

# Uniflair™ InRow® Direct Expansion Air Conditioners

## RD100 & RD200 Series (Indoor Unit)

## ACCD752XX Air-cooled Condenser Series (Heat Rejection Unit)

## ACCD752XX Fluid Cooler Series (Heat Rejection Unit)

### Online Guide

#### 300 mm Indoor Unit:

ACRD100: 10kW 208-240V/1ph/60Hz, Single Power

ACRD101: 10kW 220-240V/1ph/50Hz, Single Power

ACRD200: 10kW 208-240V/1ph/60Hz, Single Power

ACRD201: 10kW 220-240V/1ph/50Hz, Single Power

#### Air-cooled Condenser:

ACCD75214 (ACCD75215): 208-240V/1ph/60Hz, UL, 40.6°C/105°F Ambient (46°C/115°F)

ACCD75216 (ACCD75217): 380-415V/3ph/50Hz, CE, 40.6°C/105°F Ambient (46°C/115°F)

ACCD75218 (ACCD75219): 220-240V/1ph/50Hz, CE, 40.6°C/105°F Ambient (46°C/115°F)

ACCD75220: 220-240V/1ph/50Hz, CCC, 40.6°C/105°F Ambient

#### Fluid Cooler:

ACCD75210: 460V/3ph/60Hz, UL, 40°C/104°F Ambient

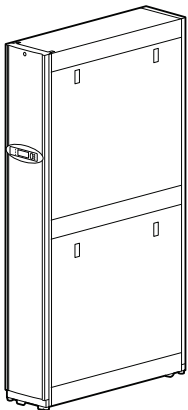
ACCD75255: 480V/3ph/60Hz, UL, 35°C/95°F Ambient

ACCD75256: 380-415V/3ph/50Hz, CE, 35°C/95°F Ambient

ACCD75257: 380-415V/3ph/50Hz, CE, 40°C/104°F Ambient

990-3632C-001

Release Date: 05/2024



# 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.**

# Table of Contents

Introduction .....	7
Product Description .....	7
Unit Overview .....	7
Features .....	7
IPv4 Initial Setup .....	7
IPv6 Initial Setup .....	8
Network Management with Other Applications .....	8
Internal Management Features .....	9
Overview .....	9
Access Priority for Logging On .....	9
Types of User Accounts .....	9
Display Interface .....	10
Status LED .....	11
Check Log LED .....	11
Warning Alarm LED .....	11
Critical Alarm LED .....	11
How to Recover from a Lost Password .....	11
Watchdog Features .....	12
Overview .....	12
Network Interface Watchdog Mechanism .....	12
Resetting the Network Timer .....	12
Web User Interface .....	13
Introduction .....	13
Overview .....	13
Supported Web Browsers .....	13
How to Log On .....	13
Overview .....	13
First Log In .....	15
URL Address Format .....	15
Home Screen .....	16
Overview .....	16
Monitoring the Status .....	17
Unit Status .....	17
Overview .....	17
Detailed Status .....	17
Run Hours .....	18
Unit Thresholds .....	18
Unit Service Intervals .....	18
Group Status .....	19
Group Overview .....	19
Network Status .....	19
Current IPv4 Settings .....	20
Current IPv6 Settings .....	20
Domain Name System Status .....	20
Port Speed .....	20
Security and Network Control .....	21
Manage User Sessions .....	21
Reset the Network Interface .....	21

- Configuring Your Settings** ..... 22
  - Unit Configuration ..... 22
    - Thresholds ..... 22
    - Unit Configuration ..... 22
  - Group Configuration ..... 23
    - Configuration ..... 23
    - Setpoints ..... 24
  - Security Menu ..... 25
    - Session Management ..... 25
    - Ping Response ..... 25
    - Local Users ..... 25
    - Remote Users Authentication ..... 27
    - Firewall ..... 29
  - Network Configuration ..... 33
    - TCP/IP Settings for IPv4 ..... 33
    - TCP/IP Settings for IPv6 ..... 33
    - DHCP Response Options ..... 34
    - Port Speed ..... 36
    - DNS Configuration ..... 36
    - DNS Testing ..... 37
    - Web Access ..... 37
    - Web SSL Certificate Configuration ..... 38
    - Console Settings ..... 38
    - SNMPv1 Access Configuration ..... 39
    - SNMPv3 Access Configuration ..... 40
    - Modbus Configuration ..... 41
    - BACnet Settings ..... 42
    - FTP Server Access Configuration ..... 44
  - Notification Menu ..... 45
    - Types of Notification ..... 45
    - Configuring Event Actions ..... 45
    - E-Mail Notification Configuration ..... 47
    - SNMP Trap Receiver Configuration ..... 49
    - SNMP Traps Test Configuration ..... 49
  - General Menu ..... 50
    - Identification Screen ..... 50
    - Date/Time Configuration ..... 50
    - Create and Import Settings with the Configuration File ..... 51
    - Configure the Links Screen ..... 51
  - Log Configuration ..... 52
    - Identify Syslog Servers ..... 52
    - Syslog Settings ..... 52
    - Syslog Test and Format Example ..... 53
- Tests** ..... 54
  - Set the Unit LED Lights to Blink ..... 54
- Logs and About Menus** ..... 55
  - Event and Data Logs ..... 55
    - Event Log ..... 55
    - Data Log ..... 57
    - Firewall Log ..... 59
    - How to Use FTP or SCP to Retrieve Log Files ..... 59

About the Network .....	60
Troubleshooting and Support.....	61
<b>Device IP Configuration Wizard.....</b>	<b>62</b>
Capabilities, Requirements, and Installation .....	62
How to Use the Wizard to Configure TCP/IP Settings.....	62
System Requirements .....	62
Installation.....	62
Use the Wizard.....	62
Launch the Wizard .....	62
Configure the Basic TCP/IP Settings Remotely .....	62
Configure or Re-Configure the TCP/IP Settings Locally.....	63
<b>How to Export Configuration Settings .....</b>	<b>64</b>
Retrieve and Export the .ini File .....	64
Summary of the Procedure .....	64
Contents of the .ini File.....	64
Detailed Procedures .....	64
The Upload Event and Error Message.....	66
The Event and Its Error Messages .....	66
Messages in config.ini.....	66
Errors Generated by Overridden Values .....	66
Related Topics .....	67
<b>Command Line Interface (CLI).....</b>	<b>68</b>
How to Log On .....	68
Remote Access to the Command Line Interface (CLI).....	68
Local Access to the Command Line Interface (CLI) .....	70
Main Screen.....	70
How to Use the CLI.....	72
Command Help Syntax.....	72
Command Response Codes .....	73
Argument Quoting.....	73
Escape Sequences .....	74
Prompts for User Input during Command Execution.....	74
Delimiter .....	74
Option and Argument Inputs .....	74
Network Management Card Command Descriptions .....	76
? or help .....	76
about .....	77
alarmcount .....	78
boot .....	79
bye, exit, or quit .....	79
cd .....	79
clrrst .....	81
console .....	82
date .....	83
delete.....	83
dir .....	84
dns .....	85
eapol .....	86
email.....	87
eventlog .....	88

exit .....	89
firewall .....	89
format .....	89
ftp .....	90
help .....	91
lang .....	92
lastrst.....	92
ledblink .....	92
logzip.....	94
netstat.....	94
ntp .....	95
ping .....	95
portSpeed .....	97
prompt .....	98
pwd .....	98
quit .....	99
radius.....	100
reboot .....	101
resetToDef .....	102
session .....	102
smtp .....	103
snmp .....	104
snmpv3.....	105
snmptrap.....	107
ssh .....	108
ssl.....	109
system .....	111
tcpip.....	112
tcpip6.....	112
user .....	114
userdft.....	115
web .....	117
whoami .....	118
Wifi .....	118
xferINI.....	119
xferStatus.....	120
<b>File Transfers.....</b>	<b>121</b>
Updating the Firmware.....	121
Firmware Module Files .....	121
<b>Troubleshooting .....</b>	<b>122</b>

# 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 (HTTP)
- Secure Shell (SSH)
- Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS)
- Simple Network Management Protocol versions 1 and 3 (SNMPv1, SNMPv3)
- File Transfer Protocol (FTP)
- Secure Copy (SCP)
- Telnet
- Syslog
- RADIUS
- Modbus TCP/IP
- BACnet

### Features

- Provides data and event logs.
- Enables you to set up notifications through e-mail 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 34.

## 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 33.

## 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 — Create components needed to help with security for the unit when you are using Secure Sockets Layer (SSL) with related protocols and encryption routines.



# Internal Management Features

## Overview

Use the Web user interface (UI) to view the status and manage the unit. You can also use SNMP to monitor the status of the unit.

Use Modbus RTU to view the network settings through the building management system.

## 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 25.



## Types of User Accounts

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

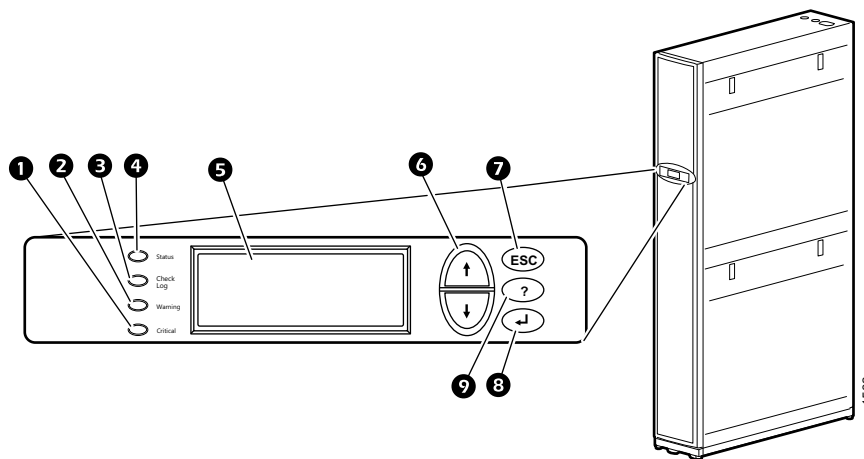
- A Super User/Administrator can use all of the menus in the UI and all of the commands in the command line interface. Administrator user types can be deleted. The default user name and password are both **apc**.
  - NOTE:** The Super User cannot be renamed or deleted, but it can be disabled. It is recommended 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.
  - IMPORTANT:** You will be prompted to enter a new password the first time you connect to the NMC with the Super User account.
- 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 the default password is `apc`.
- 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 the default password is `apc`.
- A Network-Only User can only log on using the Web user interface (UI) and CLI (through telnet 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 25.

## Display Interface



Item	Description	Function
1	Critical alarm LED (red)	When illuminated, a critical alarm condition exists that requires your immediate attention.
2	Warning alarm LED (yellow)	When illuminated, a warning alarm condition exists. Failure to correct this condition could cause a critical alarm.
3	Check log LED (yellow)	When illuminated, at least one new event has been logged since the last time the log was checked. Only events that pertain to the operation of the cooling unit will activate this LED.
4	Check log LED (yellow)	When illuminated, the cooling unit is receiving electrical power. When the LED is flashing, the cooling unit is downloading firmware for the controller. This may take a few minutes.
5	Liquid crystal display (LCD)	View alarms, status data, context-sensitive help, and modify configurable items.
6	Up and down arrow keys	Select menu items and access information.
7	ESC key	Return to previous screen or cancel current operation.
8	Enter key	Open menu items and input changes to the cooling unit settings.
9	Help key	Display context-sensitive help. Press the help key for information about each option on the screen and for instructions on performing the tasks.

## Status LED

This LED indicates the status of the unit.

Condition	Description
Off	The unit has no power.
Solid green	The unit is receiving power.
Flashing green	The unit is receiving a firmware upgrade.

## Check Log LED

When yellow, this LED indicates a new critical alarm, warning alarm, or event has occurred since the last time the event log was viewed from the display interface.

## Warning Alarm LED

When yellow, this LED indicates that a warning alarm condition exists and may require your attention to prevent it from deteriorating into a critical state. A new alarm condition causes the display interface to beep every 30 seconds, if the audible alarm is enabled. Press any function key to silence the audible alarm. If the temperature returns to normal, the LED returns to normal.

## Critical Alarm LED

When red, this LED indicates that a critical alarm condition exists and requires your immediate attention. A new alarm condition causes the display interface to beep every 30 seconds, if the audible alarm is enabled. Press any function key to silence the audible alarm. The light continues to blink to show the critical status.

## 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.

# 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 37 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. If you do not have a user name and password assigned, the default user name can be used and differs by account type:

- **apc** for Administrator
- **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 9.

When HTTPS is enabled, the unit generates its own certificate. This certificate negotiates encryption methods with your browser.



For more information, search for Security Handbook at [www.schneider-electric.com](http://www.schneider-electric.com) > **Support** > **Download Documents and Software**.

## 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). After you log in, you will be directed to the **Protocol Status 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. When you specify a non-default Web-server port in Internet Explorer, you must include http:// or https:// in the URL.

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
	<b>No Alarm:</b> No alarms are present.
	<b>Informational:</b> Provides details on any alarms that are not a warning or critical.
	<b>Warning:</b> An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
	<b>Critical:</b> 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 51.



# Monitoring the Status

## Unit Status

### Path: Main > Status > Unit

View a list of units in the group. For each unit, view location, unit-type, application firmware version, and IP address. To ensure optimal group performance, confirm that the units use the same application firmware version. The value **InRow RD** shall always display in the **unit-type** field. You can group InRow RD 100-series and InRow RD 200-series units, but do not attempt to connect other cooling-unit models to the group. Doing so may cause communication problems and prevent the group from operating correctly.



The unit and network can be configured using the **Configuration** menu options. See [Configuring Your Settings](#), page 22.

## Overview

### Path: Main > Status > Unit > Overview

- **Operating Mode:** The current operating mode of the unit:
  - **On:** The unit is providing cooling.
  - **Standby:** The user turned off the cooling functions of the unit, or the input contact is in an abnormal state.
  - **Idle:** The unit is not providing cooling because it has active alarms.
  - **Refrig:** The unit is in Refrigerant Fill mode.
- **Compressor State:** The current state of the compressor (**On/Off**).
- **Cool Output:** The actual cooling output of the unit.
- **Cool Demand:** The amount of cooling that the heat load currently requires.
- **Rack Inlet Temperature:** The average air temperature entering the racks.
- **Supply Air Temperature:** The temperature of the air leaving the unit.
- **Return Air Temperature:** The temperature of the air entering the unit.
- **Suction Temperature:** The temperature of gas entering the compressor.
- **Airflow:** The velocity at which air flows into or out of the unit.
- **Evaporator Fan Speed:** The average revolutions per minute (RPM) of all evaporator fans, given as percentage of the maximum fan speed.
- **Fluid Valve Position (ACRD100):** The position of the valve that regulates fluid flow through the unit (0% indicates that the valve is fully closed and 100% indicates that it is fully opened).
- **Hot Gas Bypass Valve Position (ACRD200):** The position of the valve that regulates hot gas bypass (0% indicates that the valve is fully closed and 100% indicates that it is fully opened).

## Detailed Status

### Path: Main > Status > Unit > Detailed Status

- **Input State:** The state of the standby digital input.
- **Output State:** The state of the output contact.
- **OHE Input State:** The current state of the Outside Heat Exchanger (OHE) input. An alarm is generated if the current state differs from the configured normal state.

- **OHE Output State:** The current state of the OHE output.
- **Filter Differential Pressure:** The amount of pressure drop through the air filter media.
- **Suction Pressure:** The pressure of the low pressure (suction) refrigerant line.
- **Discharge Pressure:** The pressure of the high pressure (discharge) refrigerant line.
- **Superheat:** The difference between the suction line temperature and the evaporation saturation temperature.

## Run Hours

### Path: Main > Status > Unit > Run Hours

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

- Unit Run Hours
  - NOTE:** When the air filter is replaced, use the **Air Filter Serviced** button to reset the maintenance alarm.
- Air Filter Run Hours
- Condensate Pump Run Hours
- Compressor Run Hours
- Evaporator Fan 1 Run Hours
- Evaporator Fan 2 Run Hours
- Evaporator Fan 3 Run Hours
- Evaporator Fan 4 Run Hours
- Evaporator Fan 5 Run Hours
- Evaporator Fan 6 Run Hours
- Upper Fan Power Supply Run Hours
- Lower Fan Power Supply Run Hours

## Unit Thresholds

### Path: Main > Status > Unit > Thresholds

View information related to the unit thresholds.

- **Rack Inlet High Temperature Threshold:** The high temperature threshold for the rack inlet air temperature as averaged by the rack inlet temperature sensors. If the temperature exceeds this threshold, an alarm will occur. (0–100°C (32–212°F))
- **Supply Air High Temperature Threshold:** The high temperature threshold for the supply air as averaged by the supply air temperature sensors. If the temperature exceeds this threshold, an alarm will occur. (0–100°C (32–212°F))
- **Return Air High Temperature Threshold:** The high temperature threshold for the air entering the cooling unit. If the temperature exceeds this threshold, an alarm will occur. (0–100°C (32–212°F))

## Unit Service Intervals

### Path: Main > Status > Unit > Service Intervals

View information related to the service intervals.

- **Air Filter Intervals:** Set the interval for the cooling air filter.
- **Air Filter Alarm Enable:** Select to **Enable** or **Disable** the alarm.

## Group Status

**Path: Main > Status > Group**

View information related to the cooling group.



You can configure your unit and network using the **Configuration > Group** menu options. See Group Configuration, page 23.

## Group Overview

**Path: Main > Status > Group > Overview**

- **Cool Setpoint:** The temperature set to maintain the room environment.
- **Supply Air Setpoint (InRow/HACS/RACS/CACS):** The target value for air leaving the cooling units in the group. The Supply Air Setpoint value must be equal to or below the Cool Setpoint value.
- **Airflow:** The combined airflow output of the units in the cooling group.
- **Active Flow Control Status:** The conditional state of the containment air pressure differential measurement device (AFC).
  - **Under:** The air flow status on at least one AFC unit is insufficient. The LED on the AFC will be illuminated as red.
  - **OK:** There is nominal air flow status on all AFC units. The LED on the AFC will be illuminated as green.
  - **Over:** There is a surplus of air flow status on at least one AFC unit. The LED on the AFC will be illuminated as blue.
  - **NA:** There are no AFC units installed or no status reading is available.
- **Rack Inlet Max Temperature:** The highest rack inlet temperature reported by any unit in the cooling group.
- **Rack Inlet Min Temperature:** The lowest rack inlet temperature reported by any unit in the cooling group.
- **Maximum Return Air Temperature:** The highest return temperature reported by any cooling unit in the cooling group.
- **Minimum Return Air Temperature:** The lowest return temperature reported by any cooling unit in the cooling group.
- **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.
- 

## 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 **Session Management** menu displays all active users currently connected to the unit. To view information about a given user, click their user name. The **Session Details** screen displays basic information about the user including what interface they are logged-in to, their IP address, and user authentication. There is also an option to **Terminate Session** for the user.

## Reset the Network Interface

**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**

Set alarms to alert you when components require service or there are high temperature violations.

When the air temperature exceeds the temperature defined by the **High Temperature Threshold**, an alarm will occur. Set **High Temperature Thresholds** for the following:

- **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 Temperature High Threshold:** An alarm condition exists when the temperature of the air output from the cooling unit exceeds the threshold.
- **Return Air Temperature High Threshold:** An alarm condition exists when the temperature of the air entering the cooling unit at the temperature sensor exceeds the threshold.

## Unit Configuration

**Path: Main > Configuration > Unit > Configuration**

- **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 Fault activates. Set to **No** to disable the cooling unit from entering idle mode if a leak is detected.

**NOTE:** The leak sensor (Schneider Electric part number AP9325) is optional.

**NOTE:** There are six alarms that will cause the cooling unit to enter idle mode:

- Water Detection Fault (when **Idle On Leak Detect** is set to **Yes**)
  - Condensate Pump Fault
  - Cooling Failure
  - Low Suction Pressure Fault
  - High Discharge Pressure Fault
  - Critical Sensor Failure
- **Input Normal State:** Set the normal state of the contact (**Open** or **Closed**). The cooling unit changes its operating mode to **Closed** when the actual state differs from the normal state.

- **Output Normal State:** Set the normal state of the contact (**Open** or **Closed**). If the state of an alarm or event mapped to this contact changes from the normal state, the contact also changes state.
- **Output Source:** Define the type of output source (alarm), either **Any Alarm** or **Only Critical Alarms**, that causes the output to change from its normal state.
- **OHE Input Normal State:** Define the normal state of the Outside Heat Exchanger (OHE), **open** or **closed**. An alarm is generated if the current state differs from the configured normal state.

## Group Configuration

### Path: Main Configuration > Group

The cooling group configuration settings determine which components are available and how the cooling group should operate.

**NOTE:** All changes to settings must be performed by qualified personnel.

## Configuration

### Path: Main > Configuration > Group > Configuration

The **Configuration** section contains settings that identify the number of units installed in this cooling group and the physical arrangement of those units.

- **Number of Units in Group:** The number of units in this cooling group. Up to 12 units can be joined together to work as a single cooling group.
- **Configuration Type:** The air flow control strategy the group uses. You can change this setting only when all of the units in the group are in **Standby** mode.
  - **Spot:** The unit regulates the Return Air Temperature. The Rack Inlet Air Temperature sensor is ignored for control purposes. Use this option for standalone units only.
  - **Rack Air Containment System (RACS):** Air flow in the enclosure is controlled by a ducting system fitted to the enclosure.
  - **Hot Aisle Containment System (HACS):** Air flow in the room is controlled by enclosing the hot air aisle.
  - **In-Row:** Air flow is horizontal to allow in-row operation of cooling solutions. (Backup and Load Assist functions are disabled in **InRow** mode.)
- **Capacity Control:** There are two setting options to determine how the cooling unit cools:
  - **Discrete:** Spot cooling configurations only. The cooling unit runs at a set speed with the hot gas bypass valve (HGBV) fully closed. The compressor comes on when the return air temperature reaches the cool setpoint plus the cool deadband.
  - **Prop (Proportional):** The cooling unit modulates the fan speeds and HGBV to match the cooling output to the load demand.
- **Active Flow Control Lamp Test:** When enabled, the Active Flow Controller (s) LEDs will cycle through a red, green, and blue illumination pattern. (Not on unit.)
- **Number of Active Flow Controllers:** The number of AFC units in the group (0–5).
- **Altitude:** Set the altitude (in feet or meters) of the unit above sea level. This number is used to estimate the density of air and is a factor in pressure measurement.

## Setpoints

### Path: Main > Configuration > Group > Setpoints

- **Cool Setpoint:** The air temperature setpoint the cooling units work to achieve and then maintain during operation. In a **Spot** cooling configuration, the cooling unit will bring the **Return Air Temperature** to the **Cool Setpoint**. In an **InRow** configuration, the cooling units will bring the **Rack Inlet Air Temperature** to the **Cool Setpoint**. In a **RACS** configuration, the cooling units will match the air flow of the loads by controlling the difference between the supply and return air temperatures as specified by the fan speed setting. The setpoint must be within 18.9 – 32.2 °C (66.0 – 90.0°F).
- **Cool Deadband:** The air temperature must exceed the **Cool Setpoint** plus the **Cool Deadband** before the cooling unit turns on the compressor.
- **Supply Air Setpoint (InRow/HACS/RACS/CACS):** The target value for air leaving the cooling units in the group. The Supply Air Setpoint value must be equal to or below the Cool Setpoint value.
- **Capacity Control:** The method the units use to regulate the cooling demand. **Discrete** is used for the Spot Cooling configuration mode only. **Proportional** is used for all other configuration modes.
  - **Proportional Mode:** The unit modulates the fan speeds and Hot Gas Bypass Valve (HGBV) to match the cooling output to the load demand, so the compressor turns off less frequently.
  - **Discrete Mode:** The unit runs the fans at a set speed with the HGBV fully closed. The unit activates the compressor when the Return Air Temperature reaches the Cool Setpoint plus the Cool Deadband. The unit deactivates the compressor when the Return Air Temperature reaches the Cool Setpoint.
- **Fan Speed Preference:** The preferred fan speed for normal operation of the cooling unit. Selecting the **RACS** or **HACS** mode sets the desired temperature difference between the rack inlet air temperature and the rack outlet air temperature.
- **Active Flow Control Bias:** This setting is used to change the bias of the controller by adjusting the contained aisle pressure threshold. **Zero** is the default setting. Only qualified service personnel can make changes to these settings.
  - Hot Aisle Containment (HACS)
    - If the cooling units seem to be under-cooling, select **Negative** or **Slightly Negative** to adjust the aisle pressure for additional cooling.
    - If the cooling units seem to be over-cooling, select **Positive** or **Slightly Positive** to adjust the aisle pressure for less cooling.
  - Cold Aisle Containment (CACS)
    - If the cooling units seem to be under-cooling, select **Positive** or **Slightly Positive** to adjust the aisle pressure for additional cooling.
    - If the cooling units seem to be over-cooling, select **Negative** or **Slightly Negative** to adjust the aisle pressure for less cooling.

Setting	Blue LED—HACS Red LED—CACS	Setpoint Green LED	Red LED—HACS Blue LED—CACS
<b>Positive</b>	< -0.008 in. ±3%	0.004 ±0.0004 in.	> 0.016 in. ±3%
<b>Slightly Positive</b>	< -0.010 in. ±3%	0.002 ±0.0004 in.	> 0.014 in. ±3%
<b>Zero</b>	< -0.012 in. ±3%	0.000 ±0.0004 in.	> 0.012 in. ±3%
<b>Slightly Negative</b>	< -0.014 in. ±3%	-0.002 ±0.0004 in.	> 0.010 in. ±3%
<b>Negative</b>	< -0.016 in. ±3%	-0.004 ±0.0004 in.	> 0.008 in. ±3%

**NOTE:** Only a Schneider Electric Field Service Engineer can change the following values:

- **Cool Gain “P”:** Set the proportional multiplier to correct for differences between the temperature and the setpoint of the selected control sensor.



- **Cool Reset Rate “I”**: Set the integral multiplier to correct for the proportional offset.
- **Cool Derivative “D”**: Set the derivative multiplier to counteract overshoot and droop during changes in the room load.

## 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.

**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 25 and Remote Users Authentication, page 27.

**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 55 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 47 and SNMP Trap Receiver Configuration, page 49.

## 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 Method

Specify how you want users to be authenticated at logon.

The following authentication and authorization functions of remote authentication dial-in user service (RADIUS) are supported:

- When a user accesses the unit or other network-enabled device that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the permission level of the user.
- RADIUS user names are limited to 32 characters with the unit.

Select one of the following:

- **Local Authentication Only:** RADIUS is disabled.



See Local Users, page 25.

- **RADIUS, then Local Authentication:** Both are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server does not respond, local authentication is used.
- **RADIUS Only:** There is no local authentication.

If **RADIUS Only** is selected, and the RADIUS server is 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 or radiusLocal.

For example, the command to change the access setting to local would be **radius -a local**.

## Radius

**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:

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

The **RADIUS Server** menu for each RADIUS server contains the following options:

- **RADIUS Server:** The name or IP address (IPv4 or IPv6) of the RADIUS server.
- **Port:** The port on which the RADIUS server listens to authenticate users. This is port 1812 by default but can be changed to any unused port between 5000-32678.
- **Secret:** The shared secret between the RADIUS server and the unit.
- **Reply Timeout:** The time in seconds that the unit waits for a response from the RADIUS server.
- **Test Settings:** Enter the user name and password configured on the RADIUS server order to test the configured settings.
- **Skip Test and Apply:** Applies the RADIUS server settings without testing.

## Configuring the RADIUS Server

You must configure your RADIUS server to work with the cooling unit.

Add the IP address of the unit to the RADIUS server client list (file).

- 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 UI only).
- VSAs can be used instead of the Service-Type attributes provided by the RADIUS server.
- VSAs require a dictionary entry and a RADIUS user 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  
thawk Auth-Type = System  
APC-Service-Type = Device
```

## Supported RADIUS servers

FreeRADIUS and Microsoft IAS 2003 are supported. Other commonly available RADIUS applications may work but have not been fully tested.

## 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 59. 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 EAP-TLS as an authentication method which requires you to upload 3 client-side certificates. The private key is stored in an encrypted

format. You need to provide a valid passphrase to be able to enable 802.1X security access.

**NOTE:** The NMC supports only EAP-TLS authentication method.

The Web UI offers the following options for EAPoL configuration:

- **EAPoL Access:** Used to enable or disable 802.1X security access.
  - NOTE:** 802.1X security access is disabled by default. You can only enable access when valid certificates and a valid passphrase for the private key are provided.
- **Supplicant Identifier:** Allows you to set your own supplicant identifier (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.
- **CA Certificate:** Upload/replace or remove a CA root certificate. The supported file formats are PEM (Privacy Enhanced Mail) or the DER (Distinguished Encoding Rules) format with permitted file extension .pem, .PEM, .der, or .DER.
- **Private Key Certificate:** Upload/replace or remove an encrypted private key. The supported file formats are PEM (Privacy Enhanced Mail) or the DER (Distinguished Encoding Rules) format with permitted file extensions .key or .KEY.
  - NOTE:** Unencrypted private keys are not accepted.
- **Private Key Passphrase:** Provide the passphrase to decrypt the encrypted private key. Allows up to 64 characters including whitespace.
- **User/Public Certificate:** Upload/replace or remove a user/public certificate. The supported file formats are PEM (Privacy Enhanced Mail) or the DER (Distinguished Encoding Rules) format with permitted file extensions .pem, .PEM, .der, or .DER.

## 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	<p>When this radio box is selected, DHCPv6 is controlled by the <b>M</b> (Managed Address Configuration Flag) and <b>O</b> (Other Stateful Configuration Flag) flags received in IPv6 router advertisements.</p> <p>When a router advertisement is received, the unit checks whether the M and O flags are set. The unit interprets them as follows:</p> <ul style="list-style-type: none"> <li>• <b>Neither is set:</b> 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.</li> <li>• <b>M, or M and O are set:</b> In this situation, full DHCPv6 address configuration occurs. DHCPv6 is used to obtain addresses AND other configuration settings. This is known as “DHCPv6 stateful.”</li> </ul> <p>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.</p> <p>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.</p> <ul style="list-style-type: none"> <li>• <b>Only O is set:</b> 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.”</li> </ul>
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](http://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: <code>my_server.my_domain.com</code>
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.
  - SSL 3.0
  - TLS 1.0
  - TLS 1.1
  - TLS 1.2
- **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.
- **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 SNMP are transferred over the network as plain text. If your network requires the high security of encryption, disable SNMP access or set the access for each community to Read. (A community with Read access can receive status information and use SNMP 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:** SNMP is disabled by default.

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

Use **SNMPv1 Access** to enable or disable SNMP 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 15 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 and SETS at any time
  - **Write+:** Legacy mode that operates the same as Write
  - **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.

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

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

**NOTE:** SNMP is disabled by default.

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

For more information on management information document, see InRow ACRD100 and ACRD200 Series 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:** A phrase of 15 to 32 ASCII characters (`apc auth passphrase` by default) 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:** A phrase of 15 to 32 ASCII characters (`apc crypt passphrase` by default) 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 SHA and MD5 authentication. One of these must be selected.
- **Privacy Protocol:** The implementation of SNMPv3 supports 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 ACRD100 and ACRD200 Series 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 9600 (default) or 19200.
  - **Parity Bit** is the check bit and can be set to Even, Odd or None.
  - **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 ACRD100 and ACRD200 Series 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. (1000–30,000 ms)
- **APDU Retries:** The number of BACnet requests attempts that the unit will make before aborting the request. (1–10)

- **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.

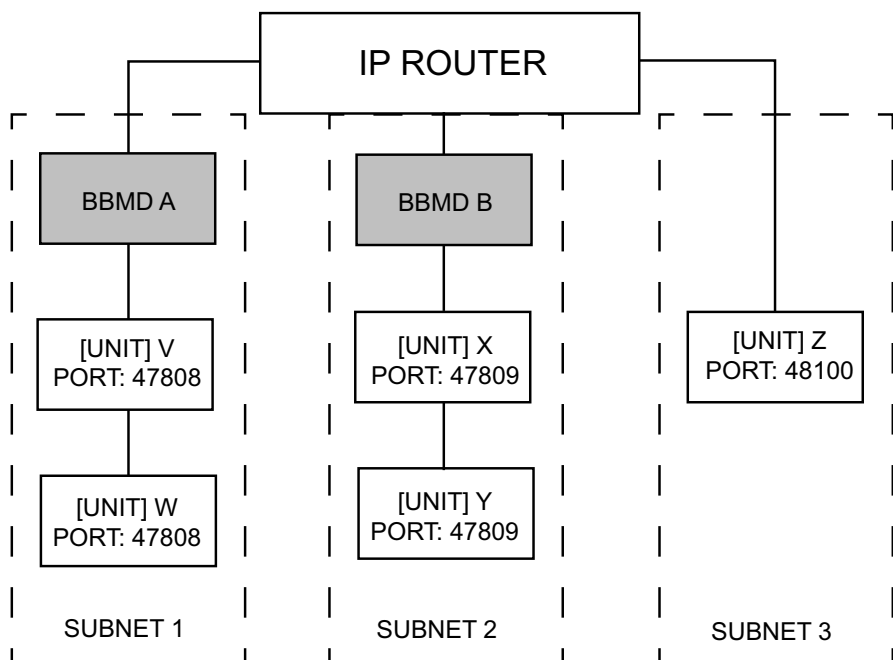
## BACnet/IP

- **Local Port:** The UDP/IP port that the unit uses to send and receive BACnet/IP messages. (5000–65,535)

**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 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.
- **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 52 for information on how to configure and use this data logging option.

- Queries (SNMP GETs)



For more information, see [SNMP Trap Receiver Configuration](#), page 49 and [SNMP Traps Test Configuration](#), page 49. 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 49 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 45).

## 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 52.
- See [E-Mail Notification Configuration](#), page 47.
- See [SNMP Trap Receiver Configuration](#), page 49.

## 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 52.

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**.
- 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 contents of the **From** field in e-mail messages sent by the cooling unit:
  - In the format `user@[IP_address]` (if an IP address is specified as Local SMTP Server)
  - In the format `user@domain` (if DNS is configured and the DNS name is specified as Local SMTP Server) in the e-mail messages

**NOTE:** The local SMTP server may require that you use a valid user account on the server for this setting. See the server documentation.
- **SMTP Server:** The IPv4/ IPv6 address or DNS name of the local SMTP server.
 

**NOTE:** This definition is required only when the SMTP server is set to Local.
- **Port:** The SMTP port number, with a default of 25. The range is 1–65535.
- **Authentication:** Enable this if the SMTP server requires authentication.

- **User Name, Password, and Confirm Password:** If your mail server requires authentication, enter your user name and password here. This performs a simple authentication, not SSI.
- **Use SSL/TLS:** Select when encryption is used.
  - **Never:** The SMTP server does not require nor support encryption.
  - **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.
  - **Always:** The SMTP server requires the STARTTLS command to be sent on connection to it.
  - **Implicitly:** The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server.
- **Require CA Root Certificate:** This should only be enabled if the security policy of your organization does not allow for implicit trust of SSL connections. If this is enabled, a valid root CA certificate must be loaded onto the unit for encrypted e-mails to be sent.
- **File Name:** This field is dependent on the root CA certificates installed on the unit and whether or not a root CA certificate is required.

## 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.
- **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. These settings are independent of the settings given under **SMTP Server**.

## E-mail SSL Certificates

### Path: Main > Configuration > Notification > E-mail > SSL Certificates

Load a mail SSL certificate on the unit for greater security. The file must have an extension of .crt or .cer. Up to five files can be loaded at any given time.



When installed, the certificate details also display here. An invalid certificate will display “n/a” for all fields except **File Name**.

Certificates can be deleted using this screen. Any e-mail recipients using the certificate should be manually modified to remove reference to this certificate.

## 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 45 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), and the **Contact** (the person responsible for the device) used by

- The SNMP agent of the unit
- StruxureWare Data Center Expert or Ecostruxure™ IT gateway



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](http://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 StruxureWare Data Center Expert obtains its time settings by using StruxureWare 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 514.
- **Protocol:** Select either UDP or TCP.
- **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 45.

- **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 45.

## Syslog Test and Format Example

### Path: Main > Configuration > Logs > Syslog > Test

Send a test message to the Syslog servers (configured through ). 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.


### Event Log

By default, the log displays all events recorded during the last two days, starting with the latest events.

Additionally, the log records any event that sends an SNMP trap, except SNMP authentication failures, and abnormal internal system events.

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**.

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 FTP or SCP to Retrieve Log Files](#), page 59.

### 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 45.

## 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 [How to Use FTP or SCP to Retrieve Log Files](#), page 59. 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 29.

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 FTP or SCP to Retrieve Log Files

A Super User/Administrator or Device User can use FTP or SCP to retrieve a tab-delimited 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.

## Use SCP to Retrieve the Files

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



See [Console Settings](#), page 38.

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
```

## 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 44. 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 and password. For the Device User, the defaults are `device` for user name and `apc` for password.
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 Network

**Path: Main > About > Network**

## Hardware Factory

This hardware information is useful for troubleshooting problems with your unit. **Management Uptime** refers to the length of time this management interface has been running continuously; that is, the length of time since the unit has been warm or cold started.

The following information is displayed:

- **Model Number**
- **Serial Number**
- **Manufacture Date**
- **MAC Address**

## Network Management Card 3

This information is the serial number of the Network Management Card 3 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 ZIP 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 network 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](http://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 user 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 FTP or SCP 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.

### 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 **Administration** tab, **General** on the top menu bar, and **User Config File** on the left navigation menu. 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 FTP or SCP, 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 <i>number</i> .	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid value on line <i>number</i> .	
Configuration file warning: Invalid section on line <i>number</i> .	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 <i>number</i> .	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 64 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 62.

# 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) 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.

**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)

From any computer on the same network as the Network Management Card, ARP and Ping can be used to assign an IP address to the Network Management Card and then use Telnet to access the CLI of that Network Management Card and configure the other TCP/IP settings.

**NOTE:** After a Network Management Card has its IP address configured, Telnet can be used, without first using ARP and Ping, to access that Network Management Card.

1. Use the MAC address of the Network Management Card in the ARP command to define an IP address for the Network Management Card. For example, to define an IP address of `156.205.14.141` for a Network Management Card that has a MAC address of `00 c0 b7 63 9f 67`, use one of the following commands:

**NOTE:** Look on the nameplate of the unit for the MAC address. The MAC address is also available on the display interface at **Main > About > Display > Device**.

- Windows command format:

```
arp -s 156.205.14.141 00-c0-b7-63-9f-67
```

- LINUX command format:

```
arp -s 156.205.14.141 00:c0:b7:63:9f:67
```

2. Use Ping with a size of 113 bytes to assign the IP address defined by the ARP command. For the IP address defined in step 1, use one of the following Ping commands:

- Windows command format:

```
ping 156.205.14.141 -l 113
```

- LINUX command format:

```
ping 156.205.14.141 -s 113
```

3. Use Telnet to access the Network Management Card at its newly assigned IP address. For example,

```
telnet 156.205.14.141
```

**NOTE:** 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.

Select **Main > Configuration > Network > Console > Access**.

4. Use `apc` for both the user name and password.
5. Contact the network administrator to obtain the IP address, subnet mask, and default gateway for the Network Management Card.
6. 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
```

7. 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. Use `apc` for the user name and password.
7. Contact the network administrator to obtain the IP address, subnet mask, and default gateway for the Network Management Card.
8. 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
```

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

## 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                               v3.1.1.1
(c)Copyright 2024 All Rights Reserved  ACRPTK2g APP                               v3.1.1.1
-----
Name      : apc7BB611                               Date      : 05/09/2024
Contact   : Unknown                               Time      : 01:24:40
Location  : Unknown                               User      : Super User
Up Time   : 0 Days  0 Hours  41 Minutes           Stat      : P+N4+ N6+ A+
-----
IPv4      : Enabled                               IPv6      : Enabled
Ping Response : Enabled
-----
HTTP      : Enabled                               HTTPS     : Enabled
FTP       : Enabled                               Telnet    : Enabled
SSH/SCP   : Enabled                               SNMPv1    : Read/Write
SNMPv3    : Enabled
-----
Super User : Enabled                               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 network through this NMC. In the example above, the NMC uses the application firmware for a Unit.  
 Network Management Card AOS vx.x.x.x  
 acrptk2g APP vx.x.x.x
- Three fields identify the system name, contact person, and location of the NMC.  
 Name : apc7BB611  
 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 0 Hours 41 Minutes
- Two fields report when you logged in, by date and time.  
 Date : 05/09/2024  
 Time : 01:24:40
- 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 72 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:



Command Line Interface (CLI)

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:  
-----  
acrd
```

### 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:                TME21445
Serial Number:                BA2323000675
Hardware Revision:            3
Manufacture Date:             06/05/2023
MAC Address:                  28 29 86 7B B6 11
Management Uptime:           0 Days 0 Hours 12 Minutes

Application Module
-----
Name:                          acrptk2g
Version:                       v3.1.1.1
Date:                           May 10 2024
Time:                           01:28:43

APC OS (AOS)
-----
Name:                          aos
Version:                       v3.1.1.1
Date:                           May 10 2024
Time:                           01:28:43

APC Boot Monitor
-----
Name:                          boot
Version:                       v1.5.3.1
Date:                           Nov 13 2023
Time:                           09:32:57

Cooling
-----
Model:                          InRow RD100
Firmware Revision:             6.9.0
Serial Number:                 E12143000153
```

**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 all active warning alarms, type:

```
apc> alarmcount  
  
E000: Success  
  
AlarmCount: 3
```

**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
DHCP Cookie:    disabled
Vendor Class:   APC
Client ID:      28 29 86 7B B5 F3
User Class:     ACRPTK2G

```

**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).
-ps	<SSH port n>	Define the SSH port used to communicate with the (22 by default).
-b	2400   9600   19200   38400	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 enable the Telnet, type

```
apc> console -t
E000: Success
Telnet: enabled
```

**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:**

```

apc> date
E000: Success
Date: 05/09/2023
Time: 01:37:20
Format: mm/dd/yyyy
Time Zone: -05:00

```

**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

1024 May 10 1:28 apc_hw21_aos_
3.1.1.1.bin/
4983316 May 10 1:28 apc_hw21_
acrptk2g_3.1.1.1.bin
45000 May 9 1:38 config.ini

0 Sep 20 2023 db/
0 Sep 20 2023 ssl/
0 Sep 20 2023 ssh/
0 Sep 20 2023 logs/
0 Sep 20 2023 sec/
0 Sep 20 2023 fw1/
0 Sep 20 2023 email/
0 Sep 20 2023 eapol/
0 Sep 20 2023 certs/
0 Sep 20 2023 acsc/
```

**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>	System-hostname sync

**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.
-p	<private key passphrase>	Set the private key passphrase.

**Example:**

```
apc>eapol
E000: Success
Active EAPoL Settings
-----
Status:          disabled
Supplicant Name: NMC-Supplicant-28:29:86:7B:B5:F3
Passphrase:     <not set>
CA file Status:  File not found
Private Key Status: File not found
Public Key Status: File not found
Result:         Failed
```

**Error Message:** None

**email****Access:** Super User, Administrator**Description:** Configure email parameters.**Parameters:**

Option	Argument
-g [n]	<enable   disable> (Generation)
-t [n]	<To Address>
-o [n]	<long   short> (Format)
-l [n]	<Language Code>
-r [n]	<Local   recipient   custom> (Route)
Custom Route Option	
-f [n]	<From Address>
-s {n}	<SMTP Server>
-p [n]	<Port>
-a [n]	<enable   disable> (Authentication)
-u [n]	<User Name>
-w [n]	<Password>
-e [n]	<none   ifsupported   always   implicit> (Encryption)
-c [n]	<enable   disable > (Required Certificate)
-i [n]	<Certificate File Name>
n = Email Recipient Number 1, 2, 3, or 4	

**Example:**

```
apc> email -o2 short
E000: Success
```

**Error Message:** E000, E102

## 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:**

**Error Message:** E000, E100



## exit

See `bye`, `exit`, or `quit`, page 79.

## 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.
Enter 'YES' to continue or <ENTER> to cancel: YES
Please reboot system to complete this task.
Reboot required for change to take effect.

```

**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:
-----
acrd
```

### 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

## 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 1:**

```
apc> ledblink 1
E101: Command Not Found
Reboot required for change to take effect.
```

**Example 2:**

Command Line Interface (CLI)

---

```
apc> ledblink  
E102: Parameter Error  
Usage: ledblink -- Configuration Options  
ledblink <duration time in minutes>  
Reboot required for change to take effect.
```

**Error Message:** E101, 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_ZA1023006009.tarCompressing files
into c:/dbg/debug_BA2323000645.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
IPv6    4      auto  FE80::2A29:86FF:FE7B:B5F3/64  configured
IPv4    0      manual  manual 192.168.1.200/24  configured
IPv6    0      manual  ::1/128    configured
IPv4    0      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 83.

**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.

**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 1:**

```
apc> ping 192.168.1.50
Ping request timed out.
Ping request timed out.
Ping request timed out.
Ping request timed out.
Reboot required for change to take effect.
```

**Example 2:**

```
apc> ping 192.168.1.200
Reply from 192.168.1.200: time (ms) = <10
Reply from 192.168.1.200: time (ms) = <10
Reply from 192.168.1.200: time (ms) = <10
Reply from 192.168.1.200: time (ms) = <10
Reboot required for change to take effect.
```

---

**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 <a href="#">Port Speed</a> , page 20 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 79.

## radius

**Access:** Super User, Administrator

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

Additional authentication parameters for RADIUS servers are available in the Web UI of the .

For detailed information about configuring the RADIUS server, see the *Security Handbook*, available at [www.apc.com](http://www.apc.com).

**Parameters:**

Option	Argument	Description
-a	<local   radiusLocal   radius>	Configure RADIUS authentication:  local: RADIUS is disabled. Local authentication is enabled.  radiusLocal: RADIUS, then Local Authentication. RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used.  radius: RADIUS is enabled. Local authentication is disabled.
-p1 -p2	<server ip>	The IP address of the primary or secondary RADIUS server.
-o1 -o2	<server port>	The server port of the primary or secondary RADIUS server.  <b>NOTE:</b> RADIUS servers use port 1812 by default to authenticate users. The supports ports 1812, 5000 to 32768.
-s1 -s2	<server secret>	The shared secret between the primary or secondary RADIUS server and the .
-t1 -t2	<server timeout>	The time in seconds that the waits for a response from the primary or secondary RADIUS server.

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

```
apc> radius
E000: Success

Access:                               Local Only
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
Secondary Server Port:                  1812
Secondary Server Secret:                 <Password Hidden>
Secondary Server Timeout:                5
```

**Example 2:** To enable RADIUS and local authentication, type

```
apc> radius -a radiusLocal
E000: Success
```

**Example 3:** To configure a 10-second timeout for a secondary RADIUS server, type

```
apc> radius -t2 10
E000: Success
```

**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       Serial     Serial       00:15:36       1
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> <b>NOTE:</b> 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)
-i	<Certificate File Name>

**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
      Cert File:           <n/a>
```

**Error Message:** E000, E102

## snmp

**Access:** Super User, Administrator

**Description:** Enable or disable SNMP 1 or SNMP 3 and configure basic SNMP settings.

**Parameters:**

Option	Argument	Description
-c	<Community>	Identify the group of .
-a	<read   write   writeplus   disable>	Set the access level.
-n	<IP or Domain Name>	The host's name or address.
-S	<enable   disable>	Enable or disable the respective version of SNMP.

**Example:**

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

Access Control #:          2
Community:
Access Type:              disabled
Address:                  0.0.0.0

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

Access Control #:          4
Community:
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:                disabled

SNMPv3 User Profiles
    Index:                  1
    User Name:              apc snmp profile1
    Authentication:        None
    Encryption:            None

    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: apc snmp profile1  
Access: disabled  
NMS IP/Host Name: 0.0.0.0

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: <ul style="list-style-type: none"> <li>• enUS - English</li> <li>• deDe - German</li> <li>• ruRu - Russian</li> <li>• zhCn - Chinese</li> <li>• jaJa - Japanese</li> <li>• koKo - Korean</li> <li>• itIt - Italian</li> <li>• ptBr - Portuguese</li> <li>• frFr - French</li> <li>• esEs - Spanish</li> </ul>
-t{n}	<Trap Type> [snmpV1   snmpV3]	Specify SNMPv1 or SNMPv3.
-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:**

```
apc> snmptrap
E000: Success
```

```
No trap receivers
configured
```

**Error Message:** E000, E102

## 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
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAPj08FR
6csvrBvi fd/QEYDt4W2HgTWnkTG0vMBDQ+a
+EnZzaVosmqtKLAdXzFvxbYS7RXPfH9NbeC7Es fOp4vw
```

**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
```



**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.		
<b>NOTE:</b> 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 84.

**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 apcxxxxxxx.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. <b>NOTE:</b> Executing this option without an argument will display the current certificate in use.
- f	<File Name>	Display the specified certificate's fingerprint. <b>NOTE:</b> 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: 6d2374558c922b3f
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:
e2:6c:b6:52:3d:7c:13:66:2a:b2:63:25:0b:0b:31:5f:
ae:db:f9:10:fa:1a:01:4a:4d:a2:4e:b3:47:01:fb:c4
Y:
d4:ad:18:a5:8e:d0:4d:1e:5b:7c:0f:35:cf:aa:c0:2f:
73:42:d9:d5:da:ad:25:72:97:0b:87:af:1a:a1:07:77
Curve: P-256
Thumbprint: 0dcb8668ab71c3d41b400c3191cd1f74d344da8d
Fingerprint:
5d90bc379215a67fa3ffcde3fa3b5a833adf69135772288e8217c022f222360
```

## 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.  <b>NOTE:</b> If a value is defined with more than one word, the value must be enclosed in quotation marks. <b>NOTE:</b> These values are also used by StruxureWare Data Center Expert and the Rack's SNMP agent.
-c	<system-contact>	
-l	<system-location>	
-m	<system-message>	When defined, a custom message will appear on the log on screen for all users.
-s	<enable   disable>] (system-hostname sync)	Allow the host name to be synchronized with the system name so both fields automatically contain the same value.  <b>NOTE:</b> When enabling this feature, the system name identifier can no longer contain a space character (since it will be synchronized to the host name field).

**Example 1:**

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

**Example 2:**

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

**Error Message:** E000, E102

## tcpip

**Access:** Super User, Administrator

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

**Parameters:**

Option	Argument	Description
-i	<IP address>	Type the IP address of the using the format xxx.xxx.xxx.xxx
-s	<subnet mask>	Type the subnet mask for the .
-g	<gateway>	Type the IP address of the default gateway. <b>Do not</b> 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 will use.
-S	<enable   disable>	Enable or disable IPv4.

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

```
apc> tcpip
E000: Success
Active IPv4 Settings
-----
Active IPv4 Address:      192.168.1.200
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:            192.168.1.200
Subnet Mask:             255.255.255.0
Gateway:                 192.168.1.1
MAC Address:             28 29 86 7B B5 F3
Domain Name:             example.com
Host Name:               apc7BB5F3
```

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

```
apc> tcpip -i
E000: Success
IPv4 Address:            192.168.1.200
```

**Error Message:** E000, E102

## tcpip6

**Access:** Super User, Administrator

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

**Parameters:**



Command Line Interface (CLI)

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. <b>Do not</b> use the loopback address (::1) as the default gateway.
-d6	<router   statefull   stateless   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:         28 29 86 7B B5 F3
Gateway:             ::
IPv6 Manual Address: disabled
IPv6 Autoconfiguration: enabled
DHCPv6 Mode:        router controlled
```

**Error Message:** E000, E102

## user

**Access:** Super User, Administrator

**Description:** Configure the user name, password, and inactivity timeout for configured users. It is not possible to edit a user name; it must be deleted and then a new user created.

**Parameters:**

Option	Argument	Description
-n	<user>	Specify these options for a user.
-pw	<user password>	
-pe	<user permission>	
-d	<user description>	
-e	<enable   disable>	Enable overall access.
-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:**

```
apc> user -n apc
E000: Success
Access: Enabled
User Name: apc
Password: <hidden>
User Permission: Super User
Touch Screen: Enabled
Touch Screen: <hidden>
User Description: User Description
Session Timeout: 3 minutes
Serial Remote Authentication Override: Disabled
Event Log Color Coding: Enabled
Export Log Format: Tab
Temperature Scale: Metric
Date Format: mm/dd/yyyy
Language: English (enUs)
```

**Error Message:** E000, E102

**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   Network-only> (user permission)	Specify the user's permission level and account type.
-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.  <b>NOTE:</b> 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.
-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 SSL3.0   TLS1.0   TLS1.1   TLS1.2
-lsp	<enable   disable>	Enable or disable the limited status page.
-lsd	<enable   disable>	Enable or disable the limited status page as the default page.

**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.

## Wifi

**Access:** Super User, Administrator

**Description:** Enable or disable wi-fi and configure the Wi-Fi network's settings.

**NOTE:** This command requires the optional APC USB Wi-Fi Device (AP9834) to be inserted in a USB port of an AP9641/AP9643 card.

**IMPORTANT:** It is recommended that you do not download a config.ini file from a wired device

and upload the entire file to a Wi-Fi-enabled device. It is also not recommended to download a

config.ini file from a Wi-Fi-enabled device and push the entire file to a wired device unless the entire [NetworkWiFi] section is removed or commented out using semi-colons (for example; WiFi=enabled).

The [NetworkWiFi] section contains device settings specific to Wi-Fi use. These settings should not be uploaded to a wired device.

**Parameters:**

Option	Argument	Description
-s	<enable   disable>	Enable or disable Wi-Fi. Disabled by default. <b>NOTE:</b> Enabling/disabling Wi-Fi will disable/enable the wired LAN connection.
-n	<network name (SSID)>	Specify the network name (SSID) of the Wi-Fi network. The maximum length is 32 characters.
-t	WPA   WPA2- AES   WPA2- Mixed   WPA2- TKIP   WPA2- Enterprise	Specify the security type (authentication and encryption) of the Wi-Fi network.
-p	<wifi password>	Specify a password for the Wi-Fi network. The maximum length is 64 characters. <b>NOTE:</b> This is required for WPA, WPA2-AES, and WPA2-Mixed security types.
-eu	<WPA2- Enterprise user name>	The user name for WPA2-Enterprise authentication. The maximum length is 32 characters.
-ep	<WPA2- Enterprise user name>	The password for WPA2-Enterprise authentication. The maximum length is 32 characters.

Command Line Interface (CLI)

Option	Argument	Description
-eo	<WPA2-Enterprise outer identity>	Specify the WPA-2-Enterprise outer identity. This is an optional unencrypted identification used by the WPA-2-Enterprise server. For example: user@example.com or anonymous. The maximum length is 32 characters.
-fw	<path/file name>	Specify the firmware file to upgrade the APC USB Wi-Fi Device's firmware. This must be an .ism file located on a USB drive inserted into the USB port of the NMC.  <b>NOTE:</b> The Wi-Fi network will be unavailable during the firmware upgrade.

**Example 1:** To enable Wi-Fi and configure the Wi-Fi network's settings, type:

```
wifi -S enable -n NETGEAR06 -t WPA2-AES -p apc123
```

**Example 2:** To upgrade the APC USB Wi-Fi Device's firmware, type:

```
wifi -fw apc_uw01_wni_1-26-7.ism
```

## 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



# File Transfers

## Updating the Firmware

A software update includes latest software features, performance improvements and bug fixes.

Updating here means placing the module files on the unit, without requiring any installation procedure.

**NOTE:** If necessary, call Technical Support for any new software updates.

## Firmware Module Files

A firmware version has three modules, and they must be updated (that is, placed on the unit) in this order:

Module	Description
❶ Boot monitor (bootmon)	Roughly equivalent to the BIOS of a PC
❷ American Power Conversion Operating System (AOS)	Can be considered the operating system of the unit
❸ Application	Specific to the unit device type

(Each module contains one or more Cyclical Redundancy Checks (CRCs) to protect its data from corruption.)

The boot monitor module, the AOS, and the application file names share the same basic format:

```
apc_hardware-version_type_firmware-version.bin
```

- **apc:** Indicates the context.
- **hardware-version:** "hw0n" where 'n' identifies the hardware version on which you can use this file.
- **type:** Identifies which module.
- **version:** The version number of the file.
- **bin:** Indicates that this is a binary file.

---

# Troubleshooting

If necessary, call Technical Support describing the nature of the fault and its possible cause displayed on the control panel.



Schneider Electric  
35 rue Joseph Monier  
92500 Rueil Malmaison  
France

+ 33 (0) 1 41 29 70 00

[www.schneider-electric.com](http://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.

© 2018 – 2024 Schneider Electric. All rights reserved.

990-3632C-001