114, your Telnet client requires one of the these commands:

  `telnet 152.214.12.114:5000` or `telnet 152.214.12.114 5000`
- **SSH Port:** This is 22 by default. See the documentation for your SSH client for the command line format required to specify a non-default port.

User Host Key Configuration

Path: Main > Configuration > Network > Console > SSH Host Key

If you are using SSH (Secure Shell Protocol) for console (CLI) access, you can add, replace, or remove the host key on the **User Host Key** screen.

- **Status:** The **Status** indicates whether the host key (private key) is valid. The **Status** can be one of the following:
  - **SSH Disabled:** No host key in use.
  - **Generating:** The unit is creating a host key because no valid host key was found.
  - **Loading:** A host key is being activated on the unit.
  - **Valid:** One of the following valid host keys is in the /ssh directory (the required location on the unit):
    - A 1024-bit or 2048-bit host key created by the Security Wizard
    - A 2048-bit RSA host key generated by the unit
- **Add or Replace Host Key:** Upload a host key file created by the Security Wizard. To use an externally created host key, load the host key before you enable SSH.

  NOTE: To reduce the time required to enable SSH, create and upload a host key in advance. If you enable SSH with no host key loaded, the unit takes up to one minute to create a host key, and the SSH server is not accessible during that time.
- **Remove:** Delete the host key. See screen text also.

To use SSH, you must have an SSH client installed. Most Linux and other UNIX platforms include an SSH client, but Microsoft Windows operating systems do not. Clients are available from various vendors.

SNMPv1 Access Configuration

All user names, passwords, and community names for SNMPv1 are transferred over the network as plain text. If your network requires the high security of encryption, disable SNMPv1 access or set the access for each community to Read. (A community with Read access can receive status information and use SNMPv1 traps.)

When using StruxureWare Data Center Expert or the EcoStruxure™ IT gateway to manage a unit on the public network of a StruxureWare system, you must have SNMPv1 or SNMPv3 enabled in the unit interface. Read access will allow the StruxureWare device to receive traps from the unit, but Write access is required while you use the unit user interface to set the StruxureWare device as a trap receiver.

NOTE: SNMPv1 is disabled by default.

Path: Main > Configuration > Network > SNMPv1 > Access

Use **SNMPv1 Access** to enable or disable SNMPv1 version 1 as a method of communication with the unit.

Access Control

Path: Main > Configuration > Network > SNMPv1 > Access Control

You can configure up to four access control entries to specify which Network Management Systems (NMSs) have access to the unit. To edit, click a community name.

By default, one entry is assigned to each of the four available SNMPv1 communities. You can edit these settings to apply more than one entry to any one community to grant access by several specific IPv4 and IPv6 addresses, host names, or IP address masks.

- By default, a community has access to the unit from any location on the network.
- If you configure multiple access control entries for any one community name, it means that one or more of the other communities have no access to the device.

- **Community Name:** The name that an NMS must use to access the community. The maximum length is 16 ASCII characters.
- **NMS IP/Host Name:** The IPv4 or IPv6 address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (for example, 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain '255' restrict access as follows:
  - 149.225.12.255: Access only by an NMS on the 149.225.12 segment.
  - 149.225.255.255: Access only by an NMS on the 149.225 segment.
  - 149.255.255.255: Access only by an NMS on the 149 segment.
  - 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.
- **Access Type:** The actions an NMS can perform through the community.
  - **Read:** GETS only, at any time
  - **Write:** GETS at any time, and SETS when no user is logged onto the UI or command line interface
  - **Write+:** GETS and SETS at any time
  - **Disable:** No GETS or SETS at any time

SNMPv3 Access Configuration

Path: Main > Configuration > Network > SNMPv3 > Access

For 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, to browse the MIB, and to receive traps.

SNMPv3 is disabled by default. A valid user profile must be enabled with passphrases (**Authentication Passphrase**, **Privacy Passphrase**) set before SNMPv3 communications can be established.

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

The unit supports SHA256, SHA or MD5 authentication and AES256, AES or DES encryption.

Enable **SNMPv3 Access** under the **Access** menu enables this method of communication with this device.

For more information on management information document, see InRow RC Gen 2 MIB.

User Profiles

Path: Main > Configuration > Network > SNMPv3 > User Profiles

By default, **User Profiles** lists the settings of four user profiles configured with the user names **apc snmp profile1** through **apc snmp profile4**, with no authentication and no privacy (no encryption). To edit the following settings for a user profile, click a user name in the list.

- **User Name**: The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters.

- **Authentication Passphrase**: A phrase of 15 to 32 ASCII characters that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be.

  It also verifies that the message has not been changed during transmission, and that the message was communicated in a timely manner. This indicates that it was not delayed and that it was not copied and sent again later at an inappropriate time.
- **Privacy Passphrase**: A phrase of 15 to 32 ASCII characters that ensures the privacy of the data that an NMS is sending to or receiving from this device through SNMPv3, by using encryption.
- **Authentication Protocol**: The implementation of SNMPv3 supports SHA256, SHA and MD5 authentication. One of these must be selected.
- **Privacy Protocol**: The implementation of SNMPv3 supports AES256, AES and DES as the protocols for encrypting and decrypting data. You must use both a privacy protocol and a privacy password, otherwise the SNMP request is not encrypted.

In turn, you cannot select the privacy protocol if no authentication protocol is selected.

Access Control

Path: Main > Configuration > Network > SNMPv3 > Access Control

You can configure up to four access control entries to specify which Network Management Systems (NMSs) have access to the unit. To edit, click a user name.

By default, one entry is assigned to each of the four user profiles. You can edit these settings to apply more than one entry to any one user profile to grant access by several specific IP addresses, host names, or IP address masks.

- By default, all NMSs that use that profile have access to this device.
- If you configure multiple access control entries for one user profile, it means that one or more of the other user profiles must have no access to this device.
- **User Name**: From the drop-down list, select the user profile to which this access control entry will apply. The selections available are the four user names that you configure through the **User Profiles** option.
- **Access Enable**: The SNMP profile (SNMP configuration file) is a configuration file format used to specify the management parameters for SNMP agent devices. Enable the access of SNMP profile , so that network administrators can manage and set the SNMP parameters of the equipment using this configuration file format.
- **NMS IP/Host Name**: The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address (for example, 149.225.12.1) allows access only by the NMS at that location. An IP address mask that contains 255 restricts access as follows:
  - 149.225.12.255: Access only by an NMS on the 149.225.12 segment.
  - 149.225.255.255: Access only by an NMS on the 149.225 segment.
  - 149.255.255.255: Access only by an NMS on the 149 segment.
  - 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.

Modbus Configuration

Use the **Modbus** menu to set up communications between the unit and the building management system (BMS).

For detailed information on Modbus Registration Map , see InRow RC Gen 2 300 mm Modbus Register Map.

Modbus Serial

Path: Main > Configuration > Network > Modbus > Serial

1. Use **Access** to enable or disable Modbus Serial as a method of communication with the NMC.
2. Set the connection parameters for the Modbus Serial connection:
   - **Baud Rate** is the data rate in bits per second. It can be set to 2400 (v3.0.x and higher), 9600 (default), 19200, 38400 (v3.0.x and higher), 57600 (v3.1.x and higher), or 115200 (v3.1.x and higher).
   - **Mode**
     - **Even Parity, 1 Stop Bit (8, E, 1)**: Data is sent with 8 data bits, even parity checking, and 1 stop bit.
     - **Odd Parity, 1 Stop Bit (8, O, 1)**: Data is sent with 8 data bits, odd parity checking, and 1 stop bit.
     - **No Parity, 2 Stop Bits (8, N, 2)**: Data is sent with 8 data bits, no parity checking, and 2 stop bits.
     - **No Parity, 1 Stop Bit (8, N, 1)**: Data is sent with 8 data bits, no parity checking, and 1 stop bit.
   - **Target Unique ID** is the unique ID of the target device. It can be set to a value between 1 and 247.
3. Click **Apply** to save your changes.

Modbus TCP

Path: Main > Configuration > Network > Modbus > TCP

1. Use **Access** to enable or disable Modbus TCP as a method of communication with the NMC.
2. Set the **Port** number for the TCP connection. It can be set to 502 (default) or to a value between 5000 and 32768.
3. Click **Apply** to save your changes.

BACnet Settings

Path: Main > Configuration > Network > BACnet

Use the BACnet options to configure your unit to use the BACnet protocol and to make data available to building automation and control networks.

For more information on the unit data points available via BACnet, see InRow ACRC300 BACnet Application Map.

BACnet Configuration

Use this section to enable BACnet access.

- **Access:** Select the check box to enable BACnet. If this is not enabled, the unit cannot be accessed via BACnet.

  NOTE: BACnet cannot be enabled until the **Device Communication Control Password** is set.
- **Device ID:** A unique identifier for this BACnet device that is used for addressing the device. (0–4194303)
- **Device Name:** A name for this BACnet device. The name must be unique on the BACnet network. The default device name is “BACn”+ the last eight digits of the NMC MAC address. The minimum length is 1 character, the maximum length is 150 characters, and special characters are permitted.

- **Network Protocol:** Select the protocol to be used.
  - BACnet/IP
- **APDU Timeout:** The number of milliseconds that the unit will wait for a response to a BACnet request. Acceptable range: 1000-30000. The default value is 6000.
- **APDU Retries:** The number of BACnet requests attempts that the unit will make before aborting the request. Acceptable range: 0–10. The default value is 3.
- **Device Communication Control Password:** The Device Communication Control service is used by a BACnet client to instruct a remote device (e.g., a BACnet-enabled NMC) to stop initiating, or stop responding to all APDUs (except the Device Communication Control service) for a specified duration of time. This service can be used for diagnostic purposes.

  Specify the **Device Communication Control Password** to ensure that a BACnet client cannot control the BACnet communication of the unit without first providing this password. The password is required to be between 8 and 20 characters and must contain the following:
  - A number
  - An uppercase character
  - A lowercase character
  - A special character

  It is recommended to update the password when you first enable BACnet. You do not need to know the current password to update the password.

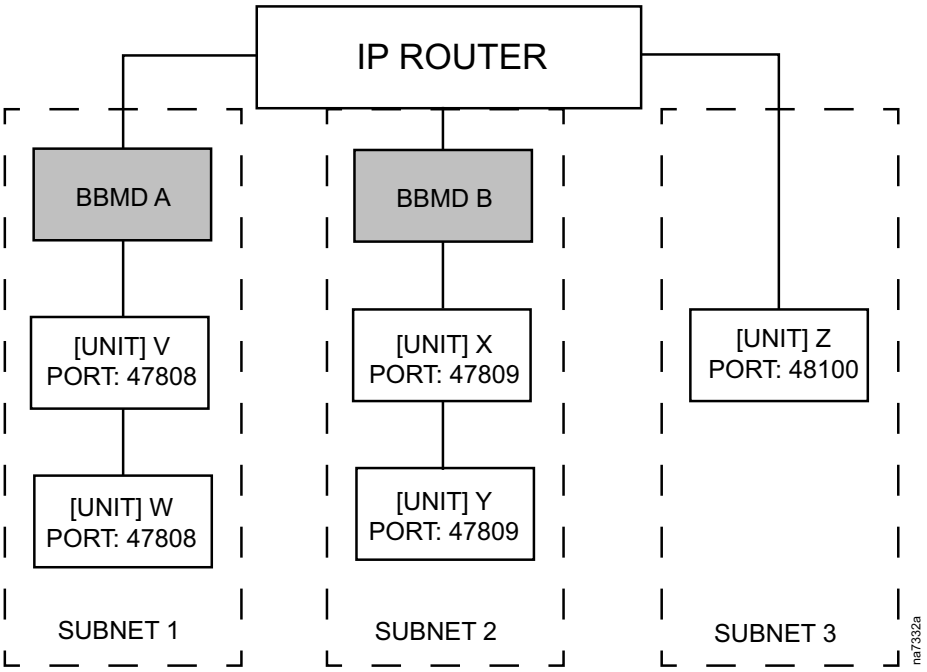
BACnet/IP

- **Local Port:** The UDP/IP port that the unit uses to send and receive BACnet/IP messages. Acceptable range: 5000–65535. Default: 47808.

  NOTE: The address of a BACnet/IP-enabled unit is defined as the IP address of the unit and the local port.

- **Enable foreign device registration:** Select the check box to register the [Application Name] with a BACnet broadcast management device (BBMD).

  NOTE: You need to register your unit as a foreign device with a BBMD if there is no BBMD currently on the subnet of the unit, or if the unit uses a different local port to the BBMD.



  In this example,

  - BBMD A manages the broadcast messages to [UNIT} V and [UNIT} W.
  - BBMD B manages the broadcast messages [UNIT] X and [UNIT] Y.
  - Only [UNIT] Z needs to register with BBMD A or B as a foreign device as there is no BBMD present on its subnet.
  - Once registered, [UNIT] Z can receive broadcast messages from the BBMD with which it is registered, and can send messages to the BBMD, which broadcasts them to all devices on its subnet, and to the other BBMDs on the network via the IP router.

- **Status:** The status of the foreign device registration (FDR):
  - Foreign device registration inactive

    FDR will be inactive if one of the following is true:
    - FDR is enabled and BACnet is disabled
    - FDR is disabled and BACnet is enabled
    - FDR is disabled and BACnet is disabled
  - Registration successful

    FDR has completed successfully
  - Registration rejected

    FDR has not completed successfully. The unit will retry registration automatically, but you can also toggle the **Enable foreign device registration** check box to prompt the unit to retry registration.
  - Registration sent

    The FDR request has been sent, but it has not yet completed.
- **BACnet/IP Broadcast Management Device:** The IP address or fully qualified domain name (FQDN) of the BACnet broadcast management device with which this unit will be registered.
- **Port:** The port of the BBMD with which this unit will be registered.

- **TTL:** The number of seconds (Time To Live) that the BBMD will maintain the unit] as a registered device. If the unit does not re-register before this time expires, the BBMD will delete it from its foreign device table, and the unit will no longer be able to send and receive broadcast messages via the BBMD. The TTL controls how frequently the unit registers with the BBMD, as the unit will attempt to re-register before this time expires.

FTP Server Access Configuration

Path: Main > Configuration > Network > FTP Server

Use this screen to enable access to an FTP server and to specify a port.

NOTE: FTP is disabled by default.

- **Access:** FTP transmits files without encrypting them. For encrypted file transfer, use Secure CoPy (SCP). SCP (via SSH) is automatically enabled when you enable SSH, but you must disable the FTP Server here to enforce high-security file transfer.

  NOTE: SCP will not allow a file transfer until the Super User default password (`apc`) is changed.

  NOTE: At any time that you want a device to be accessible for management by StruxureWare Data Center Expert, FTP Server must be enabled in the display interface of that unit.

  For detailed information on enhancing and managing the security of your system, see the Security Handbook.

- **Port:** The TCP/IP port of the FTP server (21 by default). The FTP server uses both the specified port and the port one number lower. The allowed non-default port numbers are indicated on the screen: 21, and 5001–32768.

  NOTE: Configuring the FTP server to use a non-default port enhances security by requiring users to append the port name to the IP address in an FTP command line. The appended port name must be preceded by a space or colon depending on the FTP client used.

Notification Menu

Types of Notification

You can configure notification actions to occur in response to an event. You can notify users of an event in any of several ways:

- Active, automatic notification: The specified users or monitoring devices are contacted directly.
  - E-mail notification
  - SNMP traps
  - Remote Monitoring Service
  - Syslog notification

- Indirect notification
  - Event log: If no direct notification is configured, users must check the log to determine which events have occurred.

    You can also log system performance data to use for device monitoring. See Log Configuration, page 59 for information on how to configure and use this data logging option.

  - Queries (SNMP GETs)

    For more information, see SNMP Trap Receiver Configuration, page 56 and SNMP Traps Test Configuration, page 57. SNMP enables an NMS to perform informational queries. For SNMPv1, which does not encrypt data before transmission, configuring the most restrictive SNMP access type (READ) enables informational queries without the risk of allowing remote configuration changes.

The unit supports the use of the RFC1628 MIB (Management Information Base). See SNMP Trap Receiver Configuration, page 56 for information on how you can set up a trap receiver. The 1628 MIB group of three events only works with that MIB, not the alternative Powernet MIB. They can be configured like any event (see Configuring Event Actions, page 53).

Configuring Event Actions

By Event

Path: Main > Configuration > Notification > Event Actions > By Event

By default, logging an event is selected for all events. To define event actions for an individual event:

1. To find an event, click on a column heading to see the lists under the **Device Events** or **System Events** categories.
2. Or you can click on a sub-category under these headings, like **Security** or **Temperature**. Click on the event name to view or change the current configuration, such as recipients to be notified by e-mail, or Network Management Systems (NMSs) to be notified by SNMP traps.

   If no Syslog server is configured, items related to Syslog configuration are not displayed.

   When viewing details of an event configuration, you can enable or disable event logging or Syslog, or disable notification for specific e-mail recipients or trap receivers, but you cannot add or remove recipients or receivers. To add or remove recipients or receivers, see the following:

   - See Identify Syslog Servers, page 59.
   - See E-Mail Notification Configuration, page 55.
   - See SNMP Trap Receiver Configuration, page 56.

By Group

Path: Main > Configuration > Notification > Event Actions > By Group

To configure a group of events simultaneously:

1. Select how to group events for configuration:
   - Select **Events by Severity**, and then select one or more severity levels. You cannot change the severity of an event.
   - Select **Events by Category**, and then select all events in one or more pre-defined categories.
2. Click **Next** to move to the next screen to do the following:
   - Select event actions for the group of events.
     - To select any action except **Logging** (the default), you must first have at least one relevant recipient or receiver configured.
     - If you selected **Logging** and have configured a Syslog server, select **Event Log** or **Syslog** on the next screen.

See Log Configuration, page 59.

3. Click **Next** to move to the next screen to do the following:
   - If you selected **Logging** on the previous screen, select **Enable Notifications** or **Disable Notification**.
   - If you selected **Email Recipients** on the previous screen, select the e-mail recipients to configure.
   - If you selected **Trap Receivers** on the previous screen, select the trap receiver to configure.
4. Click **Next** to move to the next screen to do the following:
   - If you are configuring **Logging** settings, view the pending actions and click **Apply** to accept the changes or click **Cancel** to revert to the previous settings.
   - If you are configuring **Email Recipients** or **Trap Receivers**, select **Enable Notifications** or **Disable Notification**and set the notification timing settings.
5. Click **Next** to move to the next screen to do the following:
   - View the pending actions and click **Apply** to accept the changes or click **Cancel** to revert to the previous settings.

Notification Parameters

These configuration fields define e-mail parameters for sending notifications of events. These are usually accessed by clicking the receiver or recipient name

Field	Description
Delay *n* time before sending	If the event persists for the specified time, the notification is sent. If the condition clears before the time expires, no notification is sent.
Repeat at an interval of *n*	The notification is sent repeatedly at the specified interval (the default is every two minutes until the condition clears).
Up to *n* times	During an active event, the notification repeats for this number of times.
or	
Until condition clears	The notification is sent repeatedly until the condition clears or is resolved.

For events that have an associated clearing event, you can also set these parameters. (An example of an event with its clearing event is `RD: Fan 2 Error Detected` and `RD: Fan 2 Error Corrected`).

E-Mail Notification Configuration

Use Simple Mail Transfer Protocol (SMTP) to send e-mail to up to four recipients when an event occurs. To use the e-mail feature, you must define the following settings:

- The IP addresses of the primary and, optionally, the secondary Domain Name System (DNS) servers.
- The IP address or DNS name for the SMTP Server and **From Address**, when **Sever** is set to **Local** for a least one e-mail recipient. See SMTP Server and E-mail recipients below.
- The e-mail addresses for a maximum of four recipients.
- You can use the **To Address** setting of the recipients option to send e-mail to a text-based screen.

SMTP Server

Path: Main > Configuration > Notification > E-mail > Server

This screen lists your primary and secondary DNS servers and displays the following fields:

- **From Address**: The address **From** which e-mail will be sent by the NMC.
- **SMTP Server**: The IPv4/ IPv6 address or DNS name of the local SMTP server.
- **Port**: The SMTP port number, with a default of 25. Common ports are 25 for unencrypted e-mail, 465 and 587 for SSL/TLS encrypted e-mail. You can change the port setting to any port from 1 to 65535.
- **Authentication**: Enable this if the SMTP server requires authentication.
  - **User Name, Password, and Confirm Password**: If the SMTP server requires authentication, type your user name and password here.
- **Use SSL/TLS**: Select when encryption is used.
  - **Never**: The SMTP server does not require nor support encryption. If the SMTP server requires authentication, type your user name and password here.
  - **If Supported**: The SMTP server advertises support for STARTTLS but does not require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given. If the SMTP server requires authentication, type your user name and password here.
  - **Always**: The SMTP server requires the STARTTLS command to be sent upon connection to the server. This is typically used with port 587.
  - **Implicitly**: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server. This is typically used with port 465.
- **Require CA Root Certificate**: This should only be enabled if the security policy of your organization does not allow for implicit trust of SSL/TLS connections. If this is enabled, a valid root CA certificatefor the SMTP server must be installed to the NMC's certificate store using the certificate loader in order for a TLS connection with the SMTP server to succeed. See **SSL Certificates**.

E-mail Recipients

Path: Main > Configuration > Notification > E-mail > Recipients

Specify up to four e-mail recipients. Click on a name to configure the settings.

- **Generation**: Enables (default) or disables sending e-mail to the recipient.

- **To Address**: The user and domain names of the recipient. To use e-mail for paging, use the email address for the recipient pager gateway account (for example, `myacct100@skytel.com`). The pager gateway will generate the page.

  To bypass the DNS lookup of the IP address of the mail server, use the IP address in brackets instead of the email domain name, e.g., use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly.

  NOTE: The recipient pager must be able to use text-based messaging.
- **Format**: The long format contains name, location, contact, IP address, serial number of the device, date and time, event code, and event description. The short format provides only the event description.
- **Language**: Chose a language from the drop-down list and any mails will be sent in that language. It is possible to use different languages for different users.
- **Server**: Select one of the following methods for routing e-mail:
  - **Local**: This is through the site-local SMTP server. This recommended setting ensures that the e-mail is sent using the site-local SMTP server. Choosing this setting limits delays and network outages and retries sending e-mail for many hours. When choosing the **Local** setting you must also enable forwarding at the SMTP server of your device and set up a special external e-mail account to receive the forwarded e-mail. Check with your SMTP server administrator before making these changes.
  - **Recipient**: This is the SMTP server of the recipient. The unit performs an MX record look-up on the recipients e-mail address and uses that as its SMTP server. The e-mail is only sent once so it could easily be lost.
  - **Custom**: This setting enables each e-mail recipient to have its own server settings. When selected, the server settings that follow are enabled. These settings are independent of the settings given under **SMTP Server**.

E-mail Test

Path: Main > Configuration > Notification > E-mail > Test

Send a test message to a configured recipient.

SNMP Trap Receiver Configuration

Path: Main > Configuration > Notification > SNMP Traps > Trap Receivers

With Simple Network Management Protocol (SNMP) traps, you can automatically get notifications for significant unit events. They are a useful tool for monitoring devices on your network.

The trap receivers are displayed by **NMS IP/Host Name**, where NMS stands for Network Management System. You can configure up to six trap receivers.

To configure a new trap receiver, click **Add Trap Receiver**. To edit (or delete) one, click its IP address/host name.

- **Trap Generation:** Enable (the default) or disable trap generation for this trap receiver.
- **NMS IP/Host Name:** The IPv4/ IPv6 address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.
- **Language:** Select a language from the drop-down list. This can differ from the UI and from other trap receivers

  Select either the **SNMPv1** or **SNMPv3** .radio button to specify the trap type. For an NMS to receive both types of traps, you must separately configure two trap receivers for that NMS, one for each trap type.

- **SNMPv1:** Settings for SNMPv1.
  - **Community Name:** The name used as an identifier when SNMPv1 traps are sent to this trap receiver.
  - **Authenticate Traps:** When this option is enabled (the default), the NMS identified by the NMS IP/Host Name setting will receive authentication traps (traps generated by invalid attempts to log on to this device).
- **SNMPv3:** Settings for SNMPv3.
  - **User Name:** Select the identifier of the user profile for this trap receiver.

If you delete a trap receiver, all notification settings configured under Configuring Event Actions, page 53 for the deleted trap receiver are set to their default values.

SNMP Traps Test Configuration

Path: Main > Configuration > Notification > SNMP Traps > Test

- **Last Test Result:** The result of the most recent SNMP trap test. A successful SNMP trap test verifies only that a trap was sent; it does not verify that the trap was received by the selected trap receiver. A trap test succeeds if all of the following are true:
  - The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
  - The trap receiver itself is enabled.
  - If a host name is selected for the To address, that host name can be mapped to a valid IP address.
- **To:** Select the IP address or host name to which a test SNMP trap will be sent. If no trap receiver is configured, a link to the **Trap Receiver** configuration screen is displayed.

General Menu

This menu contains miscellaneous configuration items including device identification, date and time, exporting and importing your unit configuration options, the three links at the bottom left of the screen, and consolidating data for troubleshooting purposes.

Identification Screen

Path: Main > Configuration > General > Identification

Define the **Name**, the **Location** (the physical location), the **System Message** (a custom defined message displayed at log on) and the **Contact** (the person responsible for the device) used by

- The SNMP agent of the unit
- EcoStruxure™ IT or Data Center Expert

Specifically, the name field is used by the **sysName**, **sysContact**, and **sysLocation** object identifiers (OIDs) in the SNMP agent of the unit. For more information about MIB-II OIDs, see the PowerNet® *SNMP Management Information Base (MIB) Reference Guide*, available at www.schneider-electric.com.

The **Name** and **Location** fields also identify the device when you register for the Remote Monitoring Service.

You may leave a **System Message** of up to 256 characters.

Date/Time Configuration

Mode

Path: Main > Configuration > General > Date/Time > Mode

Set the time and date used by the unit. You can change the current settings manually or through a Network Time Protocol (NTP) Server.

With both, you select the **Time Zone**. This is your local time difference with Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT).

- **Manual Mode:** Do one of the following:
  - Enter the date and time for the unit.
  - Select the check box **Apply Local Computer Time** to apply the date and time settings of the computer you are using.
- **Synchronize with NTP Server:** Have an NTP (Network Time Protocol) Server define the date and time for the unit. By default, any unit on the private side of a EcoStruxure™ IT or Data Center Expert obtains its time settings by using EcoStruxure™ IT or Data Center Expert as an NTP server.
  - **Override Manual NTP Settings:** If you select this, data from other sources (typically DHCP) take precedence over the NTP configurations you set here.
  - **Primary NTP Server:** Enter the IP address or domain name of the primary NTP server.
  - **Secondary NTP Server:** Enter the IP address or domain name of the secondary NTP server, when a secondary server is available.
  - **Update Interval:** Define, in hours, how often the unit accesses the NTP Server for an update. Minimum: 1; Maximum: 8760 (1 year).
  - **Update Using NTP Now:** Initiate an immediate update of the date and time by the NTP Server.

Daylight Savings

Path: Main > Configuration > General > Date /Time > Daylight Savings

Daylight Saving Time (DST) is disabled by default. You can enable traditional United States DST, or enable and configure a customized daylight saving time to match how Daylight Saving Time is implemented in your local area.

When customizing DST, the system puts the clock forward by an hour when the time and date you specify under **Start** is reached and puts the clock back an hour when the time and date you specify under **End** is reached.

- If your local DST always starts or ends on the fourth occurrence of a specific weekday of a month (e.g., the fourth Sunday), select **Fourth/Last**. If a fifth Sunday occurs in that month, you should still choose **Fourth/Last**.
- If your local DST always starts or ends on the last occurrence of a specific weekday of a month, whether it is the fourth or the fifth occurrence, select **Fifth/Last**.

Create and Import Settings with the Configuration File

Path: Main > Configuration > General > User Config File

You can speed up and simplify the configuration of new devices by re-using the existing configuration settings with this option. Use **Upload** to transfer configuration data to this interface and **Download** to transfer from this interface (and then use the file to configure another interface). The default name of the file is config.ini.

Configure the Links Screen

Path: Main > Configuration > General > Quick Links

Use this option to view and change the URL links displayed at the bottom-left of each screen of the interface.

To reconfigure a link, click the link name in the **Name** column. You can reset the links to their defaults at any time by clicking on **Reset to Defaults**.

Log Configuration

Identify Syslog Servers

Path: Main > Configuration > Logs > Syslog > Servers

Click **Add Server** to configure a new Syslog server.

- **Syslog Server:** Uses IPv4/ IPv6 addresses or host names to identify from one to four servers to receive Syslog messages sent by the unit.
- **Port:** The user datagram protocol (UDP) port that the unit will use to send Syslog messages. The default UDP port assigned to Syslog is 6514, which is the port assigned to secure Syslog (TLS).
- **Protocol:** Select either UDP, TCP, or TLS.
- **Language:** Select the language for any Syslog messages.
- **Certificate:** When the selected protocol is TLS, choose a client certificate to use for mutual authentication with the Syslog server. The default option **None** disables mutual authentication. Client certificates can be installed on the **SSL Certificates**.

Syslog Settings

Path: Main > Configuration > Logs > Syslog > Settings

- **Message Generation:** Enable the generation and the logging of Syslog messages for events that have Syslog configured as a notification method.

See Configuring Event Actions, page 53.

- **Facility Code:** Selects the facility code assigned to the Syslog messages of the unit (User, by default).

  NOTE: User best defines the Syslog messages sent by the unit. Do not change this selection unless advised to do so by the Syslog network or system administrator.

- **Severity Mapping:** This section maps each severity level of the unit or environment events to available Syslog priorities. The local options are **Critical**, **Warning**, and **Informational**. You should not need to change the mappings.
  - **Emergency:** The system is unusable
  - **Alert:** Action must be taken immediately
  - **Critical:** Critical conditions
  - **Error:** Error conditions
  - **Warning:** Warning conditions
  - **Notice:** Normal but significant conditions
  - **Informational:** Informational messages
  - **Debug:** Debug-level messages

  The following are the default settings for the **Local Priority** settings:
  - **Critical** is mapped to **Critical**
  - **Warning** is mapped to **Warning**
  - **Informational** is mapped to **Info**

To disable Syslog messages, see Configuring Event Actions, page 53.

Syslog Test and Format Example

Path: Main > Configuration > Logs > Syslog > Test

Send a test message to the Syslog servers (configured through Identify Syslog Servers, page 59). The result will be sent to all configured Syslog servers.

Select a severity to assign to the test message and then define the test message. Format the message to consist of the event type (for example, APC, System, or Device) followed by a colon, a space, and the event text. The message can have a maximum of 50 characters.

- The priority (PRI): The Syslog priority assigned to the message event, and the facility code of messages sent by the unit.
- The Header: A time stamp and the IP address of the unit.
- The message (MSG) part:
  - The TAG field, followed by a colon and space, identifies the event type.
  - The CONTENT field is the event text, followed (optionally) by a space and the event code.

    Example: `APC: Test Syslog is valid.`

Tests

Set the Unit LED Lights to Blink

Path: Main > Tests > Network > LED Blink

If you are having trouble finding your unit, enter a number of minutes in the **LED Blink Duration** field, click **Apply**, and the LED lights under the panel on the right side of the display will blink.

Logs and About Menus

Event and Data Logs

The event log records individual occurrences. The data log, by contrast, provides you with a snapshot of your system by recording values at regular time intervals.

In v3.0.x and higher, each Event contains the following information:

- **Date**: The date the event occurred.
- **Time**: The time the event occurred.
- **User**: The user that initiated the action. This can either be the username, “system” if it was part of an internal service, or “device” if it was initiated by the connected device.
- **Event**: The text which describes the event.

Event Log

In v3.0.x and higher, by default, the log displays all events. See Configuring Event Actions, page 53.

The Event Log records all events including access control, request errors, system events, configuration changes (including via config.ini file) and audit events. It can be configured to store from 25 to 30,000 events, the default is 1500. If the Event log is full and a new event occurs, the oldest event will be overwritten. If you want to retain your events, you should configure exporting events to a Syslog server.

You can enable color coding for events on the **Main > Configuration > Security > Local Users > Management** screen.

By default, the event log displays the most recent events first. To see the events listed together on a Web page, click **Launch Log in New Window** button. JavaScript must be enabled in your browser to do this.

To open the log in a text file or to save the log to disk, click on the floppy disk icon () on the same line as the **Event Log** heading.

You can also use FTP or Secure CoPy (SCP) to view the event log. See How to Use SCP or FTP to Retrieve Log Files, page 68.

Filter Event Logs

Use filtering to omit information you do not want to display.

- Filtering the log by date or time: Use the **Last** or **From** radio buttons. (The filter configuration is saved until the unit restarts.)
- Filtering the log by event severity or category:
  1. Click **Filter Log**.
  2. Clear a check box to remove it from view.
  3. After you click **Apply**, text at the upper-right corner of the **Event Log** page indicates that a filter is active. The filter is active until you clear it or until the unit restarts.
- Removing an active filter:
  1. Click **Filter Log**.
  2. Click **Clear Filter (Show All)**.
  3. As Administrator, click **Save As Default** to save this filter as the new default log view for all users.

The following are important points on filtering:

- Events are processed through the filter using OR logic. If you apply a filter, it works regardless of the other filters.
- Events that you cleared in the Filter By Severity list never display in the filtered Event Log, even if selected in the Filter by Category list.
- Similarly, events that you clear in the Filter by Category list never display in the filtered Event Log.

Delete Event Log

To delete all events, click **Clear Log**. Deleted events cannot be retrieved.

To disable the logging of events based on their assigned severity level or their event category, see Configuring Event Actions, page 53.

Launch Log in New Window

Click **Launch Log in New Window** to launch the event log in a new browser window that provides a larger view of the graph.

With reverse lookup enabled, when a network-related event occurs, both the IP address and the domain name for the network device with the event are logged in the event log. If no domain name entry exists for the device, only its IP address is logged with the event.

Since domain names generally change less frequently than IP addresses, enabling reverse lookup can improve the ability to identify addresses of networked devices that are causing events.

Reverse lookup is disabled by default. You should not need to enable it if you have no DNS server configured or have poor network performance because of heavy network traffic.

Use **Event Log Size** to specify the maximum number of log entries.

IMPORTANT: When you re-size the event log in order to specify a maximum size, all existing log entries are deleted. When the log subsequently reaches the maximum size, the older entries are deleted.

Configure Reverse Lookup

Path: Main > Logs > Events > Reverse Lookup
With reverse lookup enabled, when a network-related event occurs, both the IP address and the domain name for the networked device with the event are logged in the Event Log. If no domain name entry exists for the device, only its IP address is logged with the event. Since domain names generally change less frequently than IP addresses, enabling reverse lookup can improve the ability to identify addresses of networked devices that are causing events. Reverse lookup is disabled by default. You should not need to enable it if you have no DNS server configured or have poor network performance because of heavy network traffic.

Resize the Event Log

Path: Main > Logs > Events > Size
Use **Event Log Size** to specify the maximum number of log entries.

⚠CAUTION

DATA LOSS

When you resize the **Event Log**, in order to specify a maximum size, all existing log entries are deleted. To avoid losing log data, use SCP or FTP to retrieve the log first, see . When the log subsequently reaches the maximum size, the older entries are deleted

Failure to follow these instructions can result in injury or equipment damage.

Data Log

Path: Main > Logs > Data > Log

Use the data log to display measurements about the unit, the power input to the unit, and the ambient temperature of the unit.

The steps to display and re-size the data log are the same as for the event log, except that you use menu options under **Data** instead of **Events**.

Filter Data Log

Use filtering to omit information you do not want to display.

Filter Log by Date or Time

Use the **Last** or **From** radio buttons. (The filter configuration is saved until the unit restarts.)

Delete Data Log

To delete all events, click **Clear Data Log**. Deleted events cannot be retrieved.

Data Graphing

Path: Main > Logs > Data > Graphing

Data log graphing provides a graphical display of logged data and is an enhancement of the existing data log feature. How the graphing enhancement displays data and how efficiently it performs will vary depending on your computer hardware, computer operating system, and the Web browser you use to access the interface of the unit.

NOTE: JavaScript® must be enabled in your browser to use the graphing feature. Alternatively, you can use FTP or SCP to import the data log into a spreadsheet application, and graph data in the spreadsheet.

- **Graph Time:** Select **Last** to graph all records or to change the number of hours, days, or weeks for which data log information is graphed. Select a time option from the drop-down menu. Select **From** to graph data logged during a specific time period.

  NOTE: Enter time using the 24-hour clock format.
- **Apply:** Click **Apply** to graph the data.
- **Launch Graph in New Window:** Click **Launch Log in New Window** to launch the data log in a new browser window that provides a larger view of the graph.

Data Log Intervals

Path: Main > Logs > Data > Interval

Define, in the **Log Interval** setting, how frequently data is searched for and stored in the data log. When you click **Apply**, the number of possible storage days is recalculated and display at the top of the screen. When the log is full, the oldest entries are deleted.

> **NOTE:** Because the interval specifies how often the data is recorded, the smaller the interval, the more times the data is recorded and the larger the log file.

Data Log Rotation

Path: Main > Logs > Data > Rotation

Rotation causes the contents of the data log to be appended to the file you specify by name and location. Use this option to set up password-protection and other parameters.

- **FTP Server:** The IP address or host name of the server where the file will reside.
- **User Name/Password:** The user name with password required to send data to the repository file. This user must also be configured to have read and write access to the data repository file and the directory (folder) in which it is stored.
- **File Path:** The path to the repository file.
- **Filename:** The name of the repository file (an ASCII text file), e.g. datalog.txt. Any new data is appended to this file: it does not overwrite it.
- **Unique Filename:** Select this check box to save the log as mmddyyyy_ <filename>.txt, where filename is what you specified in the **Filename** field. Any new data is appended to the file but each day has its own file.
- **Delay n hours between uploads:** The number of hours between uploads of data to the file (max. 24 hours).
- **Upon failure, try uploading every n minutes:** The number of minutes between attempts to upload data to the file after a failed upload.
- **Maximum Attempts:** The maximum number of times the upload will be attempted after it fails initially.
- **Until upload succeeds:** Attempt to upload the file until the transfer is completed.

Data Log Size

Path: Main > Logs > Data > Size

Use **Data Log Size** to specify the maximum number of log entries.

IMPORTANT: When you resize the data log in order to specify a maximum size, all existing log entries are deleted. When the log subsequently reaches the maximum size, the older entries are deleted.

Firewall Log

Path: Main > Logs > Firewall

If you create a firewall policy, firewall events will be logged here.

For more information on implementing a policy, see Firewall, page 36.

The information in the log can be useful to help the technical support team solve problems. Log entries contain information about the traffic and the rules action (allowed, discarded). When logged here, these events are not logged in the main Event Log .

A Firewall log contains up to 50 of the most recent events. The Firewall log is cleared when the display reboots.

How to Use SCP or FTP to Retrieve Log Files

A Super User/Administrator or Device User can use SCP or FTP to retrieve a tab-delineated event log file (event.txt) or data log file (data.txt) and import it into a spreadsheet. Both reside on the unit.

- The file reports all events or data recorded since the log was last deleted or, in the case of the data log, truncated because it reached maximum size.
- The file includes information that the event log or data log does not display.
  - The version of the file format (first field)
  - The date and time the file was retrieved
  - The **Name**, **Contact**, and **Location** values and IP address of the unit
  - The unique **Event Code** for each recorded event (event.txt file only)
  - The unit uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits.

If you are using the encryption-based security protocols, see Use SCP to Retrieve the Files, page 68.

If you are using unencrypted authentication methods for security, see Use FTP to Retrieve the Files, page 69.

See the Security Handbook for information on available protocols and methods for setting up the type of security you need.

Use SCP to Retrieve the Files

Enable SSH on the unit to use SCP to retrieve files.

See Console Settings, page 45.

To retrieve the event.txt file, use the following command:

```
scp <username@hostname> or <ip_address>:event.txt./event.txt
```

To retrieve the data.txt file, use the following command:

```
scp <username@hostname> or <ip_address>:data.txt./data.txt
```

NOTE: When the SCP command is used in OpenSSH version 9.0 or higher, SFTP is used by default for file transfers. This causes an issue as the NMC does not support SFTP. To use SCP with version 9.0 or higher, the `-O` option must be added to the SCP command in order to use the SCP protocol (scp -O <file><User>@<remote>:<file>).

Use FTP to Retrieve the Files

To use FTP to retrieve the event.txt or data.txt file:

1. At a command prompt, type `ftp` and the IP address of the unit, and press `Enter`.

   If the **Port** setting for the **FTP Server** option has been changed from its default (21), you must use the non-default value in the FTP command.

   For Windows-based FTP clients, use the following command, including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)

   ```
   ftp>open ip_address port_number
   ```

   To set a non-default port value to enhance security for the FTP Server, see FTP Server Access Configuration, page 52. You can specify any port from 5001 to 32768.

2. Use the case-sensitive **User Name** and **Password** for the Super User/ Administrator or Device User to log on. For Administrator, `apc` is the default for the user name. For the Device User, the defaults user name is `device`.
3. Use the `get` command to transmit the text of a log to your local drive.

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

   or

   ```
   ftp>get data.txt
   ```
4. You can use the `del` command to clear the contents of either log.

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

   or

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

   You will not be asked to confirm the deletion.

   - If you clear the data log, the event log records a deleted-log event.
   - If you clear the event log, a new event.txt file records the event.
5. Type `quit` at the `ftp>` prompt to exit from FTP.

About the Unit

Path: Main > About > Device

The information displayed varies according to the device used.

- **Model Number**
- **Serial Number**
- **Firmware Revision**
- **Hardware Revision**
- **Ctrl Bootloader Rev**
- **PIC 1–2 F/W Rev**
- **PIC 1–2 Bootloader Rev**

About the Network

Path: Main > About > Network

NOTE: Some items may not appear for your unit.

Hardware Factory

This hardware information is useful for troubleshooting problems with your NMC device including model and serial number, hardware revision, manufacture date, MAC address, and management uptime.

- **Management Uptime**: refers to the length of time this management interface has been running continuously; that is, the length of time since the NMC has been warm or cold started.
- **Application Module ,APC OS(AOS)**, and **Boot Monitor**: This information is useful for troubleshooting, and for determining if updated firmware is available at www.apc.com/shop/us/en/tools/software-firmware.

Network Management Card 3

This information is the serial number of the Network Management Card embedded in the display interface.

Application Module, APC OS (AOS), and APC Boot Monitor

This information is useful for troubleshooting and for determining if updated firmware is available.

- **Name:** The name of the firmware module. The APC AOS module is always named aos, and the boot monitor module is always named bootmon.
- **Version:** The version number of the firmware module. Version numbers of the modules may differ, but compatible modules are released together. Never combine application modules and AOS modules from different releases.

  NOTE: If the boot monitor module must be updated, a boot monitor module is included in the firmware release. Otherwise, the boot monitor module that is installed on the card is compatible with the firmware update.
- **Date/Time:** The date and time at which the firmware module was loaded

Troubleshooting and Support

Path: Main > About > Support

There are three links to useful websites. These links access the URLs for these Web pages:

- Link 1: Knowledge Base
- Link 2: Schneider Electric Product Center
- Link 3: Schneider Electric Downloads

Technical Support Debug Information Download

With this option, you can consolidate various data in this interface into a single ZIP file for troubleshooting purposes and customer support. The data includes the event and data logs, the configuration file, and complex debugging information.

Click **Generate Logs** to create the file and then **Download**. You are asked whether you want to view or save the TAR file.

Device IP Configuration Wizard

Capabilities, Requirements, and Installation

How to Use the Wizard to Configure TCP/IP Settings

- Remotely over your TCP/IP network to discover and configure any unconfigured cooling units on the same nettwork segment as the computer running the Wizard.
- Through a direct connection from a serial port of your computer to the cooling unit to configure or reconfigure it.

System Requirements

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

NOTE: The Wizard is for IPv4 only.

Installation

To install the Wizard from a downloaded executable file:

1. Go to www.apc.com/shop/tools/software-firmware..
2. Filter by **Software / Firmware > Wizards and Configurators**.
3. Run the executable file in the folder to which you downloaded it.

Use the Wizard

NOTE: Most software Firewalls must be temporarily disabled for the Wizard to discover unconfigured units.

Launch the Wizard

The installation creates a shortcut link in the **Start** menu to launch the Wizard.

Configure the Basic TCP/IP Settings Remotely

Prepare to Configure the Settings

Before you run the Wizard:

1. Contact your network administrator to obtain valid TCP/IP settings.
2. If you are configuring multiple unconfigured units, obtain the MAC address of each one to identify it when the Wizard discovers it. (The Wizard displays the MAC address on the screen on which you then enter the TCP/IP settings.)
   - The MAC address is accessible on the Web suer interface on the **Main > About > Display > Device** screen.

Run the Wizard to Perform the Configuration

To discover and configure unconfigured units over the network:

1. From the **Start** menu, launch the Wizard. The Wizard detects the first cooling unit that is not configured.
2. Select **Remotely (over the network)**, and click **Next >**.
3. Enter the system IP, subnet mask, and default gateway for the cooling unit identified by the MAC address. Click **Next >**.

   On the **Transmit Current Settings Remotely** screen, if you select the **Start a Web browser when finished** check box, the default Web browser connects to the cooling unit after the Wizard transmits the settings.
4. Click **Finish** to transmit the settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
5. If the Wizard finds another unconfigured cooling unit, it displays the screen to enter TCP/IP settings. Repeat this procedure beginning at step 3, or to skip the cooling unit whose MAC address is currently displayed, click **Cancel**.

Configure or Re-Configure the TCP/IP Settings Locally

1. Contact your network administrator to obtain valid TCP/IP settings.
2. Connect the serial configuration cable (which came with the cooling unit) from an available communications port on your computer to the serial port of the card or device. Make sure no other application is using the computer port.
3. From the **Start** menu, launch the Wizard application.
4. If the cooling unit is not configured, wait for the Wizard to detect it. Otherwise, click **Next >**.
5. Select **Locally (through the serial port)**, and click **Next >**.
6. Enter the system IP, subnet mask, and default gateway for the cooling unit, and click **Next >**.

   On the **Transmit Current Settings Remotely** screen, if you select the **Start a Web browser when finished** check box, the default Web browser connects to the cooling unit after the Wizard transmits the settings.
7. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.

If you selected **Start a Web browser when finished** in step 6, you can now configure other parameters through the Web interface of the device.

How to Export Configuration Settings

Retrieve and Export the .ini File

Summary of the Procedure

An Administrator can retrieve the .ini file of a unit and export it to another unit or to multiple units.

1. Configure one unit to have the settings you want to export.
2. Retrieve the .ini file from that unit.
3. Customize the file to change at least the TCP/IP settings.
4. Use a file transfer protocol supported by the unit to transfer a copy to one or more other units. For a transfer to multiple units, use an SCP or FTP script or the Schneider Electric .ini file utility.

Each receiving unit uses the file to re-configure its own settings and then deletes it.

Contents of the .ini File

The config.ini file you retrieve from the unit contains the following:

- *section headings* and *keywords* (only those supported for the device from which you retrieve the file)*:* Section headings are category names enclosed in brackets ([ ]). Keywords, under each section heading, are labels describing specific unit settings. Each keyword is followed by an equals sign and a value (either the default or a configured value).
- The `override` keyword: With its default value, this keyword prevents the exporting of one or more keywords and their device-specific values, e.g., in the `[NetworkTCP/IP]` section, the default value for `Override` (the MAC address of the cooling unit) blocks the exporting of values for the `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.

Detailed Procedures

Retrieving

To set up and retrieve an .ini file to export:

1. If possible, use the interface of a unit to configure it with the settings to export. Directly editing the .ini file risks introducing errors.
2. To use FTP to retrieve config.ini from the configured unit:
   a. Open a connection to the unit, using its IP address:

      ```
      ftp> open ip_address
      ```

   b. Log on using the Administrator user name and password.
   c. Retrieve the config.ini file containing the unit settings:

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

   The file is written to the folder from which you launched FTP.

To retrieve configuration settings from multiple Units and export them to other units, see Knowledge Base article FA156117 at http://www.apc.com/support.

Customizing

You must customize the file before you export it.

1. Use a text editor to customize the file.
   - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   - Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
   - Enclose in quotation marks any values that contain leading or trailing spaces or are already enclosed in quotation marks.
   - To export scheduled events, configure the values directly in the .ini file.
   - To export a system time with the greatest accuracy, if the receiving cooling units can access a Network Time Protocol server, configure enabled for `NTPEnable`:

     `NTPEnable=enabled`

     Alternatively, reduce transmission time by exporting the `[SystemDate/Time]` section as a separate .ini file.
   - To add comments, start each comment line with a semicolon (;).
2. Copy the customized file to another file name in the same folder:
   - The file name can have up to 64 characters and must have the .ini suffix.
   - Retain the original customized file for future use.

     IMPORTANT: The file that you retain is the only record of your comments.

Transfer the File to a Single Unit

To transfer the .ini file to another unit, do either of the following:

- From the Web user interface of the receiving unit, select the **Main > Configuration > General > User Config File**. Enter the full path of the file, or use **Browse**.
- Use any file transfer protocol supported by units, i.e., FTP, FTP Client, SCP, or TFTP). The following example uses FTP:
  1. From the folder containing the copy of the customized .ini file, use FTP to log in to the unit to which you are exporting the .ini file:

     `ftp> open ip address`
  2. Export the copy of the customized .ini file to the root directory of the receiving unit:

     `ftp> put filename.ini`

Export the File to Multiple Units

To export the .ini file to multiple units:

- Use SCP or FTP, but write a script that incorporates and repeats the steps used for exporting the file to a single unit.
- Use a batch processing file and the Schneider Electric .ini file utility.

The Upload Event and Error Message

The Event and Its Error Messages

The following event occurs when the receiving cooling unit completes using the .ini file to update its settings:

`Configuration file upload complete, with` *`number`* `valid values`

If a keyword, section name, or value is invalid, the upload by the receiving unit succeeds, and additional event text states the error.

Event Text	Description
Configuration file warning: Invalid keyword on line *number*. Configuration file warning: Invalid value on line *number*.	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line *number.*	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line *number*.	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, an incomplete upload occurs. Reduce the size of the file, or divide it into two files, and try uploading again.

Messages in config.ini

A device associated with the cooling unit from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the device is not present or, for another reason, is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values.

If you did not intend to export the configuration of the device as part of the .ini file import, ignore these messages.

Errors Generated by Overridden Values

The `Override` keyword and its value will generate error messages in the event log when it blocks the exporting of values.

See Contents of the .ini File, page 74 for information about which values are overridden.

Because the overridden values are device-specific and not appropriate to export to other cooling units, ignore these error messages. To prevent these error messages, you can delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Related Topics

On Windows operating systems, instead of transferring .ini files, you can use the Device IP Configuration Wizard to update the basic TCP/IP settings of units and configure other settings through their user interface.

See Device IP Configuration Wizard, page 72.

Command Line Interface (CLI)

The Command Line Interface (CLI) can be used to view the status of and configure and manage the unit. In addition, the CLI allows for creating scripts for automated operation. All parameters of the unit (including those for which there are not specific CLI commands) can be configured by using the CLI to transfer an INI file to the unit. The CLI uses XMODEM to perform the transfer, however, the current INI file cannot be read through XMODEM.

How to Log On

To access the command line interface, use a local serial connection or a remote connection (Telnet or SSH. Only SSH is enabled by default) with a computer on the same network as the Network Management Card (NMC). Use case-sensitive user name and password entries to log on (by default, User name: `apc` and Password: `apc` for a Super User). The default user name for device users is `device`. A Read-Only User cannot access the command line interface.

NOTE: You will be prompted to enter a new password the first time you connect to the NMC with the super user account. New password requires the following:

- shall not be the same as the old password
- shall be at least 8 characters in length
- shall not appear in list of known passwords

Security Lockout: If a valid user name is used with an invalid password consecutively for the number of times specified in the NMC web interface under **Configuration > Security > Local Users > Default Settings**, the user account will be locked for one hour or until the super user or an Administrator-level account unlocks the account.

Remote Access to the Command Line Interface (CLI)

You can access the command line interface through Telnet or SSH. Only SSH is enabled by default. To enable or disable these access methods, use the Web interface. On the **Configuration** menu, select **Network > Console > Access**. You can also enable or disable Telnet or SSH access through the command line interface. For more information, see console, page 90.

SSH for high-security access. If you use the high security of SSL/TLS for the Web interface, use 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. Enabling SSH also enables SCP (Secure Copy), for secure file transfer.

Telnet for basic access. 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:

1. From a computer that has access to the network on which the NMC is installed, at a command prompt, type telnet and the IP address for the NMC (for example, telnet 139.225.6.133, when the NMC uses the default Telnet port of 23), and press ENTER.

   NOTE: This example works for command prompt based Telnet clients. The commands may differ for different Telnet clients.

   If the NMC uses a non-default port number (from 5000 to 32768), you must include a colon or a space, depending on your Telnet client, between the IP address (or DNS name) and the port number. (These are commands for general usage: some clients don't allow you to specify the port as an argument and some types of Linux might want extra commands).

2. Enter the user name and password. NOTE: You will be prompted to enter a new password the first time you connect to the NMC with the

Super User account.

1. Use the following example command to use SSH to access the NMC: ssh -c aes256-ctr apc@156.205.14.141 NOTE: This SSH command is for OpenSSH. The command may differ depending on the SSH tool used.
2. Enter the user name and password.

   NOTE: You will be prompted to enter a new password the first time you connect to the NMC with the Super User account.

1. Use these three commands to configure network settings (text in *italics* indicates a variable):

   a. `tcpip -i` *yourIPaddress*

   b. `tcpip -s` *yourSubnetMask*

   c. `tcpip -g` *yourDefaultGateway*

   For each variable, enter a numeric value with the format xxx.xxx.xxx.xxx.

   For example, to set a system IP address of 156.205.14.141, enter the following command and press **ENTER**:

   `tcpip -i 156.205.14.141`

2. Type `reboot`. The Network Management Card restarts to apply the changes.

Local Access to the Command Line Interface (CLI)

It is possible to use a computer connected to the serial port on the front of the display to access the CLI.

1. Select a serial port on the local computer and disable any service that uses that port.
2. Use the provided serial cable to connect the selected serial port to the serial on the front of the display.
3. Run a terminal program (such as HyperTerminal®, TeraTerm, or PuTTY) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Save the changes.
5. Press **ENTER**, repeatedly if necessary, to display the **User Name** prompt.
6. Enter the user name and password.

   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.

Main Screen

Sample Main Screen

Following is an example of the screen displayed when you log on to the command line interface at the Network Management Card (NMC).

```
 Schneider Electric                                Network Management Card AOS          v3.3.0.6
 (c)Copyright 2025 All Rights Reserved  ACRC2g APP                                      v3.3.0.1
 ------------------------------------------------------------------------
 Name   : apc9E1C7B                                    Date : 06/17/2025
 Contact  : Unknown                                    Time : 17: 53: 58
 Location : Unknown                                    User : Super User
 Up Time  : 0 Days  2 Hours  24 Minutes                Stat : P+N4+ N6+ A+
 ------------------------------------------------------------------------
 IPv4               : Enabled      IPv6                        : Enabled
 Ping Response      : Enabled
 ------------------------------------------------------------------------
 HTTP               : Disabled     HTTPS                       : Enabled
 FTP                : Enabled      Telnet                      : Disabled
 SSH/SCP            : Enabled      SNMPv1                      : Disabled
 SNMPv3             : Disabled

 ------------------------------------------------------------------------
 Super User         : Enabled      RADIUS                      : Disabled
 User Authentication      : Local
 Administrator      : Disabled     Device User                 : Disabled
 Read-Only User     : Disabled     Network-Only User           : Disabled
 ------------------------------------------------------------------------
 Type ? for command listing
 Use tcpip command for IP address(-i), subnet(-s), and gateway(-g)
 apc>
```

Main Screen Information Fields

- Two fields identify the American Power Conversion operating system (AOS) and application (APP) firmware versions. The application firmware name identifies the device that connects to the networkthrough this NMC. In the example above, the NMC uses the application firmware for a Unit.
  `Network Management Card AOS vx.x.x.x`
  `ACRC2g APP vx.x.x.x`

- Three fields identify the system name, contact person, and location of the NMC.
  ```
  Name : apc9E1C7B
  Contact : Unknown
  Location : Unknown
  ```
- The **Up Time** field reports how long the NMC management interface has been running since it was last turned on or reset.
  ```
  Up Time : 0 Days 2 Hours 24 Minutes
  ```
- Two fields report when you logged in, by date and time.
  ```
  Date : 06/17/2025
  Time : 17:53:58
  ```
- The **User** field reports whether you logged in through the **Super User**, **Administrator**, **Device Manager**, **Network-Only** or **Read-Only** account. When you log on as Device Manager (equivalent to Device User in the user interface), you can access the event log, configure some Unit settings, and view the number of active alarms.
  ```
  User : Super User
  ```

Main Screen Status Fields

- The Stat field reports the NMC status. The middle status varies according to whether you are running IPv4, IPv6, or both, as indicated in the second table below. Stat : P+ N4+ N6+ A+
  ```
  Stat : P+ N4+ N6+ A+
  ```

P+	The operating system (AOS) is functioning properly.

IPv4 only	IPv6 only	IPv4 and IPv6*	Description
N+	N6+	N4+ N6+	The network is functioning properly,
N?	N6?	N4? N6?	A DHCP or BOOTP request cycle is in progress.
N-	N6-	N4- N6-	The NMC did not connect to the network.
N!	N6!	N4! N6!	Another device is using the IP address of the NMC.

* The N4 and N6 values can be different from one another, you could, for example, have N4-N6 +.

A+	The application is functioning properly.
A-	The application has a bad checksum.
A?	The application is initializing.
A!	The application is not compatible with AOS.

How to Use the CLI

At the command line interface, use commands to view and configure settings for the appliance. To use a command, type the command, option (if applicable), and any applicable arguments, then press ENTER. Commands and arguments are valid in lowercase, uppercase, or mixed case. Options are case sensitive.

While using the CLI, it is also possible to do the following:

- Type ? and press ENTER to view a list of available commands, based on the account type.

- To obtain information about the purpose and syntax of a specified command, type the command, a space, and `?` or the word `help`. For example, to view RADIUS configuration options, type

  `radius ?`

  or

  `radius help`

  NOTE: See Command Help Syntax, page 82 for more detailed information.
- Press the UP arrow key to view the command that was entered most recently in the session. Use the UP and DOWN arrow keys to scroll through a list of up to ten previous commands.
- Type at least one letter of a command and press the TAB key to scroll through a list of valid commands that match the text typed in the command line.
- Type `exit`, `quit`, or `bye` to close the connection to the CLI.

Command Help Syntax

When using ? or help to obtain information about a specific command, the following syntax defines how that command can be used:

Item	Description
-	Options are preceded by a hyphen.
[...]	If a command accepts multiple options or an option accepts mutually exclusive arguments, the values may be enclosed in brackets.
<...>	Definitions of options are enclosed in angle brackets. For example: `-dp <device password>`
|	A vertical line between items enclosed in brackets or angle brackets indicates that the items are mutually exclusive. One of the items must be used.

Example of a command that supports multiple options:

`ftp [-p <port number>] [-S <enable | disable>]`

In this example, the ftp command accepts the option `-p`, which defines the port number, and the option `-S`, which enables or disables the FTP feature.

To change the FTP port number to 5010, and enable FTP:

1. Type the ftp command, the port option, and the argument 5010:

   `ftp -p 5010`
2. After the first command succeeds, type the ftp command, the enable/disable option, and the enable selection:

   `ftp -S enable`

Example of a command that accepts mutually exclusive arguments for an option:

`alarmcount -p [all | warning | critical]`

In this example, the option `-p` accepts only three arguments: `all`, `warning`, or `critical`. For example, to view the number of active critical alarms, type: `alarmcount -p critical`

The command will fail if typing an argument that is not specified.

Command Response Codes

The command response codes enable scripted operations to detect error conditions reliably without having to match error message text. All CLI commands issue:

```
E [0-9] [0-9] [0-9]: Error message
```

Code	Message
E000	Success
E001	Successfully Issued
E002	Success, Reboot Required
E100	Command Failed
E101	Command Not Found
E102	Parameter Error
E103	Command Line Error
E107	Serial communication with the Rack PDU has been lost
E108	EAPoL disabled due to invalid/encrypted certificate

Argument Quoting

Argument values may optionally be enclosed in double quote characters (ASCII 0x22). String values beginning or ending with spaces, or containing commas or semicolons, must be enclosed in quotes for both input and output. Quote and backslash ("\", decimal code 92) characters appearing inside strings should NOT be encoded using traditional escape sequences (see Escape Sequences below).

All binary characters (ASCII decimal ranges 0..31, 127..159) that appear inside strings are treated as unreadable characters and rejected. When a quote or backslash character is supplied as a part of an input string, the input string must be enclosed in double quotes.

Escape Sequences

Escape sequences, traditionally a backslash followed by a lower case letter or by a combination of digits, are ignored and should not be used to encode binary data or other special characters and character combinations.

The result of each escape sequence is parsed as if it were both a backslash and the traditionally escaped character.

Example: `<command> <arg1> [<agr2> <arg3a | arg3b> [<arg4a | arg4b | arg4c>]]`

- arg1 must be used, but arg2 - 4 are optional.
- If arg2 is used, then arg3a or arg3b must also be used.
- arg4 is optional, but arg1 - 3 must precede arg4.

With most commands, if the last argument is omitted, the command provides information, otherwise the last argument is used to change/set new information.

Example:

```
apc>ftp -p (displays the port number when omitting the arg2)

E000: Success
FTP Port: 5001

apc>ftp -p 21 (sets the port number to arg2)
E000: Success
```

Prompts for User Input during Command Execution

Certain commands require additional user input (ex. transfer .ini prompting for baud rate). There is a fixed timeout of 1 minute for such prompts. If any text is entered within the timeout period, then the command prints `E100: Command Failed.` and the command prompt is redisplayed.

Delimiter

The CLI uses `<space> (ASCII 0x20)` as the delimiter between commands and arguments. Extra white space between commands and arguments is ignored.

Command responses have all fields delimited with commas for efficient parsing.

Option and Argument Inputs

Entering a command with no options or arguments returns the current value of all options available from that command.

Entering the command and an option with no arguments returns the current value of that option only.

Any command followed by a question mark `?` returns help explaining the command.

`<space>` `::` = (" " | multiple" ")

`<valid letter_number>` `::`= (a-z | A-Z | 0-9)

`<string>` `::` = (1 - 64 consecutive printable valid ASCII characters [ranging from hex 0x20 to 0x7E inclusive])

> **NOTE:** If the string includes a blank, the entire string MUST be surrounded by quotes(" ").

`<option>` `::` = "-"(<valid letter_number> | <valid letter_number><valid letter_number>)

`<argument>` `::=` `<helpArg>` | `<alarmcountArg>` | `<bootArg>` | `<cdArg>` | `<consoleArg>` | `<dateArg>` | `<deleteArg>` | `<ftpArg>` | `<pingArg>` | `<portspeedArg>` | `<promptArg>` | `<radiusArg>` | `<resettodefArg>` | `<systemArg>` | `<tcpipArg>` | `<userArg>` | `<webArg>` | `<string>`

`<optionArg>` ::= <option><argument>

Network Management Card Command Descriptions

? or help

Access: Super User, Administrator, Device User, Read Only User

Description: View a list of all the CLI commands available to the user account type. To view help text for a specific command, type the command followed by a question mark.

Parameters: [<command>]

Example 1:

```
apc> ?
  System Commands:
  ------------------------------------------------------------
  For command help: command ?
  ?            about        alarmcount   boot         bye          cd
  clrrst       console      date         delete       dir          dns
  eapol        email        eventlog     exit         firewall     format
  ftp          help         lang         lastrst      ldap         ledblink
  logzip       netstat      ntp          ping         portspeed    prompt
  pwd          quit         radius       reboot       resetToDef   session
  smtp         snmp         snmptrap     snmpv3       ssh          ssl
  system       tacacs+      tcpip        tcpip6       user         userauth
  userdflt     web          whoami       wifi         xferINI      xferStatus
  Device Commands:
  ------------------------------------------------------------
  acrc
```

Example 2:

```
apc> help boot
Usage: boot - - Configuraiton Options
  boot     [-b <dhcpBootp | dhcp | bootp | manual>] (IPv4 Boot Mode)
           [-c <enable | disable>] (Require DHCPv4 Cookie)
           [-v <vendor class>]
           [-i <client id>]
           [-u <user class>]
```

Error Message: E000, E102

about

Access: Super User, Administrator, Device User, Read Only User

Description: Displays system information (Model Number, Serial Number, Manufacture Dates, etc.)

Parameters: None.

Example:

```
apc> about

E000: Success
Hardware Factory
- - - - - - - -
Model Number:                   0N-1591
Serial Number:                  MB2427000654
Hardware Revision:              05
Manufacture Date:               07/06/2024
MAC Address:                    28 29 86 9E 1C 7B
Management Uptime:              0 Days 2 Hours 25 Minutes

Application Module
- - - - - - - -
Name:                           acrc2g
Version:                        v3.3.0.1
Date:                           Apr 16 2025
Time:                           11:17:26

APC OS (AOS)
- - - - - - - -
Name:                           aos
Version:                        v3.3.0.6
Date:                           Apr 16 2025
Time:                           11:15:41

APC Boot Monitor
- - - - - - - -
Name:                           boot
Version:                        v1.5.4.1
Date:                           Jun 4 2024
Time:                           16:20:19

Cooling
- - - - - - - -
Model:                          InRow ACRC301H
Firmware Revision:              2.49.0
Serial Number:                  - - -
```

Error Message: `E000`

alarmcount

Access: Super User, Administrator, Device User, Read Only User

Description: Displays alarms present in the system.

Parameters:

Option	Argument	Description
-p	all	View the number of active alarms reported by the . Information about the alarms is provided in the event log.
	warning	View the number of active warning alarms.
	critical	View the number of active critical alarms.

Example: To view the number of active informational alarms:

```
apc> alarmcount
E000: Success
AlarmCount: 4

apc> alarmcount -p warning
E000: Success
WarningAlarmCount: 4

apc> alarmcount -p critical
E000: Success
CriticalAlarmCount: 0

apc> alarmcount -p informational
E000: Success
InformationalAlarmCount: 0
```

Error Message: E000, E102

boot

Access: Super User, Administrator

Description: View or set the network startup configuration of the device, such as setting boot mode (DHCP vs BOOTP vs MANUAL).

Parameters:

Option	Argument	Description
-b <boot mode>	dhcp | bootp | manual	Define how the TCP/IP settings will be configured when the power turns on, resets, or restarts. for information about each boot mode setting.
-c	[<enable | disable>] (Require DHCP Cookie)	dhcp boot mode only. Enable or disable the requirement that the DHCP server provide the APC cookie.
-v	[<vendor class>]	Vendor Class is APC.
-i	[<client id>]	The MAC address of the ’s NMC, which uniquely identifies it on the network.
-u	[<user class>]	The name of the application firmware module.

Example:

```
apc> boot

E000: Success

Boot Mode:          manual

Vendor Class:       APC

Client ID:          28 29 86 9E 1C 7B

User Class:         ACRC2G
```

Error Message: E000, E102

bye, exit, or quit

Access: Super User, Administrator, Device User, Read Only User

Description: Exit the CLI.

Parameters: None.

Example 1:
```
apc> bye
Bye
```
Example 2:
```
apc> exit
Bye
```
Example 3:
```
apc> quit
Bye
```

Error Message: None.

cd

Access: Super User, Administrator, Device User, Read Only User

Description: Allows the user to set the working directory of the file system. The working directory is set back to the root directory '/' when the user logs out of the CLI.

Parameters: <directory name>

Example:

```
apc> cd logs
E000: Success

apc> cd /
E000: Success
```

Error Message: E000, E102

clrrst

Access: Super User, Administrator

Description: Clear reset reason.

Parameters: None.

Example:

```
apc> clrrst
E000: Success
```

Error Message: E000

console

Access: Super User, Administrator

Description: Define whether users can access the CLI using Telnet, which is enabled by default, or Secure SHell (SSH), which provides protection by transmitting user names, passwords, and data in encrypted form. The Telnet or SSH port setting can be changed for additional security. Alternately, disable network access to the CLI.

Parameters:

Option	Argument	Description
-s	<enable | disable> (ssh)	Enable or disable access to the CLI through SSH. Enabling SSH enables SCP.
-t	<enable | disable> (telnet)	Disable or enable access to the CLI through Telnet.
-pt	<telnet port n>	Define the Telnet port used to communicate with the (23 by default). The other range is 5000–32768.
-ps	<SSH port n>	Define the SSH port used to communicate with the (22 by default). The other range is 5000–32768.
-b	2400 | 9600 | 19200 | 38400 | 57600 | 115200	Configure the speed of the serial port connection (9600 bps by default).

Example 1: To enable SSH access to the CLI, type

```
apc> console -s enable
E002: Success
Reboot required for change to take effect.
```

Example 2: To change the Telnet port to 5000, type

```
apc> console -pt 5000
E000: Success
Reboot required for change to take effect.
```

Error Message: E000, E102

date

Access: Super User, Administrator

Description: Get and set the date and time of the system. .

Parameters:

Option	Argument	Description
-d	<"datestring">	Set the current date. The format must match the current -f setting.
-t	<00:00:00>	Configure the current time, in hours, minutes, and seconds. Use the 24-hour clock format.
-f	<mm/dd/yy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd>	Select the numerical format in which to display all dates in this user interface. Each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.
-z	<time zone offset>	Set the difference with Greenwich Mean Time (GMT) in order to specify the time zone needed. This allows the synchronization with other people in different time zones.

Example 1: To display the date using the format yyyy-mm-dd, type

```
apc> date -f yyyy-mm-dd
E000: Success
* Reboot required for change to take effect
```

Example 2: To define the date as Jun 17, 2025, type

```
apc> date -d "2025-06-17"
E000: Success
* Reboot required for change to take effect
```

Example 3: To define the time as 5:21:03 p.m., type

```
apc> date -t 17:21:03
E000: Success
* Reboot required for change to take effect
```

Error Message: E000, E100, E102

delete

Access: Super User, Administrator

Description: Delete a file in the file system.

Parameters:

Argument	Description
<file name>	Type the name of the file to delete.

Example:

```
apc> delete /event.txt
E000: Success
```

Error Message: E000, E102

dir

Access: Super User, Administrator, Device User, Read Only User

Description: Displays the content of the working directory.

Parameters: None.

Example:

```
apc> dir

E000: Success

6661028 Apr 16 11:15   apc_hw21_aos_3.3.0.6.bin

6662052 Apr 16 11:17       apc_hw21_acrc2g_3.3.0.1.bin

45000 Jun 17 17:58
config.ini
0 Jun 10 19:21                      config.ini

0 Jun 10 19:21                          db/

0 Jun 10 19:21                          ssl/

0 Jun 10 19:21                          ssh/

0 Jun 10 19:21                         logs/

0 Jun 10 19:21                          sec/

0 Jun 10 19:21                          fwl/

0 Jun 10 19:21                        certs/
```

Error Message: `E000`

dns

Access: Super User, Administrator

Description: Configure the manual Domain Name System (DNS) settings.

Parameters:

Option	Argument	Description
-OM	<enable | disable>	Override the manual DNS.
-p	<primary DNS server>	Set the primary DNS server.
-s	<secondary DNS server>	Set the secondary DNS server.
-d	<domain name>	Set the domain name.
-n	<domain name IPv6>	Set the domain name IPv6.
-h	<host name>	Set the host name.
-y	<enable | disable>	Synchronizes the system and the hostname. This is the same as using “system -s”.

Example:

```
apc> dns -h myHostName
E000: Success
```

Error Message: E000, E102

eapol

Access: Super User, Administrator

Description: Configure EAPoL (802.1X Security) settings..

Parameters:

Option	Argument	Description
-s	<enable | disable>	Enable or disable EAPoL.
-n	<supplicant name>	Set the supplicant name.
-c	<certificate filename>	The name of the file that contains the end-entity device certificate to use for EAPoL authentication..
-r		Restart authentication using current settings.

Example:

```
apc>eapol

E000: Success

Active EAPoL Settings

-----------------------
Status:              disabled

Supplicant Name:     NMC-Supplicant-28:29:86:9E:1C:7B
Certificate:         nmc.pem
Certificate status:  loaded
```

Error Message: None

email

Access: Super User, Administrator

Description: Configure email parameters.

Parameters:

Option	Argument	Description
-g[n]	<enable | disable> (Generation)	Enables (default) or disables sending email to the recipient.
-t[n]	<To Address>	The e-mail address of the recipient.
-o[n]	<long | short> (Format)	The long format contains name, location, contact, IP address, serial number of the device, date and time, event code, and event description. The short format provides only the event description.
-l[n]	<Language Code>	The language in which the emails will be sent. This is dependent on the installed language pack.
-r[n]	<Local | recipient | custom> (Route)	Set the SMTP Server options: • **Local** (recommended): Choose this option if your SMTP server is located on your internal network, or is set up for your e-mail domain. Choose this setting to limit delays and network outages. If you choose this setting, you must also enable forwarding at the SMTP server of the device, and set up a special external e-mail account to receive the forwarded e-mail. **NOTE:** Check with your SMTP server administrator before making these changes. • **Recipient**: This setting sends email directly to the recipient's SMTP server, which is determined by an MX record lookup of the domain of the To: Address. The device tries only once to send the e-mail. A network outage or a busy remote SMTP server can cause a timeout and cause the e-mail to be lost. This setting requires no additional administrative tasks on the SMTP server. **NOTE:** When using this setting, the “From Address” will match the “To Address”, authentication and encryption (TLS) will be disabled, and port 25 will be used. • **Custom**: This setting allows each email recipient to have its own server settings. These settings are independent of the settings given by the smtp command.
-f[n]	<From Address>	The address from which email will be sent by the NMC.
-s{n}	<SMTP Server>	The IPv4/IPv6 address or DNS name of the local SMTP server.
-p[n]	<Port>	The SMTP port number, default is 25. Common ports are 25 for unencrypted e-mail, and 465 and 587 for SSL/TLS encrypted e-mail. You can change the port setting to any port from 1 to 65535.
-a[n]	<enable | disable> (Authentication)	Enable this if your SMTP server requires authentication.
-u[n]	<User Name>	If the SMTP server requires authentication, type the user name and password here.
-w[n]	<Password>	
-e[n]	<none | ifsupported | always | implicit> (Encryption)	Encryption options: • **none**: The SMTP server does not require/ support encryption. • **ifsupported**: The SMTP server advertises support for STARTTLS but does not require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given. This is typically used with port 25.

Option	Argument	Description
		• **always**: The SMTP server requires the STARTTLS command to be sent upon connection to the server. This is typically used with port 587. • **implicit**: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server. This is typically used with port 465.
`-c[n]`	`<enable | disable > (Required Certificate)`	Require CA Root Certificate: This should be enabled if the security policy of your organization does not allow for implicit trust of SSL/TLS connections. If this is enabled, a valid CA certificate for the SMTP server must be installed to the NMC's certificate store using the certificate loader for a TLS connection with the SMTP server to succeed. See the User Guide for more information about loading TLS certificates.
`n=`	`Email Recipient Number (1,2,3, or 4)`	Specifies the recipient of the e-mail, identified by the recipient number.

Example: To enable email to be sent to email recipient 1 with email address recipient1@apc.com, using the local SMTP server, type:

```
email -g1 enable -r1 local -t1 recipient1@apc.com
```

eventlog

Access: Super User, Administrator, Device User, Read Only User

Description: View the date and time in which the event log was retrieved. View the status of the , and the status of sensors connected to the . View the most recent device events and the date and time they occurred.

Parameters: Use the following keys to navigate the event log:

Key	Description
Esc	Close the event log and return to the CLI.
Enter	Update the log display. Use this command to view events that were recorded after the last time the log was retrieved and displayed.
Spacebar	View the next page of the event log.
B	View the preceding page of the event log. This command is not available at the main page of the event log.
D	Delete the event log. Follow the prompts to confirm or deny the deletion. Deleted events cannot be retrieved.

Example:

```
apc> eventlog

E000: Success

---- Event Log -------------------------------------------------------

   Date: 06/     Time:
   17/2025       19:28:-
                 32
   ------------------------------------

   Date          Time      User      Event

   ------------------------------------------------------------------------
   --
   06/17/2025    19:28:-   apc       Configuration change. Email recipient 2
                 09                  format. Value: Short
   06/17/2025    19:27:-   System    System Network service started. IPv6
                 46                  address
                                     FE80::DDF3:F873:275E:5AD8 assigned by
                                     link-local autoconfiguration.
   06/17/2025    19:27:-   System    Network service stopped.
                 41
   06/17/2025    19:21:-   apc       File data.txt deleted via CLI
                 03                  Successful
   06/17/2025    19:21:-   apc       Data Log cleared.
                 03
   06/17/2025    19:20:-   apc       CLI user 'apc' logged in from serial
                 41                  port.
   06/17/2025    19:19:-   Device    ACRC301H: Circulation Pump Needs
                 37                  Service.
   06/17/2025    19:19:-   Device    Device ACRC301H: Unexpected Number of
                 37                  Rack Inlet
                                     emperature Sensors Present.
 <ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

Error Message: E000, E100

exit

See bye, exit, or quit, page 89.

firewall

Access: Super User, Administrator

Description: Establishes a barrier between a trusted, secure internal network and another network.

Parameters:

Option	Argument	Description
-S	<enable | disable>	Enable or disable the Firewall.
-f	<file name to activate>	Name of the firewall to activate.
-t	<file name to test> <duration time in minutes>	Name of firewall to test and duration time in minutes.
-fe	No argument. List only	Shows active file errors.
-te	No argument. List only	Shows test file errors.
-c	No argument. List only	Cancel a firewall test.
-r	No argument. List only	Shows active firewall rules.
-l	No argument. List only	Shows firewall activity log.
-Y	No argument.	Skip firewall test prompt.

Example:

```
apc> firewall
E000: Success
Firewall:    disabled
File name:   example.fwl
```

Error Message: E000, E102

format

Access: Super User, Administrator

Description: Format the flash file system. This deletes all configuration data (including network settings), event and data logs, certificates and keys.

NOTE: The user must confirm by entering “YES” when prompted.

Parameters: None.

Example:

```
apc> format
Format FLASH file system


Warning: This will delete all configuration data,
event and data logs, certs and keys.
Note: Network configuration settings WILL NOT be preserved. You may preserve
them by passing the –p flag.
Enter 'YES' to continue or <ENTER> to cancel:
```

Error Message: None.

ftp

Access: Super User, Administrator

Description: Get/set the ftp configuration data.

NOTE: The system will reboot if any configuration is changed.

Parameters:

Option	Argument	Description
-p	<port number> (21 and 5000-32768)	Define the TCP/IP port that the FTP server uses to communicate with the (21 by default). The FTP server uses both the specified port and the port one number lower than the specified port. Valid port numbers are 21 and 5000–32768.
-S	<enable | disable>	Configure access to the FTP server.

Example:

```
apc> ftp -p 5001
E000: Success

apc> ftp
E000: Success
Service:        Enabled
Ftp Port:       5001

apc> ftp -p 21
E000: Success
```

Error Message: E000, E102

help

Access: Super User, Administrator, Device User, Read Only User

Description: View a list of all the CLI commands available to the user account type. To view help text for a specific command, type the command followed by a question mark.

Parameters: [<command>]

Example 1:

```
apc> ?

  System Commands:
  ------------------------------------------------------------
  For command help: command ?
  ?            about        alarmcount   boot         bye          cd
  clrrst       console      date         delete       dir          dns
  eapol        email        eventlog     exit         firewall     format
  ftp          help         lang         lastrst      ldap         ledblink
  logzip       netstat      ntp          ping         portspeed    prompt
  pwd          quit         radius       reboot       resetToDef   session
  smtp         snmp         snmptrap     snmpv3       ssh          ssl
  system       tacacs+      tcpip        tcpip6       user         userauth
  userdflt     web          whoami       wifi         xferINI      xferStatus
  Device Commands:
  ------------------------------------------------------------
  acrc
```

Example 2:

```
apc> help boot

Usage: boot - - Configuraiton Options

  boot      [-b <dhcpBootp | dhcp | bootp | manual>] (IPv4 Boot Mode)
            [-c <enable | disable>] (Require DHCPv4 Cookie)
            [-v <vendor class>]
            [-i <client id>]
            [-u <user class>]
```

Error Message: E000, E102

lang

Access: Super User, Administrator, Device User, Read Only User

Description: Displays the language in use.

Parameters: None.

Example:

```
apc> lang
E000: Success
Languages
enUs - English
```

Error Message: `E000`

lastrst

Access: Super User, Administrator

Description: Last network interface reset reason. Use the output of this command to troubleshoot network interface issues with the guidance of technical support.

Argument	Definition
`02 NMI Reset`	The network interface was reset via the Reset button on the NMC faceplate.
`09 Coldstart Reset`	The network interface was reset by removing power from the hardware.
`12 WDT Reset`	The network interface was reset via a firmware command.

Example:

```
apc> lastrst
12 WDT Reset
E000: Success
```

Error Message: `E000, E102`

ldap

Access: Super User, Administrator, Network-Only User

Description: View and configure LDAP settings. You can set up the device to use an LDAP server to authenticate remote users. Two common examples of this are Microsoft Active Directory and OpenLDAP. Authentication is always performed using a simple bind request over a TLS connection. Ensure that the LDAP server's CA certificate is installed in order for the TLS connection to the LDAP server to complete.

For more information to use LDAP, see the User Guide.

Option	Argument	Definition
`–s`	`<Search User URI>`	• **ldaps://ldap.domain.com** “ldap.domain.com” at port 636 is connected to and a TLS handshake is immediately performed without sending a StartTLS request. If this succeeds, then an anonymous bind is performed. From here a search for the user logging in is performed.

		• **ldap://ldap.domain.com:42/ CN=searchuser,OU=users,DC=domain,DC=com** This is the same as the first example except that if the SRV record is not found then “ldap.domain.com” at port 42 is connected to.
–p	<Search User Password>	The password to use in the initial bind request to the search user as described above. If left blank, then either an anonymous or unauthenticated bind is performed depending on whether or not a search user DN is provided.
–t	<2-60>	The timeout in seconds to use when connecting to and communicating with the LDAP server. The initial TCP connection must complete within this amount of time. If it does, then each LDAP response from the server must be received within this amount of time following each LDAP request. Because a single LDAP authentication can consist of multiple requests (and even to multiple servers if referrals are chased), the overall authentication time may end up being much longer than the timeout value specified here.
–u	<Users Base DN>	This is the DN of the base object entry under which all users who login must exist.
–g	<Groups Base DN>	This is the DN of the base object entry under which the user groups specified in the following settings must exist.
-ag	<Admins Group Name>	This is the common name (CN) of the LDAP group to which NMC Administrators are members of. If the user logging in is a member of this group, then the user is granted Administrator access.
-dg	<Device Users Group Name>	This is the common name (CN) of the LDAP group to which NMC Device Users are members of. If the user logging in is a member of this group, then the user is granted Device User access.
–ng	<Network Users Group Name>	This is the common name (CN) of the LDAP group to which NMC Network Users are members of. If the user logging in is a member of this group, then the user is granted Network User access.
–rg	<Read Only Users Group Name>	This is the common name (CN) of the LDAP group to which NMC Read Only Users are members of. If the user logging in is a member of this group, then the user is granted Read Only User access.
–ad	<enable | disable>	If this is enabled, then LDAP directories containing users of the “User” class and groups of the “Group” class following the standard Active Directory schema will be supported.
-posix	<enable | disable>	If this is enabled, then LDAP directories containing users of the “posixAccount” class and groups of the “posixGroup” class following the schema defined in RFC 2307 will be supported.
-4519	<enable | disable>	If this is enabled, then LDAP directories containing users of the “uidObject” class and groups of either the “groupOfNames” class or the “groupOfUniqueNames” class following the schema defined in RFC 4519 will be supported.
-2798	<enable | disable>	If this is enabled, then LDAP directories containing users of the “inetOrgPerson” class as defined in RFC 2798 will be supported.
-cuser	<enable | disable>	If this is enabled, then LDAP directories containing users of classes that do not conform to any of the supported classes above can be supported. When this is enabled, the settings –ucn (Custom User Class Name) and –ucua (Custom User Username Attr) must be provided, and – ucga (Custom User Group Number Attr) may optionally be provided.
-cgro-up	<enable | disable>	If this is enabled, then LDAP directories containing groups of classes that do not conform to any of the supported classes above can be supported. When this is enabled, the settings –gcn (Custom Group Class Name) and – gcma (Custom Group Member Attr) must be provided, and –gcga (Custom Group Group Number Attr) may optionally be provided. –gcmt (Custom Group Member Type) must also be set correctly.
-ucn	<Custom User Class Name>	This is the name of the object class that user entries belong to. It is only used when –cuser (Custom User Class) is enabled.
-ucua	<Custom User Username Attr>	This is the name of the attribute that contains a user's username for the object class specified by –ucn (Custom User Class Name). It is only used when –cuser (Custom User Class) is enabled.
-ucga	<Custom User Group Number Attr>	This is the name of the attribute that contains the group number for a user's primary group for the object class specified by –ucn (Custom User Class Name). This is optional, and only used when –

		cuser (Custom User Class is enabled. It is used the same way as the “gidNumber” attribute in the “posixAccount” class.
-gcn	<Custom Group Class Name>	This is the name of the object class that group entries belong to. It is only used when -cgroup (Custom Group Class) is enabled.
-gcma	<Custom Group Member Attr>	This is the name of the attribute that contains the members of the group for the object class specified by -gcn (Custom Group Class Name). It is only used when - cgroup (Custom Group Class) is enabled. When -gcmt (Custom Group Member Type) is set to DN, then the values in this attribute are DNs. When it is set to username, then the values in this attribute are user names.
-gcga	<Custom Group Group Number Attr>	This is the name of the attribute that contains the group number of the group for the object class specified by -gcn (Custom Group Class Name). This is optional, and only used when -cgroup (Custom Group Class) is enabled. It is used the same way as the “gidNumber” attribute in the “posixGroup” class.
-gcmt	<DN | user name>	This specifies how members of the group for the object class specified by -gcn (Custom Group Class Name) are specified. It can be set to either DN or username.

Example 1: To view the existing LDAP settings for the NMC, type:
`ldap`

Example 2: To configure LDAP to connect to an LDAP server using only an Active Directory schema at **ldap.company.com** (or to use the ldap SRV record at company.com if available) with a timeout of five seconds, and bind with an initial user with search privileges at DN cn=admin, dc=company, dc=com with password “password”, with NMC administrators in the nmc-admins group, NMC read-only users in the nmc-ro-users group, and network only and device only users disabled, type:
`ldap -s ldap://ldap.company.com/cn=admin,dc=company,dc=com -p password -t 5 -u ou=users,dc=company,dc=com -g ou=groups,dc=company,dc=com -ag nmc-admins -rg nmcro- users -dg “” -ng “” -ad enable -posix disable -4519 disable -2798 disable - cuser disable -cgroup disable`

ledblink

Access: Super User, Administrator

Description: Sets the blink rate to the LED on the .

Parameters:

Argument	Description
<time>	Number of minutes to blink the LED

Example:

```
apc> ledblink 1
E000: Success
```

Error Message: E000, E102

logzip

Access: Super User, Administrator

Description: Places large logs into a zip file before sending.

Parameters:

Option	Argument	Description
-m	<email recipient>	Email recipient number (1–4).

Example:

```
apc> logzip -m 1

Generating files

Compressing files into c:/dbg/debug_ACRC301H_MB2427000654_20250617_
193936.tar
Emailing log files to email recipient - 1

E000: Success
```

Error Message: E000, E102

netstat

Access: Super User, Administrator

Description: Displays incoming and outgoing network connections.

Parameters: None.

Example:

```
apc > netstat

Current IP Information

Family   mHome    Type     IPAddress                          Status
IPv4     4        auto     FE80::DDF3:F873:275E:5AD8/64       configured
IPv6     0        manual   manual ::1/128                     configured
IPv4     0        manual   manual 127.0.0.1/32                configured
```

Error Message: None.

ntp

Access: Super User, Administrator

Description: Synchronizes the time of the Network Interface to the time of the specified NTP server. The time is defined as Coordinated Universal Time (UTC), formerly Greenwich Mean Time. The timezone must be set correctly using the date command. See date, page 91.

Parameters:

Option	Argument	Description
-OM	<enable | disable>	Override the manual settings.
-p	<primary NTP server>	Specify the primary server.
-s	<secondary NTP server>	Specify the secondary server.
-e	<enable | disable>	Enables or disables the use of NTP.
-u	<update now>	Immediately updates the NMC time from the NTP server.

Example 1: To enable the override of manual setting, type

```
apc> ntp -OM enable
E000: Success
```

Example 2: To specify the primary NTP server, type

```
apc> ntp -p 150.250.6.10
E000: Success
```

Error Message: E000, E102

ping

Access: Super User, Administrator, Device User

Description: Perform a network 'ping' to any external network device.

Parameters:

Argument	Description
<IP address or DNS name>	Type an IP address with the format xxx.xxx.xxx.xxx, or the DNS name configured by the DNS server.

Example:

```
apc> ping 192.168.1.50
E000: Success
Reply from 192.168.1.50: time(ms) = <10
Reply from 192.168.1.50: time(ms) = <10
Reply from 192.168.1.50: time(ms) = <10
Reply from 192.168.1.50: time(ms) = <10
```

Error Message: E000, E100, E102

portSpeed

Access: Super User, Administrator

Description: Get/set the network port speed.

NOTE: The system will reboot if any configuration is changed.

Parameters:

Option	Argument	Description
-s	<auto | 10H | 10F | 100H | 100 F>	Define the communication speed of the Ethernet port. The auto command lets the Ethernet devices negotiate to transmit at the highest possible speed. See Port Speed, page 23 for more information about the port speed settings.
H = Half Duplex		10 = 10 Meg Bits
F = Full Duplex		100 = 100 Meg Bits

Example:

```
apc> portspeed
E000: Success
Port Speed: Auto_negotiation
Current Port Speed: 100 Half_Duplex

apc> portspeed -s 10h
E002: Success
Reboot required for change to take effect.

apc> portspeed -s auto
E002: Success
Reboot required for change to take effect.
```

Error Message: E000, E102

prompt

Access: Super User, Administrator, Device User

Description: Change the format of the prompt, either short or long.

Parameters:

Option	Argument	Description
-s	long	The prompt includes the account type of the currently logged-in user.
	short	The default setting. The prompt is four characters long: APC>

Example:

```
apc> prompt -s long
E000: Success

Administrator@apc> prompt -s short
E000: Success
```

Error Message: E000, E102

pwd

Access: Super User, Administrator, Device User, Read Only User

Description: Used to output the path of the current working directory.

Parameters: None.

Example:

```
apc> pwd
/

apc> cd logs
E000: Success

apc> pwd
/logs
```

Error Message: E000, E102

quit

See bye, exit, or quit, page 89.

radius

Access: Super User, Administrator, Network-Only User

Description: View the existing RADIUS settings, enable or disable RADIUS authentication, and configure basic authentication parameters for up to two RADIUS servers.

For a summary of RADIUS server configuration and a list of supported RADIUS servers, see the User Guide.
Additional authentication parameters for RADIUS servers are available at the user interface of the NMC.
For detailed information about configuring your RADIUS server, see the Security Handbook.

Option	Argument	Description
`-p1` `-p2`	`<server IP>`	The server name or IP address of the primary or secondary RADIUS server.
`-o1` `-o2`	`<port>`	The server port of the primary or secondary RADIUS server. **NOTE:** RADIUS servers use port 1812 by default to authenticate users. The NMC supports ports 1 to 65535.
`-s1` `-s2`	`<server secret>`	The shared secret between the primary or secondary RADIUS server and the NMC.
`-t1` `-t2`	`<server timeout>`	The time in seconds that the NMC waits for a response from the primary or secondary RADIUS server.
`-m1` `-m2`		Enabling this setting (disabled by default) will require the NMC to receive a valid Message-Authenticator attribute in the response from the RADIUS server.

Example 1: To view existing RADIUS settings for the NMC, type `radius` and press Enter.

```
apc> radius
E000: Success
Primary Server:                     0.0.0.0
Primary Server Port:                1812
Primary Server Secret:              <Password Hidden>
Primary Server Timeout:             5
Secondary Server:                   0.0.0.0
Primary Require Message-Auth:       disabled
Secondary Server Port:              1812
Secondary Server:                   0.0.0.0
Secondary Server Port:              1812
Secondary Server Secret:            <Password Hidden>
Secondary Server Timeout:           5
Secondary Require Message-Auth:     disabled
```

Example 2: To configure a 10-second timeout for a secondary RADIUS server, type: `radius -t2 10`

Error Message: `E000, E102`

reboot

Access: Super User, Administrator

Description: Restart the NMC interface only. Forces the network device to reboot.

Parameters:

Option	Description
`-Y`	Skip confirmation prompt (Uppercase Y only).

Example 1:

```
apc> reboot
E000: Success
Reboot Management Interface
Enter 'Y' to continue or <ENTER> to cancel : <user enters 'YES'>
Rebooting...
```

Example 2:

```
apc> reboot -Y
E000: Success
Reboot Management Interface
Rebooting...
```

Error Message: `E000, E100`

resetToDef

Access: Super User, Administrator

Description: Reset all parameters to their default.

Parameters:

Option	Argument	Description
-p	<all | keepip>	Reset all configuration changes, including event actions, device settings, and, optionally, TCP/IP configuration settings. all: all configuration data, including the IP address. keepip: all configuration data, except the IP address.

Example: To reset all of the configuration changes except the TCP/IP settings, type

```
apc> resettodef -p keepip

Reset to Defaults Except TCP/IP

Enter 'YES' to continue or <ENTER> to cancel: <user enters 'YES'>

Now initializing system to default values including
all User Names, Passwords.

Please wait...

Please reboot system for changes to take effect!
```

Error Message: E000, E100

session

Access: Super User, Administrator

Description: Records who is logged in (user), the interface, the Address, time, and ID.

Parameters:

Option	Argument	Description
-d	<session ID>	Delete session
-m	<enable | disable>	Multi-User Enable
-a	<enable | disable>	Remote Authentication Override

Example:

```
apc> session

User        Interface      Address       Logged In Time     ID

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

apc         Telnet         192.168.1-    00:00:20           3
                           .53

E000: Success
```

Error Message: E000, E102

smtp

Access: Super User, Administrator

Description: Internet standard for electronic mail.

Parameters:

Option	Argument
-f	<From Address>
-s	<SMTP Server>
-p	<Port> **NOTE:** Port options are 25, 465, 587, and 5000–32768
-a	<enable | disable> (Authentication)
-u	<User Name>
-w	<Password>
-e	<none | ifavail | always | implicit> (Encryption)
-c	<enable | disable> (Require Certificate)

Example:

```
apc> smtp
E000: Success
    From:                address@example.com
    Server:              mail.example.com
    Port:                25
    Auth:                disabled
    User:                User
    Password:            <not set>
    Encryption:          none
    Req. Cert:           disabled
```

Error Message: E000, E102

snmp

Access: Super User, Administrator

Description: Enable or disable SNMPv1 or SNMPv3 and configure basic SNMP settings.

NOTE: SNMPv1 is disabled by default. The Community Name (-c[n]) must be set before SNMPv1 communications can be established. In the table below, n is the access control number: 1,2,3, or 4.

Parameters:

Option	Argument	Description
-c[n]	<Community>	Specify a community name or string.
-a[n]	<read | write | writeplus | disable>	Indicate the usage rights.
-n[n]	<IP or Domain Name>	The host's name or address.
-S	<enable | disable>	Enable or disable the respective version of SNMPv1.

Example:

```
apc> snmp
E000: Success
  SNMPv1: enabled
  Access Control summary:
  Access Control #:          1
  Community:                 public
  Access Type:               read
  Address:                   0.0.0.0

  Access Control #:          2
  Community:                 private
  Access Type:               write+
  Address:                   0.0.0.0

  Access Control #:          3
  Community:                 public2
  Access Type:               disabled
  Address:                   0.0.0.0

  Access Control #:          4
  Community:                 private2
  Access Type:               disabled
  Address:                   0.0.0.0
```

Error Message: E000, E102

snmpv3

Access: Super User, Administrator

Description: Enable or disable SNMPv3, and configure basic SNMPv3 parameters.

Parameters:

Option	Argument	Description
-S	<enable | disable>	Enable or disable the respective version of SNMP
-u[n]	<User Name>	User Name
-a[n]	<Auth phrase>	Authentication pass phrase of the user profile.
-c[n]	<Crypt phrase>	Crypt phrase of the user profile.
-ap[n]	<sha | md5 | none>	Authentication protocol
-pp[n]	<aes | des | none>	Privacy protocol
-ac[n]	<enable | disable>	Access
-au[n]	<User Profile Name>	Access User Profile
-n[n]	<NMS IP>	The host name or IP address
n = access control number (1, 2, 3, or 4)		

Example:

```
apc> snmpv3
E000: Success
SNMPv3 Configuration
  SNMPV3:                 enabled

SNMPv3 User Profiles
  Index:                  1
  User Name:              acrc301H_SNMPv3
  Authentication:         MD5
  Encryption:             DES

  Index:                  2
  User Name:              apc snmp profile2
  Authentication:         None
  Encryption:             None

  Index:                  3
  User Name:              apc snmp profile3
  Authentication:         None
  Encryption:             None

  Index:                  4
  User Name:              apc snmp profile4
  Authentication:         None
  Encryption:             None


SNMPv3 Access Control
```

```
Index:                  1
User Name:              acrc301H_SNMPv3
Access:                 enabled
NMS IP/Host Name:       192.168.1.51

Index:                  2
User Name:              apc snmp profile2
Access:                 disabled
NMS IP/Host Name:       0.0.0.0

Index:                  3
User Name:              apc snmp profile3
Access:                 disabled
NMS IP/Host Name:       0.0.0.0

Index:                  4
User Name:              apc snmp profile4
Access:                 disabled
NMS IP/Host Name:       0.0.0.0
```

Error Message: E000, E102

snmptrap

Access: Super User, Administrator

Description: Enable or disable SNMP trap generation.

Parameters:

Option	Argument	
-c{n}	<Community>	Specify a community name or string.
-r[n]	<Receiver NMS IP>	The IPv4/IPv6 address or host name of the trap receiver.
-l[n]	<Language> [language code]	Specify a language. A language pack containing the desired language must be installed, and the language codes are: • enUS - English • deDe - German • ruRu - Russian • zhCn - Chinese • jaJa - Japanese • koKo - Korean • itIt - Italian • ptBr - Portuguese • frFr - French • esEs - Spanish
-t[n]	<Trap Type> [snmpV1 | snmpV3]]	Specify SNMPv1 or SNMPv3.
-p[n]	<Port>	Specify the SNMP trap port number for this trap receiver (162 by default). The range is 1 to 65535.
-g[n]	<Generation> [enable | disable]	Specify the SNMP trap port number for this trap receiver (162 by default). The range is 1 to 65535.
-a[n]	<Auth Trap> [enable | disable]	Enable or disable trap generation for this trap receiver. Enabled by default.
-u[n]	<profile1 | profile2 | profile3 | profile4> (User Name)	Select the identifier of the user profile for this trap receiver, SNMPv3 only.
n = Trap receiver number = 1, 2, 3, 4, 5 or 6		

Example: To enable and configure an SNMPv1 trap for Receiver 1, with the Community Name of public, receiver 1 IP address of 192.168.1.200, using the default English language, type:

```
apc>snmptrap -c1 public -r1
192.168.1.200 -l1 enUS -t1
snmpV1 -g1 enable
```

E000 Success

ssh

Access: Super User, Administrator

Description: Show, delete, and generate SSH server keys.

NOTE: The options in the table below are available with the `ssh key` command.

Parameters:

Option	Argument	
`-s`		
`-f`		
`-d`		
`-I`	<File Name>.pk15	Import the SSH server key from a PKCS #15 file.
`-ecdsa`	256	Generate an Elliptic Curve Digital Signature Algorithm (ECDSA) SSH server key with the specified size in bits.
`-rsa`	1024 | 2048 | 4096	Generate a Rivest–Shamir–Adleman (RSA) SSH server key with the specified size in bits.

Example 1: To display the current SSH server key, type:

```
apc>ssh key -s

E000: Success

SSH Key
- - - - -
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBFg6jI7uhfF
+VSpBdYoUMYnfq9HQc7qFCIazWe1b2L8p3ZDTSU/TTc+7tz1F4eFrMOs
+EbmMBT5o8N0HJuat5ts
```

Example 2: To import the SSH server key from a .p15 file generated by the NMC Security Wizard CLI Utility, type:

```
ssh key -i nmc.p15

E000: Success
```

ssl

Access: Super User, Administrator, Network-Only User

Description: Configure and manage the NMC's public key and Web UI certificate, and create a Certificate Signing Request (CSR).

NOTE: There are three sets of options for this command, indicated below (`key`, `csr`, and `cert`).

Configure public keys (`key`):

Parameters:

Option	Argument	
`-s`		
`-f`		
`-d`		
`-I`	`<File Name>.p15`	
`-ecdsa`	`256 | 384 | 521`	Generate an Elliptic Curve Digital Signature Algorithm (ECDSA) public key with the specified size in bits.
`-rsa`	`1024 | 2048 | 4096`	Generate a Rivest–Shamir–Adleman (RSA) public key with the specified size in bits.

Example 1: To generate a new ECDSA-521 public key, type:

```
apc>ssl key -ecdsa 521
E000: Success
```

Example 2: To import the public key from a .p15 file generated by the NMC Security Wizard CLI Utility, type:

```
ssl key -i nmc.
p15
E000: Success

SSL Key
-------
-----BEGIN PUBLIC KEY-----
MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEF/3mlLCg8RFXaHt88Lez2poPPDZf
v6i9TeD26OW1wcV9qC/JYjg4fxaK38m7+gS7Y24qAV6dI0DtbtcrJQFMEQ
-----END PUBLIC KEY-----
```

Configure Certificate Signing Request (`csr`):

Option	Argument	Description
`-s`	`<File Name>`	Display the current Certificate Signing Request (CSR).
`-q`	`<File Name>`	Create a Certificate Signing Request (CSR) from active configuration.
`-CN`	`<Common Name>`	Create a custom Certificate Signing Request (CSR). The Common Name is the fully qualified domain name (FQDN) of the NMC. For example, its IP address or *.nmc.local.
Custom Certificate Signing Request (CSR) options. **NOTE:** The below options are only available for -CN.		
`-O`	`<Organization>`	The name of your organization.
`-OU`	`<Organizational Unit>`	The division of your organization handling the certificate.
`-C`	`<Country>`	The two-letter country code of where your organization is located.
`-san`	`<Common Name | IP Address>`	The Common Name or IP address of the NMC.

NOTE: Created Certificate Signing Requests will be stored in the NMC's ssl directory. See dir, page 92.

Example 3: To create a quick Certificate Signing Request (CSR) from active configuration, type:

```
apc>ssl csr -q
E000: Success
```

Example 4: To create a minimal Certificate Signing Request (CSR), type:

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

Example 5: To create a custom Certificate Signing Request (CSR), type:

```
apc>ssl csr -CN apcxxxxxx.nmc.local -C US -san *.
nmc.local -san 190.0.2.0
E000: Success
```

Configure the Web UI's certificate (`cert`):

Option	Argument	Description
-s	<File Name>	Display the specified certificate. **NOTE:** Executing this option without an argument will display the current certificate in use.
-f	<File Name>	Display the specified certificate's fingerprint. **NOTE:** Executing this option without an argument will display the current certificate's fingerprint.
-I	<File Name>	Import a certificate.

Example 6: To display the active certificate, type:

```
apc>ssl cert -s
E000: Success
Certificate
--------
  Serial Number: 09b9af8fe5285ade
  Issuer: CN=., C=US
  Validity:
    Not Before: Sat Jul 22 15:55:36 2023 UTC
    Not After : Sat Dec 15 23:59:59 2035 UTC
  Subject: CN=., C=US
    Subject Public Key Info:
      Public Key Algorithm: ECDSA (256 bit)
      X:
          17:fd:e6:94:b0:a0:f1:11:57:68:7b:7c:f0:b7:b3:da:
          9a:0f:3c:36:5f:bf:a8:bd:4d:e0:f6:e8:e5:b5:c1:c5
      Y:
          d:a8:2f:c9:62:38:38:7f:16:8a:df:c9:bb:fa:04:bb:
          63:6e:2a:01:5e:9d:23:40:ed:6e:d7:2b:25:01:4c:11
      Curve: P-256
  Thumbprint: 7e0ce871841fbf7bc2fc3181db10954cde5cdc57
  Fingerprint:
  c211cdf02bc0cbfda52722e5dd446e4e10c174316228188d584c4c1c6f143d44
```

system

Access: Super User, Administrator

Description: View and set the system identification, contact, and location. View up time, date and time, the logged-on user, and the high-level system status P, N, A.

Parameters:

Option	Argument	Description
-n	<system-name>	Define the device name, the name of the person responsible for the device, and the physical location of the device. **NOTE:** If a value is defined with more than one word, the value must be enclosed in quotation marks. **NOTE:** These values are also used by EcoStruxure™ IT Expert or Data Center Expert and the NMC's SNMP agent.
-c	<system-contact>	
-l	<system-location>	
-m	<system-message>	Show a configurable custom message or banner on the logon page of the Web UI, CLI (Serial, Telnet, SSH), FTP or FCP.
-s	<enable | disable>] (system-hostname sync)	Synchronize the system and the hostname. This is the same as using "dns -y".

Example 1:

```
apc> system -l "Test Lab"
E000: Success
```

Example 2:

```
apc> system -n
E000: Success
Name: apc64575F
```

Error Message: E000, E102

tacacs+

Access: Super User, Administrator, Network-Only User

Description: View the existing TACACS+ settings and configure basic authentication parameters for up to two TACACS+ servers.

For a summary of TACACS+ server configuration and a list of supported TACACS+ servers, see the User Guide.
For detailed information about configuring your TACACS+ server, see the Security Handbook.

Option	Argument	Description
-p1 -p2	<server IP>	The server name or IP address of the primary or secondary TACACS+ server.
-o1 -o2	<port>	The port number of the primary or secondary TACACS+ server. **NOTE:** TACACS+ servers use port 49 by default to authenticate users. The NMC supports ports 1 to 65535.
-s1 -s2	<server secret>	The shared secret between the primary or secondary TACACS+ server and the NMC.
-p1 -p2	<server IP>	
-t1 -t2	<server time-out>	The time in seconds that the NMC waits for a response from the primary or secondary TACACS+ server.
-d1 -d2		Delete the primary or secondary TACACS+ server configuration.
-r	<0-15>	Read-Only User privilege level.
-a	<0-15>	Administrator privilege level.

Example 1: To view the existing TACACS+ settings for the NMC, type:

```
apc>tacacs+

E000: Success

Primary Server:          0.0.0.0

Primary Server           49
Port:

Primary Server           <Secret Hidden>
Secret:

Primary Server           5
Timeout:

Secondary Server:        0.0.0.0

Secondary Server         49
Port:

Secondary Server         <Secret Hidden>
Secret:

Secondary Server         5
Timeout:

Read-Only User           1
Privilege Level:

Administrator            15
Privilege Level:

apc>
```

```
E000: Success
```

Example 2: To configure a 10-second timeout for a secondary TACACS+ server, type:

```
tacacs+ -t2 10
```

tcpip

Access: Super User, Administrator

Description: View and manually configure these network settings for the Rack.

Parameters:

Option	Argument	Description
-i	<IP address>	Type the IP address of the Rack using the format xxx.xxx.xxx.xxx
-s	<subnet mask>	Type the subnet mask for the Rack.
-g	<gateway>	Type the IP address of the default gateway. **Do not** use the loopback address (127.0.0.1) as the default gateway.
-d	<domain name>	Type the DNS name configured by the DNS server.
-h	<host name>	Type the host name that the Rack will use.
-S	<enable | disable>	Enable or disable IPv4.

Example 1: To view the network settings of the Rack, type `tcpip` and press Enter.

```
apc> tcpip
E000: Success
Active IPv4 Settings
---------------------
  Active IPv4 Address:       192.168.1.185
  Active IPv4 Subnet Mask:   255.255.255.0
  Active IPv4 Gateway:       192.168.1.1


Manually Configured IPv4 Settings
----------------------------------
  IPv4:                      enabled
  Manual Settings:           enabled
  IPv4 Address:              192.168.1.185
  Subnet Mask:               255.255.255.0
  Gateway:                   192.168.1.1
  MAC Address:               28 29 86 64 57 5F
  Domain Name:               example.com
  Host Name:                 apc64575F
```

Example 2: To view the IP address of the Rack, type

```
apc> tcpip -i
E000: Success
IPv4 Address:         192.168.1.185
```

Error Message: `E000, E102`

tcpip6

Access: Super User, Administrator

Description: Enable IPv6 and view and manually configure these network settings for the .

Parameters:

Option	Argument	Description
-S	<enable | disable>	Enable or disable IPv6.
-man	<enable | disable>	Enable manual addressing for the IPv6 address of the .
-auto	<enable | disable>	Enable the to automatically configure the IPv6 address.
-i	<IPv6 address>	Set the IPv6 address of the .
-g	<IPv6 gateway>	Set the IPv6 address of the default gateway. **Do not** use the loopback address (::1) as the default gateway.
-d6	<router | statefull | statelss | never>	Set the DHCPv6 mode, with parameters of router controlled, statefull (for address and other information, they maintain their status), stateless (for information other than address, the status is not maintained), never.

Example: To view the network settings of the , type `tcpip6` and press Enter.

```
apc> tcpip6
E000: Success

IPv6:                    enabled
Manual Settings:         enabled

IPv6 Address:            ::/64
MAC Address:             00 C0 B7 92 F2 71
Gateway:                 ::
IPv6 Manual Address:     disabled
IPv6                     enabled
Autoconfiguration:
DHCPv6 Mode:             router controlled
```

Error Message: `E000, E102`

user

Access: Super User, Administrator

Description: Configure the user name and password for each account type, and configure the inactivity timeout. (You can't edit a user name, you must delete and then create a new user).

For information on the permissions granted to each account type (Super User, Administrator, Device User, Read-Only User, Network-Only User), see the User Guide.
.

Parameters:

Option	Argument	Description
-n	<user>	Indicate the user.
-cp	<current password>	For a Super User, you must specify the current password. **NOTE:** The -cp option is only required when changing the Super User's password remotely.
-pw	<user password>	Specify these options for a user. **NOTE:** Description must be enclosed in quotation marks.
-pe	<user permission>	
-d	<user description>	
-e	<enable | disable>	Enable overall access.
-te	<enable | disable>	Enable touch screen access.
-tp	<touch screen access pin>	This option is only available on certain devices.
-tr	<enable | disable>	Enable the touch screen remote authorization override. This option is only available on certain devices. If you enable this override, the NMC will allow a local user to log on using the password for the NMC that is stored locally on the NMC.
-st	<session timeout>	Specify how long a session lasts waits before logging off a user when the keyboard is idle.
-sr	<enable | disable>	Bypass RADIUS by using the serial console (CLI) connection, also known as Serial Remote Authentication Override
-el	<enable | disable>	Indicate the Event Log color coding.
-lf	<tab | csv>	Indicate the format for exporting a log file.
-ts	<us | metric>	Indicate the temperature scale, fahrenheit or celsius.
-df	<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd>	Specify a date format.
-lg	<language code (e.g. enUs)>	Specify a user language.
-del	<user name>	Delete a user.
-l	no argument	Display the current user list.

Example: To change the log off time to 10 minutes for user "JMurphy", type:

```
user -n "JMurphy" -st 10
```

Error Message: E000, E102

userauth

Access: Super User, Administrator, Network-Only User

Description: View or configure the user authentication method. Local authentication, as well as the LDAP, RADIUS, and TACACS+ protocols are supported..

Option	Argument	Description
`-l`	`first | last | off`	Specify if and when the local user database is checked: **first**: The local user database is always checked first. If the username is found, then the password is checked and the login either succeeds or is unsuccessful. If the username is not found, then remote authentication is used, if enabled. **last**: The local user database is checked after attempting remote authentication, if there is an error contacting the remote authentication server. When remote authentication is off, it behaves the same as first. **off**: The local user database is never checked. **NOTE:** Setting this to `off` is not recommended as it can result in being permanently locked out of the NMC if the remote authentication server goes down or is misconfigured on the NMC. If off is used, it is strongly recommended to enable the Remote Authentication Override setting (`session -a`) and to set the Serial Remote Authentication Override option (`user -sr`) for the Super User or an Administrator. **NOTE:** If both Local and Remote User Authentication settings are set to **off**, then Local User Authentication will automatically be set to **first**.
`-r`	`off | radius | tacacs+ | ldap`	Specify which, if any, remote authentication protocol is used: **off**: Do not use remote user authentication and always perform local user authentication. **radius**: Remote user authentication will use RADIUS. **tacacs+**: Remote user authentication will use TACACS+. **ldap**: Remote user authentication will use LDAP.

Example: To configure local authentication first, followed by TACACS+ authentication, type:

```
apc>userauth

E000: Success

Local Authentication: First

Remote Authentication: Off
```

userdflt

Access: Super User, Administrator

Description: Complimentary function to “user” establishing default user preferences. There are two main features for the default user settings:

- Determine default values when the Super User or Administrator-level account creates a new user. These values can be changed before the settings are applied to the system.
- For remote users (user accounts not stored in the system that are remotely authenticated, such as RADIUS), these values are used when a value is not provided by the authenticating server. For example, if a RADIUS server does not provide the user with a temperature preference, the value defined in this section will be used.

Parameters:

Option	Argument	Description
`-e`	`<enable | disable> (Enable)`	By default, user will be enabled or disabled upon creation. Remove (Enable) from the end
`-pe`	`<Administrator | Device | Read-Only`	Specify the user's permission level and account type.

Option	Argument	Description
	| Network-only> (user permission)	
-d	<user description>	Provide a user description.
-st	<session timeout> minute(s)	Provide a default session timeout.
-bl	<bad login attempts>	Number of incorrect login attempts a user has before the system disables their account. Upon reaching this limit, a message is displayed informing the user the account has been locked. The Super User or an Administrator-level account is needed to re-enable the account to allow the user to log back in. **NOTE:** A Super User account cannot be locked out, but can be manually disabled if necessary.
-el	<enable | disable> (Event Log Color Coding)	Enable or disable event log color coding.
-lf	<tab | csv> (Export Log Format)	Specify the log export format, tab or CSV.
-ts	<us | metrics> (Temperature Scale)	Specify the user's temperature scale. This setting is also used by the system when a user preference is not available (for example, email notifications).
-df	<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd> (Date Format)	Specify the user's preferred date format.
-lg	<language code (enUs, etc)>	User language
-sp	<enable | disable>	Strong password
-pp	<interval in days>	Required password change interval

Example:

```
apc> userdflt
E000: Success
Access: Disabled
User Permission: Administrator
User Description: User Description
Session Timeout: 3 minutes
Bad Login Attempts: 0
Event Log Color Coding: Enabled
Export Log Format: Tab
Temperature Scale: Metric
Date Format: mm/dd/yyyy
Language: English (enUs)
Strong Passwords: Disabled
Require Password Change: 0 day(s) (Disabled)
```

Error Message: E000, E102

web

Access: Super User, Administrator

Description: Enable access to the web interface using HTTP or HTTPS.

For additional security, the port setting for HTTP and HTTPS can be changed to any unused port from 5000 to 32768. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114, type `http://152.214.12.114:5000`

Parameters:

Option	Argument	Description
`-h`	`<enable | disable>`	Enable or disable access to the user interface for HTTP.
`-s`	`<enable | disable>`	Enable or disable access to the user interface for HTTPS. When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate, using SSL/TLS.
`-ph`	`<http port #>`	Specify the TCP/IP port used by HTTP to communicate with the (80 by default). The other available range is 5000–32768.
`-ps`	`<https port #>`	Specify the TCP/IP port used by HTTPS to communicate with the (443 by default). The other available range is 5000–32768.
`-mp`	`<minimum protocol>`	Specify the minimum HTTPS protocol to use. Options are `TLS1.1 | TLS v1.2, or TLS v1.3.`
`-lsp`	`<enable | disable>`	Enable or disable the limited status page.
`-lsd`	`<enable | disable>`	Enable or disable the limited status page as the default page.
`-cs`	`<0 | 1 | 2 | 3 | 4>`	Select the level of security of TLS v1.2 cipher suites between 0 - 4, where 4 is the highest level of security, and 0 is the lowest level of security. The default value is 4. **NOTE:** The `-cs` option is only applied when `-mp` is set to TLS v1.2. When a value between 0 - 4 is entered, the CLI responds with a list of the currently allowed SSL cipher suites.
`-hs`	`<enable | disable>`	Enable/ disable the HTTP Strict Transport Security Header (HSTS) response header.

Example 1: To prevent all access to the Web UI, type

```
apc> web -h disable -s disable
```

Example 2: To define the TCP/IP port used by HTTP, type

```
apc> web
E000: Success


HttP:                    enabled
Https:                   disabled
Http Port:               80
Https Port:              443
Minimum Protocol:        TLS1.2


Limited Status           disabled
Access:
Lim. Status Page Used:   n/a
```

```
TLS1.2 Cipher Suite      4
Filter:
HSTS:                    disabled
```

Error Message: E000, E102

whoami

Access: Super User, Administrator, Device User, Read Only User

Description: Provides login information on the current user.

Parameters: None.

Example:

```
apc> whoami
E000: Success
admin
```

Error Message: None.

xferINI

Access: Super User, Administrator

Description: Use XMODEM to upload an INI file while accessing the CLI through a serial connection. After the upload completes:

- If there are any system or network changes, the CLI restarts and the user must log on again.
- If you selected a baud rate for the file transfer that is not the same as the default baud rate for the , you must reset the baud rate to the default to reestablish communication with the .

Parameters: None.

Example:

```
apc> xferINI
Enter 'YES' to continue or <ENTER> to cancel : <user enters 'YES'>
- - - - - - - File Transfer Baud Rate - - - - - - - - - - - - - - - - - - - - - - - - - - -
  1-2400
  2-9600
  3-19200
  4-38400
> <user enters baudrate selection>
Transferring at current baud rate (9600), press <ENTER>...
<user presses <ENTER>>
Start XMODEM-CRC Transfer Now!
CC
<user starts sending INI>
150 bytes have successfully been transmitted.
```

Error Message: None.

xferStatus

Access: Super User, Administrator

Description: View the result of the last file transfer.

Parameters: None.

Example:

```
apc> xferStatus
E000: Success
Result of last file transfer: Failure unknown
```

Error Message: `E000`

Troubleshooting

If necessary, contact *Schneider Electric Technical Support* describing the nature of the fault and its possible cause displayed on the control panel.

First Aid

IMPORTANT: The following measures can be carried out by trained and qualified personnel only.

First Aid Measures in Case of Electrical Shock

In case of electrical shock, follow this procedure:

1. Turn off the electricity source, if possible. If not, remove the same using a dry, non-conducting object made of paperboard, plastic or wood
2. In case of electrical burn, cover any burned areas with a sterile gauze bandage, if available, or a clean cloth. Don't use a blanket or towel, because loose fibers may stick to the burns
3. If necessary, perform mouth-to-mouth resuscitation when the person shows no signs of circulation, such as breathing, coughing or movement

In case of persisting irritations or symptoms, contact the emergency aid.

First Aid Measures in Case of Burn

In case of burn, follow this procedure:

1. Cool the burn: place the burned area under running cool (not cold) water for at least five minutes or apply a clean wet compress to reduce pain and swelling
2. Remove rings or other tight items from the burned area: do this quickly and gently before the area swells
3. Do not break blisters as they prevent infection. If a blister breaks, clean the area with water and apply an antibiotic ointment
4. When a burn is completely cooled, apply a lotion to relieve the area and prevent it from drying
5. Loosely wrap a sterile gauze bandage around the burn
6. If needed, take a pain reliever making sure to carefully read the related information leaflet

In case of severe burn, contact the emergency aid or go to the nearest hospital.

First Aid Measures in Case of Cut from Sharp Edges

In case of deep cuts, follow this procedure:

1. Have the injured person lie down and elevate the site of bleeding. Do not breathe on an open wound. Any objects in the wound should not be removed.
2. Remove or cut clothing around the wound. Gently remove rings or other tight items from the injured area, also to allow blood circulation in case of swelling
3. Apply direct pressure and elevate the area for fifteen minutes. If blood soaks through the cloth, apply another one without lifting the first. If there is an object that could not be removed, apply pressure around the object and not directly over it and then seek medical attention
4. Once the bleeding has stopped, clean the wound to reduce the chance of infection: wash the wound for five minutes with cool water
5. Apply a bandage to protect the cut from dirt and prevent infection. Moisture-enhancing bandages are usually available in first-aid kits

If an infection occurs under the bandage, contact a doctor.

If the cut does not stop bleeding, contact the emergency aid.

First Aid Measures in Case of Fall

In case of fall from considerable heights, do not move the person to avoid further injury.

Call for medical help and, if necessary:

1. Stop any bleeding by applying pressure to the wound with a clean cloth
2. Immobilize the injured area. Do not try and realign any bone sticking out
3. Apply ice packs to limit swelling and help relieve the pain. Do not apply ice directly to the skin

Worldwide Customer Support

Customer support for this product is available at no charge in any of 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.se.com (Corporate Headquarters)

    Connect to localized Schneider Electric websites for specific countries, each of which provides customer support information.
  - www.se.com/support/

    Get global support by searching the Schneider Electric Knowledge Base and using esupport.
- Contact the Schneider Electric Customer Support Center by telephone or e-mail.

  Go to **www.se.com > Support > Contact Support** to find contact information for country-specific centers.

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

+ 33 (0) 1 41 29 70 00

www.schneider-electric.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.

990–2022726B–001