

# User's Guide

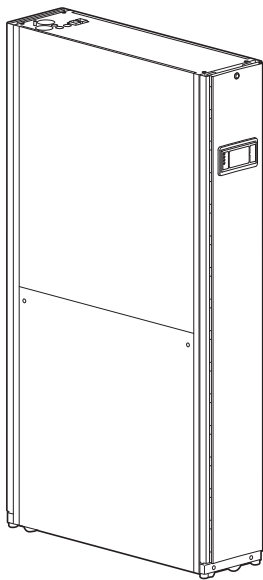
## InRow™ Chilled Water Air Conditioners

InRow™ RC

ACRC301S, ACRC301H

990-5567-001

Publication Date: January 2014



## Schneider Electric IT Corporation Legal Disclaimer

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

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

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

Copyright, intellectual, and all other proprietary rights in the content (including but not limited to software, audio, video, text, and photographs) rests with Schneider Electric It Corporation or its licensors. All rights in the content not expressly granted herein are reserved. No rights of any kind are licensed or assigned or shall otherwise pass to persons accessing this information.

This Publication shall not be for resale in whole or in part.

# Contents

---

Introduction.....	1
Product Description.....	1
Features.....	1
IPv4 initial setup.....	1
IPv6 initial setup.....	2
Network management with other applications.....	2
Internal Management Features.....	2
Overview.....	2
Access priority for logging on.....	2
Types of user accounts.....	3
Display Interface.....	4
LED Descriptions.....	5
Alarm LED.....	5
Status LED.....	5
Link-RX/TX (10/100) LED.....	5
How to Recover From a Lost Password.....	6
Watchdog Features.....	6
Overview.....	6
Network interface watchdog mechanism.....	6
Resetting the network timer.....	7
Web User Interface.....	8
Introduction.....	8
Overview.....	8
Supported Web browsers.....	8
How to Log On.....	8
Overview.....	8
URL address formats.....	9
Home Screen.....	10
Overview.....	10

# Monitoring the Status..... 11

## Unit Status.....11

Overview .....	11
Detailed Status .....	11
Unit Run Hours .....	12

## Group Status.....12

Overview .....	12
Group Units .....	13

## Network Status.....13

Current IPv4 Settings .....	13
Current IPv6 Settings .....	13
Domain Name System Status .....	13
Ethernet Port Speed .....	14

# Security and Network Control..... 15

## Managing User Sessions.....15

## Resetting the Network Interface.....15

# Configuring Your Settings..... 17

## Unit Configuration.....17

Unit thresholds .....	17
General unit settings .....	17
Input contacts configuration .....	18
Output relay screen .....	18

## Group Configuration.....19

Setpoints .....	19
Group Configuration .....	19

## Security Menu.....20

Session management screen .....	20
Ping response .....	21
Local Users .....	21
Remote users authentication .....	22
RADIUS screen .....	23
Configuring the RADIUS Server .....	23
Firewall Menus .....	24

Network Configuration Menu .....	24
TCP/IP settings for IPv4 screen .....	24
TCP/IP settings for IPv6 screen .....	25
DHCP response options .....	26
Port speed screen .....	27
DNS screen .....	28
Testing DNS screen .....	28
Web access screen .....	29
Web SSL certificate screen .....	29
Console screen .....	30
SNMP screens .....	31
Modbus .....	33
FTP server screen .....	34
 Notification Menu .....	 34
Types of notification .....	34
Configuring event actions .....	35
E-mail notification screens .....	37
SNMP trap receiver screen .....	39
SNMP traps test screen .....	40
Remote Monitoring Service .....	40
 General Menu .....	 40
Identification screen .....	40
Date/Time screen .....	41
Creating and importing settings with the configuration file .....	42
Configuring the links screen .....	42
 Logs in the Configuration Menu.....	 42
Identifying Syslog servers .....	42
Syslog settings .....	42
Syslog test and format example .....	43
 <b>Tests Menu .....</b>	 <b>44</b>
Setting the Active Flow Controller Lamp Test .....	44
Setting the Cooling Unit LED Lights to Blink .....	44
 <b>Logs and About Menus.....</b>	 <b>45</b>
Using the Event and Data Logs .....	45
Event log .....	45
Data log .....	46
Firewall Logs .....	48
How to use FTP or SCP to retrieve log files .....	49

About the Cooling Unit .....	51
About the cooling unit .....	51
About the cooling unit and the firmware modules .....	51
Support screen .....	51
<b>Device IP Configuration Wizard.....</b>	<b>52</b>
Capabilities, Requirements, and Installation .....	52
System requirements .....	52
Installation .....	52
<b>How to Export Configuration Settings.....</b>	<b>53</b>
Retrieving and Exporting the .ini File .....	53
Summary of the procedure .....	53
Contents of the .ini file .....	53
Detailed procedures .....	53
The Upload Event and Error Messages .....	55
The event and its error messages .....	55
Errors generated by overridden values .....	55
Related Topics .....	55
<b>File Transfers.....</b>	<b>57</b>
Upgrading Firmware .....	57
Firmware module files (InRow RC) .....	57
Firmware File Transfer Methods .....	57
Using the Firmware Upgrade Utility .....	58
Use FTP or SCP to upgrade one cooling unit .....	59
Use XMODEM to upgrade one cooling unit .....	60
Use a USB drive to transfer and upgrade the files .....	60
Upgrading the firmware on multiple cooling units .....	61
Verifying Upgrades .....	61
Verify the success of the transfer .....	61
Last Transfer Result codes .....	61
Verify the version numbers of installed firmware .....	62
<b>Troubleshooting .....</b>	<b>63</b>
Network Access Problems .....	63

SNMP Issues..... 64





# Introduction

---

## Product Description

### Features

The InRow Cooling ACRC301S and ACRC301H are Web-based, IPv6-ready products. They can manage supported devices using multiple open standards such as:

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

### 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 cooling unit.
- Supports using the Remote Monitoring Service (RMS).
- Provides the ability to export a user configuration (.ini) file from a configured cooling unit to one or more unconfigured cooling units.
- Provides a selection of security protocols for authentication and encryption.
- Communicates with StruxureWare Data Center Expert.
- 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 cooling unit before it can operate on the network:

- The IP address of the cooling unit
- The subnet mask of the cooling 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 the TCP/IP settings to their defaults.



For detailed information on how to use a DHCP server to configure the TCP/IP settings for a cooling unit, see “DHCP response options” on page 26.

## 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 the “TCP/IP settings for IPv6 screen” on page 25.

## Network management with other applications

These applications and utilities work with the cooling unit.

- PowerNet<sup>®</sup> Management Information Base (MIB) with a standard MIB browser — Perform SNMP SETs and GETs and receive SNMP traps.
- StruxureWare Data Center Expert — 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 cooling units over the network.
- Security Wizard — Create components needed to help with security for the cooling 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 cooling unit. You can also use SNMP to monitor the status of the cooling unit.

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



For more information about the UIs, see “Web User Interface” on page 7. See “SNMP screens” on page 31 for information about how SNMP access to the cooling unit is controlled. See “Modbus” on page 33 for information on Modbus access.

## 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 screen” on page 20.

## Types of user accounts

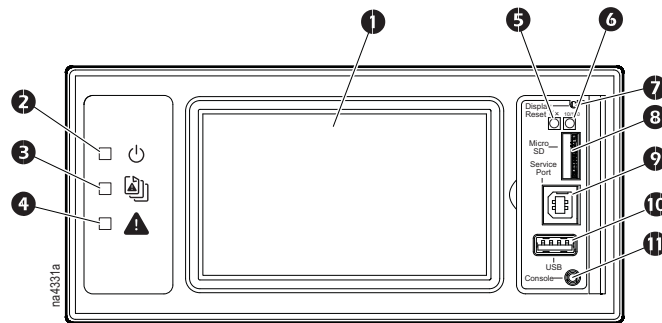
The cooling unit has various levels of access — Administrator, Device User, Read-Only User, and Network-only User — and these are protected by user name and password requirements.

- 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`.
- A Device User has read and write access to device-related screens. Administrative functions like **Session Management** under the **Security** menu and **Firewall** under **Logs** are grayed out.
  - The default user name is `device`, and the default password is `apc`.
- 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 (telnet not serial). A network-only user has read-write access to the network-related menus only. There is no default name and password.



To set User Name and Password values for the top three account types, see “Local Users” on page 21.

# Display Interface



Item	Description	Function
1	LCD display	4.3-in. touch-screen color display.
2	Power LED	The cooling unit is powered when the LED is illuminated. Unit firmware is updating when LED is blinking.
3	Check Log LED	When this LED is illuminated, a new entry has been made to the event log.
4	Alarm LED	Displays current alarm condition of unit.
5	Status LED	Displays current network management card status.
6	Link-RX/TX (10/100) LED	Displays current network link status.
7	Display Reset button	Resets the display microprocessor. This has no effect on the air conditioner controller.
8	Micro SD card slot	Memory card expansion slot.
9	Service port	USB-B port used only by service personnel.
10	USB-A port	Supports firmware upgrades.
11	Serial Configuration port	Connects the display to a local computer to configure initial network settings or access the command line interface (CLI).

# LED Descriptions

## Alarm LED

This LED indicates active alarms on the display.

Condition	Description
Off	No Alarms
Solid yellow	Warning Alarm
Solid red	Critical Alarm

## Status LED

This LED indicates the status of the display.

Condition	Description
Off	One of the following situations exist: <ul style="list-style-type: none"><li>• The display is not receiving input power.</li><li>• The display is not operating properly. It may need to be repaired or replaced. Contact Schneider Electric Customer Support.</li></ul>
Solid green	The display has valid TCP/IP settings.
Solid orange	A hardware malfunction has been detected in the display. Contact Schneider Electric Customer Support.
Flashing green	The display does not have valid TCP/IP settings.
Flashing orange	The display is making BOOTP requests.
Alternately flashing green and orange	If the LED is flashing slowly, the display is making DHCP requests. If the LED is flashing rapidly, the display is starting up.

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

This LED indicates the network status of the display.

Condition	Description
Off	One or more of the following situations exist: <ul style="list-style-type: none"><li>• The display is not receiving input power.</li><li>• The cable or device that connects the cooling unit to the network is disconnected or not functioning properly.</li><li>• The display itself is not operating properly. It may need to be repaired or replaced. Contact Schneider Electric Customer Support</li></ul>
Solid green	The display is connected to a network operating at 10 megabits per second (Mbps).
Solid orange	The display is connected to a network operating at 100 Mbps.
Flashing green	The display is receiving or transmitting at 10 Mbps.
Flashing orange	The display is receiving data packets at 100 Mbps.

# How to Recover From a Lost Password

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

1. Select a serial port on the local computer, and disable any service that uses that port.
2. Connect the provided serial cable (part number 940-0299) 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 redisplayed, 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 cooling 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 cooling unit and to view the status of the cooling unit.



See “Web access screen” on page 29 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

You can use Microsoft® Internet Explorer® (IE) 7.x or higher (on Windows® operating systems only) or Mozilla® Firefox® 3.0.6 or higher (on all operating systems) to access the cooling unit through its UI. Other commonly available browsers might work but have not been fully tested.

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

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

## How to Log On

### Overview

You can use the DNS name or the System IP address of the cooling 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.



See also “Types of user accounts” on page 3.

When HTTPS is enabled, the cooling unit generates its own certificate. This certificate negotiates encryption methods with your browser. Refer to the Security Guide on the <http://www.apc.com> cooling unit web site for more details.



## URL address formats

Type the DNS name or IP address of the cooling unit in the Web browser's 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
"This page cannot be displayed."	Internet Explorer	Web access is disabled, or the URL was not correct.
"Unable to connect."	Firefox	




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

# Home Screen


## Overview


**Home.** On the **Home** screen of the Web user interface, you can view 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 cooling unit:

Symbol	Description
	<b>No Alarms:</b> No alarms are present.
	<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, which requires immediate action.

In the upper-right corner of every screen, the same icons report the cooling 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 the  icon 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 websites. By default, the links access the URLs for these Web pages:

- Link 1: APC Web Site
- Link 2: Testdrive Demo
- Link 3: APC Monitoring



To reconfigure the links, see “Configuring the links screen” on page 42.

# Monitoring the Status

---

The **Status** menu options report on the current state of the cooling unit and network.



You can configure your cooling unit and network using the **Configuration** menu options. See “Configuring Your Settings” on page 17.

## Unit Status

**Path: Main > Status > Unit**

This screen displays useful information about the cooling unit.

### Overview

**Operating Mode.** Identifies the operating mode of the cooling unit.

- **Standby:** The cooling unit is receiving power but not enabled for cooling.
- **On:** The cooling unit is cooling.
- **Idle:** The cooling unit is no longer cooling due to active alarms.
- **Maintenance:** Testing mode used by qualified service personnel.

**Rack Inlet Temperature.** The maximum temperature of the rack inlet temperature sensors connected to the unit.

**Supply Air Temperature.** The temperature of the air leaving the cooling unit.

**Return Air Temperature.** The temperature of the air entering the cooling unit.

**Dew Point Temperature.** The dew point of the environment (ACRC301H only).

**Airflow.** The velocity at which air flows into or out of the unit.

**Fan Speed.** The speed of the fans that regulate the airflow through the cooling unit.

**Cool Output.** The actual cooling output of the cooling unit.

**Cool Demand.** The output required of the cooling unit to meet the current heat load of the conditioned space.

**Unit Energy.** The electrical energy consumed by the unit since the last Reset Unit Energy command (**Main > Configuration > Unit > Unit Configuration**).

**Unit Power.** The electrical power being consumed by the cooling unit.

### Detailed Status

**Chilled Water Valve Position.** The position of the valve that controls how much chilled water enters the cooling unit.

**Chilled Water Flow.** The rate at which chilled water flows through the cooling unit.

**Entering Chilled Water Temperature.** The temperature of the chilled water as it enters the cooling unit.

**Leaving Chilled Water Temperature.** The temperature of the chilled water as it leaves the cooling unit.

**Coil Chilled Water Temperature.** The temperature of chilled water entering the coil (ACRC301H only).

**Standby Input State.** The current state of the input. If the input is in an abnormal state, an alarm will occur and the unit will stop cooling.

**Output 1-4 State.** The current state of the four output relays.

**Filter Differential Pressure.** The difference in air pressure across the air filter.

**Active Power Source.** The power source being used by the unit. The unit supports a redundant power input.

## Unit Run Hours

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

- **Unit**
- **Condensate Pump (ACRC301S only)**
- **Circulation Pump (optional for ACRC301H only)**
- **Fan Power Supply 1-2**
- **Air Filter**  
**NOTE:** When the air filter is replaced, use the **Air Filter Serviced** button to reset the maintenance alarm.
- **Fan 1-8 (Fan 1 is the bottom fan; Fan 8 is the top fan)**

## Group Status

**Path: Main > Status > Group**

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

### Overview

**Cool Output.** The actual cooling output of the cooling group.

**Cool Demand.** The output required to meet the current heat load of the conditioned space.

**Cool Setpoint.** The temperature setting that the air entering the rack should maintain (InRow, CACS modes only).

**Airflow.** The total airflow output of the cooling units in the cooling group.

**Maximum Rack Inlet Temperature.** The highest rack temperature reported by any cooling unit in the cooling group.

**Minimum Rack Inlet Temperature.** The lowest rack temperature reported by any cooling unit in the cooling group.

**Active Flow Control Status.** Indicates whether the correct amount of airflow is being provided to the load. Status can be one of the following:

- **Over:** Airflow provided by the cooling units is more than the load requires.
- **Okay:** Airflow provided by the cooling units is equal to what the load requires.
- **Under:** Airflow provided by the cooling units less than the load requires.
- **N/A:** The cooling units are not using the Active Flow Controller.

## Group Units

**Name.** The names of cooling units in this group.

**Location.** The physical location of cooling units in this group.

**App Version.** The application version of the display of cooling units in the group.

**IP Address.** The IP addresses of cooling units in this group.

## Network Status

**Path: Main > Status > Network**

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

### Current IPv4 Settings

**System IP.** The IP address of the unit.

**Subnet Mask.** The IP address of the sub-network.

**Default Gateway.** The IP address of the router used to connect to the network.

**MAC Address.** The MAC address of the 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.

#### Ethernet 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.

## Managing User Sessions

**Path: Main > Control > Security > Session Management**

The **Session Management** menu displays all active users currently connected to the cooling 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.

## Resetting 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).





# Configuring Your Settings

---

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

## Unit Configuration

Under the **Configuration > Unit** menu, several options are available to make changes to the cooling unit.

### Unit thresholds

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

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

**Rack Inlet Temperature High Threshold.** The air entering the rack at the temperature sensor.

**Supply Air Temperature High Threshold.** The air leaving the cooling unit.

**Return Air Temperature High Threshold.** The air entering the cooling unit.

**Entering Chilled Water High Temperature Threshold.** The chilled water entering the cooling unit.

### General unit settings

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

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

**Startup Delay.** The delay begins when the cooling unit is started and initialized. The cooling unit cannot begin operation until this delay has expired. 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 Detected Error** activates. Set to **No** to disable the cooling unit from entering idle mode if a leak is detected.

**Idle on Cool Fail.** When set to **Yes**, the cooling unit will enter idle mode if the cooling unit is unable to supply conditioned air. Set to **No** to disable the cooling unit from entering idle mode if a cooling failure is detected.

**Bypass Valve Position.** Reflects the position of the manual bypass valve. This setting must match the physical setting of the valve. When the bypass valve is closed, the maximum chilled water flow is limited via the **Maximum Chilled Water Flow** setting.

**Air Filter.** The number of hours the air filter has been in operation.

**Air Filter Serviced.** Select this check box to reset an **Air Filter Run Hours Violation** or air filter status after the physical air filter is cleaned or replaced.

**Air Filter Service Alarm Enable.** **Enable** or **Disable** the air filter service alarm.

**Air Filter Service Interval.** Enter the number of weeks between air filter service alarms.

**Air Filter Type.** The type of air filter installed in the cooling unit: **Standard** or **Pleated**.

**Maximum Chilled Water Flow.** Restricts the maximum chilled water flow rate of the unit. This setting is only used when the bypass valve is closed. The input range is 0-100 gallons per minute (0-379 liters per minute). Only qualified service personnel can make changes to this setting.

**Chilled Water Valve Control.** The setting used to determine chilled water flow. When **Automatic** is selected, the unit operates based on measured demand. Only qualified service personnel can make changes to this setting.

**Power Source.** Indicates the number of power sources connected to the cooling unit. Select **Single** when using one power connection. Select **Dual** when using two power connections.

**Number of Rack Inlet Temp Sensors in Unit.** The number of expected rack inlet sensors for the unit. The maximum number of rack inlet temperature sensors is four.

**Number of Leak Detectors in Unit.** The number of expected leak detectors in the unit. The maximum number of leak detectors is four.

**Unit Service Alarm Enable.** **Enable** or **Disable** the unit service alarm. Only qualified service personnel can make changes to this setting.

**Unit Service Alarm Interval.** Enter the number of weeks between unit service alarms. Only qualified service personnel can make changes to this setting.

**Unit Energy.** The electrical energy consumed by the unit since the last time the **Unit Energy** has been reset or the cooling unit has been powered on.

**Reset Unit Energy.** Select this check box to reset the **Unit Energy**.

## Input contacts configuration

**Path: Main > Configuration > Unit > Input Contacts**

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

## Output relay screen

**Path: Main > Configuration > Unit > Output Relays**

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

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

# Group Configuration

**Path:** Main > Configuration > Group

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

## Setpoints

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

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

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

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

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

**Delta-T Setpoint.** When the group is programmed for HACS or RACS mode and an AFC is not being used, this property specifies the desired temperature difference across the equipment from the following options.

- 10°F/5.6°C
- 15°F/8.3°C
- 20°F/11.1°C
- 25°F/13.9°C
- 30°F/16.7°C
- 35°F/19.4°C
- 40°F/22.2°C

## Group Configuration

**Number of Units in Group.** Indicates the number of cooling units in this cooling group. Up to twelve cooling units can be joined together to work as a single cooling group.

**Configuration Type.** The airflow control strategy for the cooling units of this cooling group. Only qualified service personnel can make changes to this setting.

- **In-Row:** Air flow is horizontal to allow in-row operation of the cooling. The loads share a common open cold aisle.
- **HACS (Hot Aisle Containment System):** Air flow in the room is controlled by enclosing the hot air aisle. The loads share an enclosed common hot aisle. This is not a sealed system.
- **RACS (Rack Air Containment System):** Air flow in the enclosure is controlled by a ducting system fitted to the enclosure. This is not a sealed system.
- **CACS (Cold Aisle Containment System):** Air flow in the room is controlled by enclosing the cold air aisle. The loads share an enclosed common cold aisle. This is not a sealed system.

**Percent Glycol.** This specifies the percentage of glycol by volume in the chilled water. This setting affects how cooling output is reported. Only qualified service personnel can make changes to this setting.

**Maximum Fan Speed.** Defines the maximum speed at which the fans in the unit operate when in **Auto** mode.

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

**Number of Active Flow Controllers.** Sets number of AFC units in the group (0 to 5).

**Active Flow Control Bias.** This setting is used to control the difference between the cooling airflow and the airflow of the load as measured by the Active Flow Controller(s). A setting of **Zero** will control the fans to match the airflow of the load. A setting of **Positive** will provide more cooling airflow than required by the load. A setting of **Negative** will provide less cooling airflow than required by the load. Only qualified service personnel should make changes to these settings.

**Altitude.** Set the altitude (in feet or meters) of the cooling unit above sea level. This number is used to estimate the density of air and is a factor in pressure measurement.

**Airflow control.** When **Automatic** is selected, the cooling unit operates based on measured demand. When set to **60%, 70%, 80%, 90%, 100%**, the fans will operate at the selected output.

**Cool Gain “P”.** The proportional multiplier (gain) for this mode or actuator. The proportional multiplier adjusts for the difference (error) between the measured temperature and the setpoint. The proportional multiplier is expressed in percent of output per unit error. Only qualified service personnel can make changes to this setting.

**Cool Derivative “D”.** The derivative multiplier (derivative) for this mode or actuator. The derivative multiplier adjusts the output for rapid changes in the error, correcting for the rate of change of the error over time. It is expressed in percent of output for each unit of error per minute (error divided by minutes). Only qualified service personnel can make changes to this setting.

**Cool Reset Rate “I”.** The integral multiplier (reset rate) for this mode or actuator. The integral multiplier adjusts for error measurement and for the amount of time that the error has existed. The integral multiplier adds to or subtracts from the output in small increments to correct for the offset error caused by the proportional contribution. It is expressed in percent of output for each minute and unit of error (error multiplied by minutes). Only qualified service personnel can make changes to this setting.

## Security Menu

Session management screen

**Path: Main > Configuration > Security > Session Management**

Enabling **Allow Concurrent Logins** means that 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 cooling unit supports remote authentication dial-in user service (RADIUS) storage of passwords on a server. However, if you enable this override, the cooling unit will allow a user with **Serial Remote Authentication Override** enabled to log on using the password for local authentication. See also “Local Users” on page 21 and “Remote users authentication” on page 22.

**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 cooling unit user interfaces. This applies to users as defined by their logon name.

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

From this menu, an administrator or super user can view the users allowed access to the UI. Click on the name link 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.

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

**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.

**Serial Remote Authentication Override.** The cooling unit will allow a user with this enabled to log-on to the cooling unit using the password for local authentication. **Remote Authentication Override** must be enabled on the **Configuration > Security > Session Management** screen for this to function.

**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 considered informational events.)
- **Export Log Format:** Exported log files can be formatted using CSV (comma-separated values) or tab-delimited.



See “Event log” on page 45 for more 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 screens” on page 37 and “SNMP trap receiver screen” on page 39.

#### **Path: Main > Configuration > Security > Local Users > Default Settings**

Setting up defaults can make adding users quicker. Use this option to set defaults for the options on the **Management** screen. A remote RADIUS user will also use these default settings.

#### Remote users authentication

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

**Authentication.** 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 cooling 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 cooling unit.

Select one of the following:

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



See “Local Users” on page 21.

- **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 screen

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

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

- List the RADIUS servers (a maximum of two) available to the cooling 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 cooling unit.

**Reply Timeout.** The time in seconds that the cooling 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 cooling unit to the RADIUS server client list (file).

1. 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).
2. VSAs can be used instead of the Service-Type attributes provided by the RADIUS server.
3. VSAs require a dictionary entry and a RADIUS user's file. In the dictionary file, define the names for the ATTRIBUTE and VALUE keywords, but not for the numeric values. If you change numeric values, RADIUS authentication and authorization will not work. VSAs take precedence over standard RADIUS attributes.

**Configuring a RADIUS server on UNIX<sup>®</sup> 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 Menus

**Path: Main > Configuration > Security > Firewall**

**Configuration.** Enable or disable the overall firewall functionality. Any configured policy is also listed, even if the firewall is disabled.

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

**Active Rules.** When a firewall is enabled, this lists the individual rules that are being enforced by a current active policy. You can edit existing rules and add or delete new rules here.

**Create/Edit Policy.** Create a new policy or edit an existing one.

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

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

## Network Configuration Menu

### TCP/IP settings for IPv4 screen

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

This option displays any current IPv4 address, subnet mask, default gateway, MAC address, and boot mode of the cooling 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), by default it uses the previously configured settings. This ensure 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 screen

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

This option displays any current IPv6 settings of the cooling unit. Use the lower part of the screen to configure those settings, including disabling IPv6.

You have a choice 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
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 cooling unit checks whether the M and O flags are set. The cooling 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 cooling 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”. Once the M flag has been received, the DHCPv6 address configuration stays in effect until the interface in question has been closed, even if subsequent Router Advertisement packets are received in which the M flag is not set. If an O flag is received first, then an M flag is received subsequently, the cooling unit performs full address configuration upon receipt of the M flag.</li> <li>• <b>Only O is set:</b> In this situation, the cooling 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 cooling unit needs in order to operate on a network. Each response also has other information that affects the operation of the cooling unit. See also ID FA156110 at <http://www.apc.com/site/support/index.cfm/faq/index.cfm>.

**Vendor Specific Information (option 43).** The cooling 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 cooling 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 cooling 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 cooling unit.
- **Subnet Mask** (option 1): The Subnet Mask value that the cooling unit needs to operate on the network.
- **Router**, i.e., Default Gateway (option 3): The default gateway address that the cooling 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 cooling unit.
- **Renewal Time**, T1 (option 58): The time that the cooling 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 cooling unit must wait after an IP address lease is assigned before it can seek to rebind that lease.

**Other options.** The cooling unit also uses these options within a valid DHCP response. All of these options except the last are described in RFC2132.

- **Network Time Protocol Servers** (option 42): Up to two NTP servers (primary and secondary) that the cooling unit can use.
- **Time Offset** (option 2): The offset of the cooling unit's 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 cooling unit can use.
- **Host Name** (option 12): The host name that the cooling unit will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the cooling 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 cooling unit will download the .ini file. After the download, the cooling unit uses the .ini file as a boot file to reconfigure its settings.

## Port speed screen

**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 choose 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 screen

**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 the **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 cooling unit to send email, you must at least define the IP address of the primary DNS server.

- The cooling unit waits up to 15 seconds for a response from the primary DNS server or the secondary DNS server. If the cooling unit does not receive a response within that time, email cannot be sent. Use DNS servers on the same segment as the cooling 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 hostname with the cooling 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 cooling unit interface (except e-mail addresses) that accepts a domain name.

**Domain Name (IPv4/IPv6).** For the cooling unit 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 cooling 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 cooling 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.

## Testing DNS screen

**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 table below.
- For **Query Question**, specify the value to be used for the selected query type as explained in the table.

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

## Web access screen

**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 cooling unit user interface.

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

**HTTPS.** Select this check box to enable access through HTTPS. HTTPS encrypts user names, passwords, and data during transmission.

**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`.

**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 screen

**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 cooling 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 cooling unit.
- **Generating:** The cooling unit is generating a certificate because no valid certificate was found.
- **Loading:** A certificate is being activated on the cooling unit.

**IMPORTANT:** If you install an invalid certificate, or if no certificate is loaded while SSL is enabled, the cooling 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 screen

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

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

You can enable access to the CLI through either **Telnet** or **SSH** or through both, by using the Enable check boxes. Telnet does not encrypt user names, passwords, and data during transmission whereas SSH 2 does.

For the ports to be used to communicate with the cooling 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. See also “SSH Host Key” below.

**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 cooling unit is creating a host key because no valid host key was found.
- **Loading:** A host key is being activated on the cooling unit.
- **Valid:** One of the following valid host keys is in the /ssh directory (the required location on the cooling unit):
  - A 1024-bit or 2048-bit host key created by the Security Wizard
  - A 2048-bit RSA host key generated by the cooling 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 (with “Console access” above).

**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 cooling 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.

## SNMP screens

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

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

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

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

**Access Control.** You can configure up to four access control entries to specify which Network Management Systems (NMSs) have access to the cooling 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 cooling 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, and the default names are public, private, public2, and private2.

**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.

#### **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 cooling unit supports SHA or MD5 authentication and AES or DES encryption.

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

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

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

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



**Authentication Passphrase.** A phrase of 15 to 32 ASCII characters (`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 Passphrase.** 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.

#### **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 cooling 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 choices available are the four user names that you configure through the **User Profiles** option.

**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

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

Configure the Modbus by enabling **Serial** or **TCP Access** and adding the required values.

**Path:** Main > Configuration > Network > Modbus > Serial

**Baud Rate.** Choose either 9600 bps or 19200 bps.

**Parity.** Choose either Even, Odd, or None.

**Target Unique ID.** Each Modbus device must have a unique target identification number. Enter a unique number (between 1 and 247) for the cooling unit.

**Path:** Main > Configuration > Network > Modbus > TCP

**Port.** Enter a port: 502, 5000-32768

FTP server screen

**Path:** Main > Configuration > Network > FTP Server

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

**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:** 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 Network Management Card interface of that cooling 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 “Logs in the Configuration Menu” on page 42 for information on how to configure and use this data logging option.

– Queries (SNMP GETs)



For more information, see “SNMP trap receiver screen” on page 39 and “SNMP traps test screen” on page 40. 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 cooling unit supports the use of the **RFC1628 MIB** (Management Information Base). See “SNMP trap receiver screen” on page 39 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 Pownet MIB. They can be configured like any event (see “Configuring event actions” on this page).

## Configuring event actions

**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.  
Or you can click on a sub-category under these headings, like **Security** or **Temperature**.
2. 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:

- “Identifying Syslog servers” on page 42
- “Path: Main > Configuration > Notification > E-mail > Recipients” on page 38
- “Path: Main > Configuration > Notification > SNMP Traps > Trap Receivers” on page 39

**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:
  - a. 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 “Logs in the Configuration Menu” on page 42.

3. Click **Next** to move to the next screen to do the following:
  - a. If you selected **Logging** on the previous screen, select **Enable Notifications** or **Disable Notification**.
  - b. If you selected **Email Recipients** on the previous screen, select the e-mail recipients to configure.
  - c. 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:
  - a. 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.
  - b. If you are configuring **Email Recipients** or **Trap Receivers**, select **Enable Notifications** or **Disable Notification** and set the notification timing settings (see “Notification parameters” on page 36 for more information on these settings).
5. Click **Next** to move to the next screen to do the following:
  - a. 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.



See “Configuring event actions” on page 35.

They are usually accessed by clicking the receiver or recipient name.

Field	Description
Delay <i>n</i> 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.

Field	Description
Repeat at an interval of <i>n</i>	The notification is sent repeatedly at the specified interval (the default is every 2 minutes until the condition clears).
Up to <i>n</i> 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 `RC: Fan 2 Error Detected` and `RC: Fan 2 Error Corrected`.)

## E-mail notification screens

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.

**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**.

**Authentication.** Enable this if the SMTP server requires authentication.

**Port.** The SMTP port number, with a default of 25. The range is 1–65535.

**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 doesn't 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 cooling unit for encrypted e-mails to be sent.

**File Name.** This field is dependent on the root CA certificates installed on the cooling unit and whether or not a root CA certificate is required.

**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 e-mail address for the recipient's 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 e-mail 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 cooling 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" above.

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

Load a mail SSL certificate on the cooling 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.

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

Send a test message to a configured recipient.

## SNMP trap receiver screen

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

With Simple Network Management Protocol (SNMP) traps, you can automatically get notifications for significant cooling 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 (“public” by default) 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” for the deleted trap receiver are set to their default values.

## SNMP traps test screen

**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.

## Remote Monitoring Service

**Path: Main > Configuration > Notification > Remote Monitoring**

The remote monitoring service (RMS) is an optional service from Schneider Electric that monitors your system from a remote operation center 24 hours a day, 7 days a week, and notifies you of device and system events.



To purchase the RMS service, contact your vendor or click on the link on the top part of this screen: [APC RMS Web site](#).

**Registration.** Once you have purchased the service, you activate RMS for the cooling unit. Select **Enable APC Remote Monitoring Service**, select **Register Company and Device** or **Register Device Only**, complete the form, and click **Apply**.

Use the **Reset APC Remote Monitoring Service Registration** check box to discontinue the service, whether permanently or temporarily (for example, if you are moving a cooling unit).

## General Menu

This menu contains miscellaneous configuration items including device identification, date and time, exporting and importing your cooling 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 cooling unit and
- StruxureWare Data Center Expert.





Specifically, the name field is used by the **sysName**, **sysContact**, and **sysLocation** object identifiers (OIDs) in the SNMP agent of the cooling unit. For more information about MIB-II OIDs, see the PowerNet<sup>®</sup> *SNMP Management Information Base (MIB) Reference Guide*, available at [www.apc.com](http://www.apc.com).

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

## Date/Time screen

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

Set the time and date used by the cooling 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 cooling 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 cooling unit. By default, any cooling 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 cooling 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.

**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), choose 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, choose Fifth/Last.

## Creating and importing 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*.

## Configuring 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**.

# Logs in the Configuration Menu

## Identifying 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 cooling unit.

**Port.** The user datagram protocol (UDP) port that the cooling unit will use to send Syslog messages. The default UDP port assigned to Syslog is 514.

**Language.** Select the language for any Syslog messages.

**Protocol.** Select either UDP or TCP.

## 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” on page 35.

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

**NOTE: User** best defines the Syslog messages sent by the cooling 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 cooling 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” on page 35.

## Syslog test and format example

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

Send a test message to the Syslog servers (configured through the “Identifying Syslog servers” option above). 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 cooling unit.
- The Header: a time stamp and the IP address of the cooling 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 Menu

---

## Setting the Active Flow Controller Lamp Test

**Path:** Main > Tests > Active Flow Controller > Lamp Test

Set the state of the AFC lamp to **On** or **Off**. When the state is set to **On**, an LED test on all AFCs in the group will be performed: the color of the LED status lights will cycle from green to blue to red. The AFCs will remain in the test state until the state is set to **Off**. You can use this command to verify the connections to the AFCs in the group.

## Setting the Cooling Unit LED Lights to Blink

**Path:** Main > Tests > Network > LED Blink

If you are having trouble finding your cooling 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

---

## Using the 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.

**Path: Main > Logs > Events > Log**

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” on page 49.

**Filtering event logs.** Use filtering to omit information you don't want to display.

- Filtering the log by date or time: Use the **Last** or **From** radio buttons. (The filter configuration is saved until the cooling unit restarts.)
- Filtering the log by event severity or category:
  - Click **Filter Log**.
  - Clear a check box to remove it from view.
  - 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 cooling unit restarts.
- Removing an active filter:
  - Click **Filter Log**.
  - Click **Clear Filter (Show All)**.
  - As Administrator, click **Save As Default** to save this filter as the new default log view for all users.

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.

**Deleting event logs.** 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” on page 35.

**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.

**Path: Main > Logs > Events > Size**

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

**CAUTION:** When you resize 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.

## Data log

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

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

**Path: Main > Logs > Data > Log**

**Filtering data logs.** Use filtering to omit information you don't want to display.

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

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

**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.

**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<sup>®</sup> 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 Data .** Select the data items that correspond to the abbreviated column headings in the data log to graph multiple data items. Hold down **CTRL** to select multiple items.

**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 Graph in New Window** to launch the data log graph in a new browser window that provides a larger view of the graph.

### 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 *mmdyyy\_<filename>.txt*, where filename is what you specified in the **Filename** field above. 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.
  - **Up to *n* times:** 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.

### Path: Main > Logs > Data > Size

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

**CAUTION:** 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 Logs

### 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 Menus” on page 24.

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 (see “Event log” on page 45).

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-delineated event log file (*event.txt*) or data log file (*data.txt*) and import it into a spreadsheet. Both reside on the cooling 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 cooling unit
  - The unique **Event Code** for each recorded event (*event.txt* file only)
  - The cooling unit uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits.



If you are using the encryption-based security protocols, see “To use SCP to retrieve the files” on page 49. If you are using unencrypted authentication methods for security, see “To use FTP to retrieve the files” on page 49.

**To use SCP to retrieve the files.** Enable SSH on the cooling unit (see “Console screen” on page 30“).

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
```

**To 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 cooling 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 screen” on page 34. 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 Cooling Unit

About the cooling unit

**Path: Main > About > Device**

The information displayed under cooling unit varies according to the device used.

**Display.** Gives information about the display unit including the **Name, Location, Application Version,** and **OS Version.**

**Controller.** Gives information about the controller including the **Model Number, Serial Number, Firmware Revision,** and **Hardware Revision.**

About the cooling unit and the firmware modules

**Path: Main > About > Network**

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

**Application Module, APC OS (AOS), and APC Boot Monitor.** This information is useful for troubleshooting and for determining if updated firmware is available, [www.apc.com/tools/download](http://www.apc.com/tools/download).

- **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.

Support screen

**Path: Main > About > Support**

With this option, you can consolidate various data in this interface into a single zipped 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 zipped file.

# Device IP Configuration Wizard

---

## Capabilities, Requirements, and Installation

The Device IP Configuration Wizard can discover cooling units that do not have an IP address assigned. Once discovered, you can configure the IP address settings for the cards.

You can also search for devices already on the network by entering an IP range to define the search. The Utility scans the IP addresses in the defined range and discovers cooling units that already have a DHCP-assigned IP address.



For detailed information on the Utility, see the Knowledge Base on the support page of the [www.apc.com](http://www.apc.com) website and search for 3061 (the ID of the relevant article).

To use the DHCP Option 12 (AOS 5.1.5 or higher), see Knowledge Base ID FA156110.

### System requirements

The Device IP Configuration Wizard runs on Microsoft® Windows® 2000, Windows Server® 2003, Windows Server® 2012, and on 32- and 64-bit versions of Windows XP, Windows Vista, Windows 2008, Windows 7, and Windows 8 operating systems.

The Device IP Configuration Wizard supports cards that have firmware version 3.0.x or higher and is for IPv4 only.

### Installation

To install the Device IP Configuration Wizard from a downloaded executable file

1. Go to <http://www.apc.com/tools/download>.
2. Download the Device IP Configuration Wizard.
3. Run the downloaded executable file.

When installed, the Device IP Configuration Wizard is available through the Windows Start menu options.

# How to Export Configuration Settings

---

## Retrieving and Exporting the .ini File

### Summary of the procedure

A Super User/Administrator can retrieve the .ini file of a cooling unit and export it to another cooling unit or to multiple cooling units. The steps are below; see details in the sections following.

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

Each receiving cooling unit uses the file to reconfigure its own settings and then deletes it.

### Contents of the .ini file

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

- Section headings and keywords (only those supported for the particular device from which you retrieve the file): **Section headings** are category names enclosed in brackets ([ ]). **Keywords**, under each section heading, are labels describing specific cooling 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. For example, 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 cooling 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 cooling unit:
  - a. Open a connection to the cooling unit using its IP address:

```
ftp> open ip_address
```

b. Log on using the Super User/Administrator user name and password.

c. Retrieve the `config.ini` file containing the settings of the cooling unit:

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

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



To retrieve configuration settings from multiple cooling units and export them to other cooling units, see Release Notes: ini File Utility, version 2.0, available at <http://www.apc.com>. Or see it in the Knowledge Base, <http://www.apc.com/site/support/index.cfm/faq/index.cfm>.

**Customizing.** You must customize the file before you transfer it to another cooling unit.

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 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.

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

**Transferring the file to a single cooling unit.** To transfer the `.ini` file to another cooling unit, do either of the following:

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

```
ftp> open ip_address
```

- b. Export the copy of the customized `.ini` file to the root directory of the receiving cooling unit:

```
ftp> put filename.ini
```

**Transferring the file to multiple cooling units.** Follow these steps:

1. Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single cooling unit.
2. Use a batch processing file and the `.ini` file utility.

# The Upload Event and Error Messages

## 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 cooling 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.

## 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” on page 53 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, 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 the cooling unit and configure other settings through its user interface.





# File Transfers

---

## Upgrading Firmware

When you upgrade the firmware on the cooling unit, you obtain the latest features, performance improvements, and bug fixes.

Upgrading here means simply placing the module files on the cooling unit; there is no installation required. Check regularly on <http://www.apc.com/tools/download> for any new upgrades.

### Firmware module files (InRow RC)

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

	Module	Description
1	boot monitor (bootmon)	Roughly equivalent to the BIOS of a PC
2	American Power Conversion Operating System (AOS)	Can be considered the operating system of the cooling unit
3	application	Specific to the cooling 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.

## Firmware File Transfer Methods

Upgrade the bootmon module first, then the AOS module, and finally, the application module by placing them on the cooling unit in that order.

Obtain the free, latest firmware version from [www.apc.com/tools/download](http://www.apc.com/tools/download). To upgrade the firmware of one or more cooling units, use one of these methods:

- On a Windows operating system, use the Firmware Upgrade Utility downloaded from the <http://www.apc.com> website.
- On any supported operating system, use FTP or SCP to transfer the individual AOS and application firmware modules.
- For a cooling unit that is NOT on your network, use XMODEM through a serial connection to transfer the individual firmware modules from your computer to the cooling unit.



See “Use XMODEM to upgrade one cooling unit” on page 60.

- Use a USB drive to transfer the individual firmware modules from your computer.



See “Use a USB drive to transfer and upgrade the files” on page 60.

## Using the Firmware Upgrade Utility

This Firmware Upgrade Utility is part of the firmware upgrade package available on the <http://www.apc.com> website. (Never use an Upgrade Utility designated for one product to upgrade the firmware of another product.)

**Using the Utility for upgrades on Windows-based systems.** On any supported Windows operating system, the Firmware Upgrade Utility automates the transferring of the firmware modules, in the correct module order.

Unzip the downloaded firmware upgrade file and double-click the .exe file. Then enter the IP address, the user name, and the password in the dialog fields and click **Upgrade Now**. You can use the Ping button to test your entered details.



See also “Using the Firmware Upgrade Utility for multiple upgrades on Windows” on page 56.

**Using the Utility for manual upgrades, primarily on Linux.** On non-Windows operating systems, the Firmware Upgrade Utility extracts the individual firmware modules but does not upgrade the cooling unit.

To extract the firmware files:

1. After obtaining the files from the downloaded firmware upgrade file, run the **Firmware Upgrade Utility** (the .exe file).
2. At the prompts, click **Next**, and then specify the directory location to which the files will be extracted.
3. When the **Extraction Complete** message displays, close the dialog box.

## Use FTP or SCP to upgrade one cooling unit

**FTP.** To use FTP to upgrade a cooling unit over the network:

- The cooling unit must be on the network, with its system IP, subnet mask, and default gateway configured.
- The FTP server must be enabled at the cooling unit.

To transfer the files, perform these steps (this procedure assumes bootmon does not need upgrading):

1. The firmware module files must be extracted.
2. At a computer on the network, open a command prompt window. Go to the directory that contains the firmware files, and list the files:

```
C:\>cd apc
```

```
C:\apc>dir
```

3. Open an FTP client session:

```
C:\apc>ftp
```

4. Type open with the IP address of the cooling unit, and press Enter. If the port setting for the FTP Server has changed from its default of 21, you must use the non-default value in the FTP command.

- For Windows FTP clients, separate a non-default port number from the IP address by a space. For example (showing a space before 21000):

```
ftp> open 150.250.6.10 21000
```

- Some FTP clients require a colon instead before the port number.

5. Log on as a Super User/Administrator (apc is the default user name and password).
6. Upgrade the AOS. (Always upgrade the AOS before the application module).

```
ftp> bin
```

```
ftp> put apc_hw06_aos_nnn.bin (where nnn is the firmware version number)
```

7. When FTP confirms the transfer, type quit to close the session.
8. After 20 seconds, repeat step 3 through step 7, using the application module file name at step 6.

**SCP.** To use Secure CoPy (SCP) to upgrade firmware for the cooling unit, follow these steps (this procedure assumes bootmon does not need upgrading):

1. Locate the firmware modules, see “Using the Utility for manual upgrades, primarily on Linux.” on page 53.
2. Use an SCP command line to transfer the AOS firmware module to the cooling unit. The following example uses nnn to represent the version number of the AOS module:

```
scp apc_hw06_aos_nnn.bin apc@158.205.6.185:apc_hw05_aos_nnn.bin
```

3. Use a similar SCP command line, with the name of the application module, to transfer the application firmware module to the cooling unit. (Always upgrade the AOS before the application module).

## Use XMODEM to upgrade one cooling unit

To use XMODEM to upgrade one cooling unit that is not on the network, you must extract the firmware files with the Firmware Upgrade Utility.

To transfer the files (this procedure assumes bootmon does not need upgrading):

1. Select a serial port at the local computer and disable any service that uses the port.
2. Connect the provided serial configuration cable (part number 940-0299) to the selected port and to the serial port at the cooling unit.
3. Run a terminal program such as HyperTerminal, and configure the selected port for 57600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press the Reset button on the cooling unit, then immediately press the Enter key twice, or until the Boot Monitor prompt displays: BM>
5. Type XMODEM, then press Enter.
6. From the terminal program's menu, select XMODEM, then select the binary AOS firmware file to transfer using XMODEM. After the XMODEM transfer is complete, the Boot Monitor prompt returns.

(Always upgrade the AOS before the application module).

7. To install the application module, repeat step 5 and step 6. In step 6, use the application module file name.
8. Type reset or press the Reset button to restart the cooling unit.



For information about the format used for firmware modules, see “Firmware module files (InRow RC)” on page 57.

Use a USB drive to transfer and upgrade the files

Before starting the transfer, make sure the USB drive is formatted in FAT32.

1. Download the firmware upgrade files and unzip them.
2. Create a folder named **apcfirm** on the USB flash drive.
3. Place the extracted module files in the **apcfirm** directory.
4. Use a text editor to create a file named *upload.rcf*. (The file extension must be .rcf, not .txt for example.)
5. In *upload.rcf*, add a line for each firmware module that you want to upgrade. For example, to upgrade to **bootmon** version 1.0.5, **AOS** v6.0.9, and ACRC2g application version v6.0.9, type:

```
BM=apc_hw06_bootmon_105.bin
```

```
AOS=apc_hw06_aos_609.bin
```

```
APP=apc_hw06_acrc2g_609.bin
```

6. Place *upload.rcf* in the **apcfirm** folder on the flash drive.
7. Insert the flash drive into a USB port on your cooling unit.
8. Press the **Display Reset** button and wait for the card to reboot fully.
9. Check that the upgrade was completed successfully using the procedures in “Verifying Upgrades”.

## Upgrading the firmware on multiple cooling units

Use one of these three methods:

- **Cooling unit Firmware Upgrade Utility on Windows.** See “Using the Firmware Upgrade Utility for multiple upgrades on Windows” on page 56.
- Use **FTP** or **SCP**. To upgrade multiple cooling units using an FTP client or using SCP, write a script which automatically performs the procedure.
- **Export configuration settings.** You can create batch files and use a utility to retrieve configuration settings from multiple cooling units and export them to other cooling units.



Utility is available from the Knowledge Base: <http://www.apc.com/site/support/index.cfm/faq/index.cfm>.

**Using the Firmware Upgrade Utility for multiple upgrades on Windows.** After downloading the Upgrade Utility from the cooling unit downloads page on the [www.apc.com](http://www.apc.com) website, double click on the exe file to run the utility (which ONLY works with IPv4) and follow these steps to upgrade your cooling unit firmware:

1. In the utility dialog, type in an IP address, a user name, and a password, and choose the Ping button if you need to verify the IP address.
2. Click the **Device List** button to open the `iplist.txt` file. Here you should type all cooling unit devices to upgrade with the necessary information: IP, user name, and password.

For example,

```
SystemIP=192.168.0.1
SystemUserName=apc
SystemPassword=apc
```

You can use an existing `iplist.txt` file if it already exists.

3. Select the **Upgrade From Device List** check box to use the `iplist.txt` file.
4. Choose the **Upgrade Now** button to start the firmware version upgrade(s).
5. Choose **View Log** to verify any upgrade.

## Verifying Upgrades

Verify the success of the transfer

To verify whether a firmware upgrade succeeded, you can use the `xferStatus` command in the command line interface to view the last transfer result. Alternatively, you can use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

Last Transfer Result codes

Possible transfer errors include the TFTP or FTP server not being found, or the server refusing access, the server not finding or not recognizing the transfer file, or a corrupt transfer file.

Verify the version numbers of installed firmware

**Path: Main > About > Network**

Use the Web UI to verify the versions of the upgraded firmware modules. You could also use an SNMP GET to the MIB II sysDescr OID. In the command line interface, use the about command.

# Troubleshooting

---

## Network Access Problems

Problem	Solution
Unable to ping the cooling unit	<p>If the cooling unit Status LED is green, try to ping another node on the same network segment as the cooling unit. If that does not work, it is not a problem with the cooling unit. If the Status LED is not green, or if the ping test succeeds, perform the following checks:</p> <ul style="list-style-type: none"><li>• Verify all network connections.</li><li>• Verify the IP addresses of the cooling unit and the NMS.</li><li>• If the NMS is on a different physical network (or subnetwork) from the cooling unit, verify the IP address of the default gateway (or router).</li><li>• Verify the number of subnet bits for the cooling unit's subnet mask.</li></ul>
Cannot allocate the communications port through a terminal program	<p>Before you can use a terminal program to configure the cooling unit, you must shut down any application, service, or program using the communications port.</p>
Cannot access the command line interface through a serial connection	<p>Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400.</p>
Cannot access the command line interface remotely	<ul style="list-style-type: none"><li>• Make sure you are using the correct access method, Telnet or Secure SHell (SSH). An Administrator can enable these access methods. By default, Telnet is enabled. Enabling SSH automatically disables Telnet.</li><li>• For SSH, the cooling unit may be creating a host key. The cooling unit can take up to one minute to create the host key, and SSH is inaccessible for that time.</li></ul>
Cannot access the user interface (UI)	<ul style="list-style-type: none"><li>• Verify that HTTP or HTTPS access is enabled.</li><li>• Make sure you are specifying the correct URL — one that is consistent with the security system used by the cooling unit. SSL requires <b>https</b>, not <b>http</b>, at the beginning of the URL.</li><li>• Verify that you can ping the cooling unit.</li><li>• Verify that you are using a Web browser supported for the cooling unit.</li><li>• If the cooling unit has just restarted and SSL security is being set up, the cooling unit may be generating a server certificate. The cooling unit can take up to one minute to create this certificate, and the SSL server is not available during that time.</li></ul>

# SNMP Issues

Problem	Solution
Unable to perform a GET	<ul style="list-style-type: none"> <li>• Verify the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3).</li> <li>• Use the command line interface or UI to ensure that the NMS has access. See “SNMP screens” on page 31.</li> </ul>
Unable to perform a SET	<ul style="list-style-type: none"> <li>• Verify the read/write (SET) community name (SNMPv1) or the user profile configuration (SNMPv3).</li> <li>• Use the command line interface or UI to ensure that the NMS has write (SET) access (SNMPv1) or is granted access to the target IP address through the access control list (SNMPv3). See “SNMP screens” on page 31.</li> </ul>
Unable to receive traps at the NMS	<ul style="list-style-type: none"> <li>• Make sure the trap type (SNMPv1 or SNMPv3) is correctly configured for the NMS as a trap receiver.</li> <li>• For SNMP v1, query the <b>mconfigTrapReceiverTable</b> MIB OID to verify that the NMS IP address is listed correctly and that the community name defined for the NMS matches the community name in the table. If either is not correct, use SETs to the <b>mconfigTrapReceiverTable</b> OIDs, or use the command line interface or UI to correct the trap receiver definition.</li> <li>• For SNMPv3, check the user profile configuration for the NMS, and run a trap test.</li> </ul> <p>See “SNMP screens” on page 31, “SNMP trap receiver screen” on page 39, and “SNMP traps test screen” on page 40.</p>
Traps received at an NMS are not identified	<p>See your NMS documentation to verify that the traps are properly integrated in the alarm/trap database.</p>









# Worldwide Customer Support

Customer support is available at no charge via e-mail or telephone. Contact information is available at [www.apc.com/support/contact](http://www.apc.com/support/contact).

© Schneider Electric, APC and the APC logo are owned by Schneider Electric Industries S.A.S., or its affiliated companies. All other trademarks are property of their respective owners.