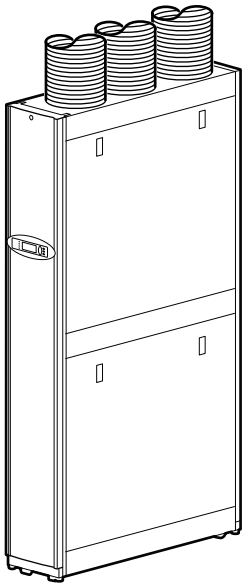
InRow™ Air-Cooled Self-Contained

InRow™ SC
ACSC100, ACSC101

Online Guide

990–2809C
Release date 04/2018



www.schneider-electric.com

Legal Information

The Schneider Electric brand and any registered trademarks of Schneider Electric Industries SAS referred to in this guide are the sole property of Schneider Electric SA and its subsidiaries. They may not be used for any purpose without the owner's permission, given in writing. This guide and its content are protected, within the meaning of the French intellectual property code (Code de la propriété intellectuelle français, referred to hereafter as "the Code"), under the laws of copyright covering texts, drawings and models, as well as by trademark law. You agree not to reproduce, other than for your own personal, noncommercial use as defined in the Code, all or part of this guide on any medium whatsoever without Schneider Electric's permission, given in writing. You also agree not to establish any hypertext links to this guide or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the guide or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

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

Table of Contents

Introduction 7
- Product Description 7
  - Unit overview 7
  - Features 7
  - IPv4 initial setup 7
  - IPv6 Initial Setup 8
  - Network Management with Other Applications 8
- Internal Management Features 9
  - Overview 9
  - Access priority for logging on 9
  - Types of User Accounts 9
- Display Interface 10
  - Status LED 10
  - Check Log LED 11
  - Warning Alarm LED 11
  - Critical Alarm LED 11
- How to Recover from a Lost Password 11
- Watchdog Features 12
  - Overview 12
  - Network Interface Watchdog Mechanism 12
  - Resetting the Network Timer 12

Web User Interface 13
- Introduction 13
  - Overview 13
  - Supported Web browsers 13
- How to Log On 13
  - Overview 13
  - URL address format 14
- Home Screen 15
  - Overview 15

Monitoring the Status 16
- Unit Status 16
  - Overview 16
  - Detailed Status 16
  - Run Hours 17
- Group Status 17
  - Group Overview 17
- Network Status 17
  - Current IPv4 settings 18
  - Current IPv6 settings 18
  - Domain name system status 18
  - Port speed 18

Security and Network Control 19
- Manage User Sessions 19
- Reset the Network Interface 19

Configuring Your Settings 20
- Unit Configuration 20

Thresholds 20
Unit Configuration 20
Group Configuration 21
Configuration 21
Setpoints 22
Security Menu 23
Session Management 23
Ping Response 23
Local Users 23
Remote Users Authentication 25
Firewall 27
Network Configuration 28
TCP/IP Settings for IPv4 28
TCP/IP Settings for IPv6 28
DHCP Response Options 29
Port Speed 31
DNS Configuration 31
DNS Testing 32
Web Access 32
Web SSL Certificate Configuration 33
Console Settings 33
SNMPv1 Access Configuration 34
SNMPv3 Access Configuration 35
Modbus Configuration 36
FTP Server Access Configuration 36
Notification Menu 36
Types of Notification 36
Configuring Event Actions 37
E-Mail Notification Configuration 38
SNMP Trap Receiver Configuration 40
SNMP Traps Test Configuration 40
General Menu 41
Identification Screen 41
Date/Time Configuration 41
Create and Import Settings with the Configuration File 42
Configure the Links Screen 42
Log Configuration 42
Identify Syslog Servers 42
Syslog Settings 42
Syslog Test and Format Example 43
Tests 44
Set the Unit LED Lights to Blink 44
Logs and About Menus 45
Event and Data Logs 45
Event Log 45
Data Log 46
Firewall Log 48
How to Use FTP or SCP to Retrieve Log Files 48
About the Unit 49
About the Network 49
Troubleshooting and Support 51

Device IP Configuration Wizard....52
Capabilities, Requirements, and Installation....52
How to Use the Wizard to Configure TCP/IP Settings....52
System Requirements....52
Installation....52
Use the Wizard....52
Launch the Wizard....52
Configure the Basic TCP/IP Settings Remotely....52
Configure or Re-Configure the TCP/IP Settings Locally....53
How to Export Configuration Settings....54
Retrieve and Export the .ini File....54
Summary of the Procedure....54
Contents of the .ini File....54
Detailed Procedures....54
The Upload Event and Error Message....56
The Event and Its Error Messages....56
Messages in config.ini....56
Errors Generated by Overridden Values....56
Related Topics....57
File Transfers....58
Updating the Firmware....58
Firmware Module Files....58
Troubleshooting....59

Introduction

Product Description

Unit overview

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

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

Features

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

IPv4 initial setup

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

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

  NOTE: Do not use the loopback address (127.0.0.1) as the default gateway. Doing so disables the card. You must then log on using a serial connection and reset 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 unit, see *DHCP Response Options, page 29*

IPv6 Initial Setup

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



See *TCP/IP Settings for IPv6, page 28*.

Network Management with Other Applications

These applications and utilities work with the unit:

- PowerNet® Management Information Base (MIB) with a standard MIB browser — Perform SNMP SETs and GETs and receive SNMP traps.
- StruxureWare Data Center Expert — Collects, organizes, and distributes critical alerts and key information, providing a unified view of complex physical infrastructure environments from anywhere on the network.
- Device IP Configuration Utility — Configure the basic settings of one or more units over the network.
- Security Wizard — Create components needed to help with security for the unit when you are using Secure Sockets Layer (SSL) with related protocols and encryption routines.

Internal Management Features

Overview

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

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

Access priority for logging on

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



See *Session Management, page 23*.

Types of User Accounts

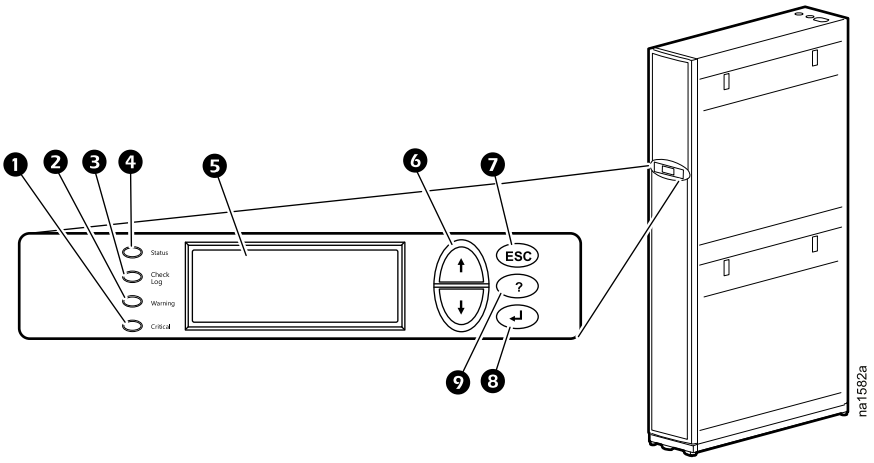
The unit has various levels of access — Administrator, Device User, Read-Only User, and Network-only User — and these are protected by user name and password requirements.

- A Super User/Administrator can use all of the menus in the UI and all of the commands in the command line interface. Administrator user types can be deleted. The default user name and password are both **apc**.
- A Device User has read and write access to device-related screens. Administrative functions like **Session Management** under the **Configuration > Security** menu and **Firewall** under **Logs** are grayed out.
  - The default user name is device, and the default password is `apc`.
- A Read-only User has the following restricted access:
  - Access through the Web UI and command line interface (CLI) only.
  - Access to the same menus as a Device User above but without the capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but disabled. (The Event and Data Logs display no button for this user to clear the log.)
  - The default user name is `readonly` and the default password is `apc`.
- A Network-only User can only log on using the Web user interface (UI) and CLI (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, page 23*.

Display Interface



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

Status LED

This LED indicates the status of the unit.

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

Check Log LED

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

Warning Alarm LED

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

Critical Alarm LED

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

How to Recover from a Lost Password

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

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

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

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

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

Watchdog Features

Overview

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

Network Interface Watchdog Mechanism

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

Resetting the Network Timer

To ensure that the display does not restart if the network is quiet for 9.5 minutes, the display unit attempts to contact the default gateway every 4.5 minutes. If the gateway is present, it responds to the display, and that response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network and is on the same subnet. The network traffic of that computer will restart the 9.5-minute timer frequently enough to prevent the display from restarting.

Web User Interface

Introduction

Overview

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



See *Web Access, page 32* 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 unit through its UI. Other commonly available browsers might work but have not been fully tested.

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

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

How to Log On

Overview

You can use the DNS name or the System IP address of the unit for the URL address of the UI. Use your casesensitive 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, page 9*.

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



For more information, search for Security Handbook at *www.schneider-electric.com* **> Support > Download Documents and Software**.

URL address format

Type the DNS name or IP address of the unit in the Web browser URL address field and press Enter. When you specify a non-default Web–server port in Internet Explorer, you must include http:// or https:// in the URL.

Common Browser Error Messages at Log-On		
Error Message	**Browser**	**Cause of the Error**
”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	**URI Format**
DNS name of `Web1`	
HTTP	`http://Web1`
HTTPS	`https://Web1`
System IP address of `139.225.6.133` and a default Web server port (80)	
HTTP	`http://139.225.6.133`
HTTPS	`https://139.225.6.133`
System IP address of `139.225.6.133` and a non-default Web server port (5000)	
HTTP	`http://139.225.6.133:5000`
HTTPS	`https://139.225.6.133:5000`
System IPv6 address of `2001:db8:1::2c0:b7ff:fe00:1100` and a non-default Web server port (5000)	
HTTP	`http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000`

Home Screen

Overview

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

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

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

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

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

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

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

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



To re-configure the links, see *Configure the Links Screen, page 42*.

Monitoring the Status

Unit Status

Path: Main > Status > Unit

View information specific to this unit.



You can configure your unit and network using the **Configuration** menu options. See *Configuring Your Settings, page 20*.

Overview

Path: Main > Status > Unit > Overview

- **Operating Mode:** The unit is in one of the following modes:
  - **On:** The unit is cooling.
  - **Standby:** The unit is receiving power but not enabled for cooling.
  - **Idle:** The unit is not operating in normal mode due to active alarms.
- **Compressor State:** The current state of the compressor (**On**/**Off**).
- **Cool Output:** The actual cooling output of the unit.
- **Cool Demand:** The amount of cooling that the heat load currently requires.
- **Rack Inlet Temperature:** The average air temperature entering the racks.
- **Supply Air Temperature:** The temperature of the air leaving the unit.
- **Return Air Temperature:** The temperature of the air entering the unit.
- **Condenser Outlet Temperature:** The temperature of the air leaving the condenser.
- **Condenser Inlet Temperature:** The temperature of the air entering the condenser.
- **Suction Temperature:** The temperature of gas entering the compressor.
- **Airflow:** The velocity at which air flows into or out of the unit.
- **Evaporator Fan Speed:** The average revolutions per minute (RPM) of all evaporator fans, given as percentage of the maximum fan speed.
- **Condenser Fan Speed:** The average revolutions per minute (RPM) of all condenser fans, given as percentage of the maximum fan speed.

Detailed Status

Path: Main > Status > Unit > Detailed Status

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

Run Hours

Path: Main > Status > Unit > Run Hours

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

- Air Filter Run Hours

  NOTE: When the air filter is replaced, use the **Air Filter Serviced** button to reset the maintenance alarm.
- Condensate Pump Run Hours
- Compressor Run Hours
- Evaporator Fan 1 Run Hours
- Evaporator Fan 2 Run Hours
- Evaporator Fan 3 Run Hours
- Condenser Fan 1 Run Hours
- Condenser Fan 2 Run Hours
- Condenser Fan 3 Run Hours
- Left Fan Power Supply Run Hours
- Right Fan Power Supply Run Hours

Group Status

Path: Main > Status > Group

View information related to the cooling group.



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

Group Overview

Path: Main > Status > Group > Overview

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

Network Status

Path: Main > Status > Network

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

Current IPv4 settings

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

Current IPv6 settings

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

Domain name system status

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

Port speed

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

Security and Network Control

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

Manage User Sessions

Path: Main > Control > Security > Session Management

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

Reset the Network Interface

Path: Main > Control > Network > Reset/Reboot

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

Configuring Your Settings

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

Unit Configuration

Thresholds

Path: Main > Configuration > Unit > Thresholds

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

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

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

Unit Configuration

Path: Main > Configuration > Unit > Configuration

- **Unit Control:** Select if the unit is a standby unit (**Standby**) or main unit (**On**).
- **Startup Delay:** The delay begins when the cooling unit is started and initialized. The cooling unit cannot begin operation until this delay expires. Use the start-up delay to restart equipment sequentially in your room after a scheduled downtime.
- **Idle On Leak Detect:** When set to **Yes**, the cooling unit will enter idle mode if a Water Detection Fault activates. Set to **No** to disable the cooling unit from entering idle mode if a leak is detected.

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

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

  - Water Detection Fault (when **Idle On Leak Detect** is set to **Yes**)
  - Condensate Pump Fault
  - Cooling Failure
  - Low Suction Pressure Fault
  - High Discharge Pressure Fault
  - Critical Sensor Failure
- **Input Normal State:** Set the normal state of the contact (**Open** or **Closed**). The cooling unit changes its operating mode to **Closed** when the actual state differs from the normal state.
- **Output Normal State:** Set the normal state of the contact (**Open** or **Closed**). If the state of an alarm or event mapped to this contact changes from the normal state, the contact also changes state.
- **Output Source:** Define the type of output source (alarm), either **Any Alarm** or **Only Critical Alarms**, that causes the output to change from its normal state.

Group Configuration

Path: Main Configuration > Group

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

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

Configuration

Path: Main > Configuration > Group > Configuration

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

- **Number of Units in Group:** The number of units in this cooling group. Up to 12 units can be joined together to work as a single cooling group.
- **Configuration Type:** Select the configuration type of the group, which is the air flow control strategy for the cooling group.
  - **Spot:** The cooling unit operates as a stand-alone unit.
  - **In-Row:** Air flow is horizontal to allow in-row operation of the cooling group.
  - **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.
- **Capacity Control:** There are two setting options to determine how the cooling unit cools:
  - **Discrete:** Spot cooling configurations only. The cooling unit runs at a set speed with the hot gas bypass valve (HGBV) fully closed. The compressor comes on when the return air temperature reaches the cool setpoint plus the cool deadband.
  - **Prop (Proportional):** The cooling unit modulates the fan speeds and HGBV to match the cooling output to the load demand.
- **Fan Speed Preference:** Set the fan speed preference, then click **Apply**. In **Discrete** mode, each fan speed setting directly sets the speed of the evaporator fans. In RACS configurations, each fan speed setting specifies a temperature difference between the supply air for the InRow SC cooling unit and the air returned from the environment being cooled. The options are the following:

Fan Speed	Adjustment of Fan Speed in Spot (Discrete) Mode	Adjustment of Fan Speed in RACS (Proportional) Automatic or InRow (Proportional) Automatic Mode
Low	60%	5.6°C (10°F) temperature difference
Medium-Low	70%	8.3°C (15°F) temperature difference
Medium	80%	11.1°C (20°F) temperature difference
Medium-High	90%	13.9°C (25°F) temperature difference
High	190%	16.7°C (30°F) temperature difference

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

Setpoints

Path: Main > Configuration > Group > Setpoints

- **Cool Setpoint:** The air temperature setpoint the cooling units work to achieve and then maintain during operation. In a **Spot** cooling configuration, the cooling unit will bring the **Return Air Temperature** to the **Cool Setpoint**. In an **InRow** configuration, the cooling units will bring the **Rack Inlet Air Temperature** to the **Cool Setpoint**. In a **RACS** configuration, the cooling units will match the air flow of the loads by controlling the difference between the supply and return air temperatures as specified by the fan speed setting. The setpoint must be within 18.0 – 26 °C (64.4 – 78.8°F).
- **Cool Deadband:** The air temperature must exceed the **Cool Setpoint** plus the **Cool Deadband** before the cooling unit turns on the compressor.
- **Supply Air Setpoint:** 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** setting is defined by Schneider Electric authorized personnel only when the cooling group is commissioned.
- **Capacity Control:** There are two setting options to determine how the cooling unit cools:
  - **Discrete:** Spot cooling configurations only. The cooling unit runs at a set speed with the hot gas bypass valve (HGBV) fully closed. The compressor comes on when the return air temperature reaches the cool setpoint plus the cool deadband.
  - **Prop (Proportional):** The cooling unit modulates the fan speeds and HGBV to match the cooling output to the load demand.
- **Fan Speed Preference:** Set the fan speed preference, then click **Apply**. In **Discrete** mode, each fan speed setting directly sets the speed of the evaporator fans. In RACS configurations, each fan speed setting specifies a temperature difference between the supply air for the InRow SC cooling unit and the air returned from the environment being cooled. The options are the following:

Fan Speed	Adjustment of Fan Speed in Spot (Discrete) Mode	Adjustment of Fan Speed in RACS (Proportional) Automatic or InRow (Proportional) Automatic Mode
Low	60%	5.6°C (10°F) temperature difference
Medium-Low	70%	8.3°C (15°F) temperature difference
Medium	80%	11.1°C (20°F) temperature difference
Medium-High	90%	13.9°C (25°F) temperature difference
High	190%	16.7°C (30°F) temperature difference

- **Fan Mode:** This selection allows air flow to be controlled automatically by the cooling unit or manually by userselected fan speed preference. This property only applies to **Spot** (Proportional), **InRow**, and **RACS** deployments.
  - **Auto:** Air flow is automatically controlled by the unit.
  - **Manual:** the air flow is fixed to the value of the **Fan Speed Preference** property.
- **Active Flow Control Bias:** This setting is used to change the bias of the controller by adjusting the contained aisle pressure threshold. **Zero** is the default setting. Only qualified service personnel can make changes to these settings.
  - Hot Aisle Containment (HACS)

- If the cooling units seem to be under-cooling, select **Negative** or **Slightly Negative** to adjust the aisle pressure for additional cooling.
- If the cooling units seem to be over-cooling, select **Positive** or **Slightly Positive** to adjust the aisle pressure for less cooling.

◦ Cold Aisle Containment (CACS)

- If the cooling units seem to be under-cooling, select **Positive** or **Slightly Positive** to adjust the aisle pressure for additional cooling.
- If the cooling units seem to be over-cooling, select **Negative** or **Slightly Negative** to adjust the aisle pressure for less cooling.

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

Security Menu

Session Management

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



See *Local Users, page 23* and *Remote Users Authentication, page 25*.

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

Ping Response

Path: Main > Configuration > Security > Ping Response

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

Local Users

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

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

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

Click **Add User** to add a user. On the resulting **User Configuration** screen, you can add a user and withhold access by clearing the **Access** check box. The maximum length for both the name and password is 64 characters, with less for

multi-byte characters. You have to enter a password. A PIN of four to eight digits may also be designated.

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

User Type

There are four levels of access (Administrator, Device User, Read-Only User, and Network-Only User).

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

    The default user name is **readonly**, and the default password is **apc**.
- A Network-Only User has the following restricted access:
  - Access through the Web interface only (UI) and CLI (telnet not serial). A network-only user has read-write access to the network-related menus only. There is no default name and password.

Touch Screen Remote Authentication Override

Use to configure whether or not this account can log in to the touch screen even when the NMC authentication is set to RADIUS.

User Description

This is a general description of the user.

Session Timeout

Use to configure the length of time that the various UIs wait before logging-out this user (three minutes by default). If you change this value, the user must log-off for the change to take effect.

Serial Remote Authentication Override

The unit will allow a user with this enabled to log-on to the 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 are considered informational events.)
- **Export Log Format:** Exported log files can be formatted using CSV (comma-separated values) or tab delimited.

See *Event Log, page 45* for information on exporting logs.

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

See *E-Mail Notification Configuration, page 38* and *SNMP Trap Receiver Configuration, page 40*.

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

Select one of the following:

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

See *Local Users, page 23*.

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

  If **RADIUS Only** is selected, and the RADIUS server is unavailable, improperly identified, or improperly configured, remote access is unavailable to all users. To regain access, you must use a serial connection to the command line interface and change the access setting to local or radiusLocal.

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

Radius

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

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

- List the RADIUS servers (a maximum of two) available to the unit and the time-out period for each.

- Configure the authentication parameters for a new or existing RADIUS server by clicking on a RADIUS server link.

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

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

Configuring the RADIUS Server

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

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

- Users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined. If no Service-Type attributes are configured, users will have read-only access (on the UI only).
- VSAs can be used instead of the Service-Type attributes provided by the RADIUS server.
- VSAs require a dictionary entry and a RADIUS user file. In the dictionary file, define the names for the ATTRIBUTE and VALUE keywords, but not for the numeric values. If you change numeric values, RADIUS authentication and authorization will not work. VSAs take precedence over standard RADIUS attributes.

Configuring a RADIUS server on UNIX® with shadow passwords

If UNIX shadow password files are used (/etc/passwd) with the RADIUS dictionary files, the following two methods can be used to authenticate users:

- If all UNIX users have administrative privileges, add the following to the RADIUS “user” file. To allow only Device Users, change the APC-Service-Type to Device.

  ```
  DEFAULT Auth-Type = System

  APC-Service-Type = Admin
  ```

- Add user names and attributes to the RADIUS “user” file, and verify the password against /etc/passwd. The following example is for users bconners and thawk:

  ```
  bconners Auth-Type = System

  APC-Service-Type = Admin

  thawk Auth-Type = System

  APC-Service-Type = Device
  ```

Supported RADIUS servers

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

Firewall

Path: Main > Configuration > Security > Firewall > Configuration

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

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

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

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

When a firewall is enabled, this 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.

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

Create a new policy or edit an existing one.

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

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

Path: Main > Configuration > Security > Firewall > Test

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

Network Configuration

TCP/IP Settings for IPv4

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

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

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

TCP/IP Settings for IPv6

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

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

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

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

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

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

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

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

DHCP Response Options

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



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

Vendor Specific Information (option 43)

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

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

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

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

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

TCP/IP Options

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

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

Other Options

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

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

Port Speed

Path: Main > Configuration > Network > Port Speed

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

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

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

DNS Configuration

Path: Main > Configuration > Network > DNS > Configuration

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

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

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

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

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

DNS Testing

Path: Main > Configuration > Network > DNS > Test

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

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

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

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

Web Access

Path: Main > Configuration > Network > Web > Access

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

- **HTTP:** Select this check box to enable access through HTTP. HTTP does not encrypt user names, passwords, and data during transmission.
- **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`.
- **Minimum Protocol:** Select the minimum encryption protocol. There are four available.
  - SSL 3.0
  - TLS 1.0
  - TLS 1.1
  - TLS 1.2
- **Require Authentication Cookie:** If enabled, a session cookie will be used for authentication tracking within the browser. The cookie will be removed upon session end.
- **Limited Status Access:** Select whether or not to display a read-only, public Web page with basic device status. This feature is disabled by default and can be set via the **Use as default page** option to show as the default landing page when a user accesses the device with just the IP/hostname (no specific page listed).

Web SSL Certificate Configuration

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

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

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

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

Console Settings

Console Access

Path: Main > Configuration > Network > Console > Access

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

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

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

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

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

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

User Host Key Configuration

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

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

- **Status:** The **Status** indicates whether the host key (private key) is valid. The **Status** can be one of the following:
  - **SSH Disabled:** No host key in use.
  - **Generating:** The unit is creating a host key because no valid host key was found.
  - **Loading:** A host key is being activated on the unit.
  - **Valid:** One of the following valid host keys is in the /ssh directory (the required location on the unit):
    - A 1024-bit or 2048-bit host key created by the Security Wizard

  - A 2048-bit RSA host key generated by the unit

- **Add or Replace Host Key:** Upload a host key file created by the Security Wizard. To use an externally created host key, load the host key before you enable SSH.

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

- **Remove:** Delete the host key. See screen text also.

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

SNMPv1 Access Configuration

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

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

Path: Main > Configuration > Network > SNMPv1 > Access

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

Access Control

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

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

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

- By default, a community has access to the unit from any location on the network.
- If you configure multiple access control entries for any one community name, it means that one or more of the other communities have no access to the device.
- **Community Name:** The name that an NMS must use to access the community. The maximum length is 15 ASCII characters, 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

SNMPv3 Access Configuration

Path: Main > Configuration > Network > SNMPv3 > Access

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

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

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

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

User Profiles

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

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

- **User Name:** The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters.
- **Authentication Passphrase:** A phrase of 15 to 32 ASCII characters (`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.

Access Control

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

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

- By default, all NMSs that use that profile have access to this device.
- If you configure multiple access control entries for one user profile, it means that one or more of the other user profiles must have no access to this device.

- **User Name:** From the drop-down list, select the user profile to which this access control entry will apply. The selections available are the four user names that you configure through the **User Profiles** option.
- **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address (for example, 149.225.12.1) allows access only by the NMS at that location. An IP address mask that contains 255 restricts access as follows:
  - 149.225.12.255: Access only by an NMS on the 149.225.12 segment.
  - 149.225.255.255: Access only by an NMS on the 149.225 segment.
  - 149.255.255.255: Access only by an NMS on the 149 segment.
  - 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.

Modbus Configuration

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

Path: Main > Configuration > Network > Modbus > TCP

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

FTP Server Access Configuration

Path: Main > Configuration > Network > FTP Server

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

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

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

Notification Menu

Types of Notification

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

- Active, automatic notification: The specified users or monitoring devices are contacted directly.
  - E-mail notification
  - SNMP traps
  - Remote Monitoring Service
  - Syslog notification
- Indirect notification
  - Event log: If no direct notification is configured, users must check the log to determine which events have occurred.

You can also log system performance data to use for device monitoring. See *Log Configuration, page 42* for information on how to configure and use this data logging option.

- Queries (SNMP GETs)

For more information, see *SNMP Trap Receiver Configuration, page 40* and *SNMP Traps Test Configuration, 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 unit supports the use of the RFC1628 MIB (Management Information Base). See *SNMP Trap Receiver Configuration, page 40* for information on how you can set up a trap receiver. The 1628 MIB group of three events only works with that MIB, not the alternative Powernet MIB. They can be configured like any event (see *Configuring Event Actions, page 37*).

Configuring Event Actions

By Event

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

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

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

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

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

- See *Identify Syslog Servers, page 42*
- See *E-Mail Notification Configuration, page 38*.
- See *SNMP Trap Receiver Configuration, page 40*.

By Group

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

To configure a group of events simultaneously:

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

- If you selected **Logging** and have configured a Syslog server, select **Event Log** or **Syslog** on the next screen.

See *Log Configuration, page 42*.

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

Notification Parameters

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

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

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

E-Mail Notification Configuration

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

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

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 does not require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given.
  - **Always:** The SMTP server requires the STARTTLS command to be sent on connection to it.
  - **Implicitly:** The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server.
- **Require CA Root Certificate:** This should only be enabled if the security policy of your organization does not allow for implicit trust of SSL connections. If this is enabled, a valid root CA certificate must be loaded onto the unit for encrypted e-mails to be sent.
- **File Name:** This field is dependent on the root CA certificates installed on the unit and whether or not a root CA certificate is required.

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

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

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

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

  NOTE: The recipient pager must be able to use text-based messaging.
- **Format:** The long format contains name, location, contact, IP address, serial number of the device, date and time, event code, and event description. The short format provides only the event description.
- **Server:** Select one of the following methods for routing e-mail:
  - **Local:** This is through the site-local SMTP server. This recommended setting ensures that the e-mail is sent using the site-local SMTP server. Choosing this setting limits delays and network outages and retries sending e-mail for many hours. When choosing the **Local** setting you must also enable forwarding at the SMTP server of your device and set up a special external e-mail account to receive the forwarded e-mail. Check with your SMTP server administrator before making these changes.

- **Recipient:** This is the SMTP server of the recipient. The unit performs an MX record look-up on the recipients e-mail address and uses that as its SMTP server. The e-mail is only sent once so it could easily be lost.
- **Custom:** This setting enables each e-mail recipient to have its own server settings. These settings are independent of the settings given under **SMTP Server**.

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

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

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

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

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

Send a test message to a configured recipient.

SNMP Trap Receiver Configuration

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

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

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

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

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

  Select either the **SNMPv1** or **SNMPv3** .radio button to specify the trap type. For an NMS to receive both types of traps, you must separately configure two trap receivers for that NMS, one for each trap type.
- **SNMPv1:** Settings for SNMPv1.
  - **Community Name:** The name (“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, page 37* for the deleted trap receiver are set to their default values.

SNMP Traps Test Configuration

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

- **Last Test Result:** The result of the most recent SNMP trap test. A successful SNMP trap test verifies only that a trap was sent; it does not verify that the trap was received by the selected trap receiver. A trap test succeeds if all of the following are true:
  - The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.

- The trap receiver itself is enabled.
- If a host name is selected for the To address, that host name can be mapped to a valid IP address.

- **To:** Select the IP address or host name to which a test SNMP trap will be sent. If no trap receiver is configured, a link to the **Trap Receiver** configuration screen is displayed.

General Menu

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

Identification Screen

Path: Main > Configuration > General > Identification

Define the **Name**, the **Location** (the physical location), and the **Contact** (the person responsible for the device) used by

- The SNMP agent of the unit
- StruxureWare Data Center Expert

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

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

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

Date/Time Configuration

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

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

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

- **Manual Mode:** Do one of the following:
  - Enter the date and time for the unit.
  - Select the check box **Apply Local Computer Time** to apply the date and time settings of the computer you are using.
- **Synchronize with NTP Server:** Have an NTP (Network Time Protocol) Server define the date and time for the unit. By default, any unit on the private side of a StruxureWare Data Center Expert obtains its time settings by using StruxureWare Data Center Expert as an NTP server.
  - **Override Manual NTP Settings:** If you select this, data from other sources (typically DHCP) take precedence over the NTP configurations you set here.
  - **Primary NTP Server:** Enter the IP address or domain name of the primary NTP server.
  - **Secondary NTP Server:** Enter the IP address or domain name of the secondary NTP server, when a secondary server is available.

- **Update Interval:** Define, in hours, how often the unit accesses the NTP Server for an update. Minimum: 1; Maximum: 8760 (1 year).
- **Update Using NTP Now:** Initiate an immediate update of the date and time by the NTP Server.

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

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

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

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

Create and Import Settings with the Configuration File

Path: Main > Configuration > General > User Config File

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

Configure the Links Screen

Path: Main > Configuration > General > Quick Links

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

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

Log Configuration

Identify Syslog Servers

Path: Main > Configuration > Logs > Syslog > Servers

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

- **Syslog Server:** Uses IPv4/ IPv6 addresses or host names to identify from one to four servers to receive Syslog messages sent by the unit.
- **Port:** The user datagram protocol (UDP) port that the unit will use to send Syslog messages. The default UDP port assigned to Syslog is 514.
- **Protocol:** Select either UDP or TCP.
- **Language:** Select the language for any Syslog messages.

Syslog Settings

Path: Main > Configuration > Logs > Syslog > Settings

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

See *Configuring Event Actions, page 37*.

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

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

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

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

To disable Syslog messages, see *Configuring Event Actions, page 37*.

Syslog Test and Format Example

Path: Main > Configuration > Logs > Syslog > Test

Send a test message to the Syslog servers (configured through *Identify Syslog Servers, page 42*). The result will be sent to all configured Syslog servers.

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

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

    Example: `APC: Test Syslog is valid.`

Tests

Set the Unit LED Lights to Blink

Path: Main > Tests > Network > LED Blink

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

Logs and About Menus

Event and Data Logs

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

Event Log

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

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

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

By default, the event log displays the most recent events first. To see the events listed together on a Web page, click **Launch Log in New Window**.

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

You can also use FTP or Secure CoPy (SCP) to view the event log. See *How to Use FTP or SCP to Retrieve Log Files, page 48*.

Filter Event Logs

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

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

The following are important points on filtering:

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

Delete Event Log

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

To disable the logging of events based on their assigned severity level or their event category, see *Configuring Event Actions, page 37*.

Launch Log in New Window

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

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

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

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

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

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

Data Log

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

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

Filter Data Log

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

Filter Log by Date or Time

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

Delete Data Log

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

Data Graphing

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

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

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

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

Log Intervals

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

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

Data Log Rotation

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

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

Data Log Size

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

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

Firewall Log

Path: Main > Logs > Firewall

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



For more information on implementing a policy, see *Firewall, page 27*.

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

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

How to Use FTP or SCP to Retrieve Log Files

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

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

Use SCP to Retrieve the Files

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



See *Console Settings, page 33*.

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

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

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

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

Use FTP to Retrieve the Files

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

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

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

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

   `ftp>open ip_address port_number`

To set a non-default port value to enhance security for the FTP Server, see *FTP Server Access Configuration, page 36*. 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 Unit

Path: Main > About > Device

The information displayed varies according to the device used.

- **Model Number**
- **Serial Number**
- **Firmware Revision**
- **Hardware Revision**

About the Network

Path: Main > About > Network

Hardware Factory

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

Network Management Card

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

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

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

- **Name:** The name of the firmware module. The APC AOS module is always named aos, and the boot monitor module is always named bootmon.

- **Version:** The version number of the firmware module. Version numbers of the modules may differ, but compatible modules are released together. Never combine application modules and AOS modules from different releases.

  NOTE: If the boot monitor module must be updated, a boot monitor module is included in the firmware release. Otherwise, the boot monitor module that is installed on the card is compatible with the firmware update.

- **Date/Time:** The date and time at which the firmware module was loaded

Troubleshooting and Support

Path: Main > About > Support

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

- Link 1: Knowledge Base
- Link 2: Company Contact Information
- Link 3: Software and Firmware Downloads

Technical Support Debug Information Download

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

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

Device IP Configuration Wizard

Capabilities, Requirements, and Installation

How to Use the Wizard to Configure TCP/IP Settings

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

System Requirements

The Wizard runs on Windows® 2000, Windows 2003, Windows Vista®, Windows XP, Windows 7, Windows Server 2008, Windows 8, and Windows 2012.

Installation

To install the Wizard from a downloaded executable file:

1. Go to *www.schneider-electric.com*.
2. Download the Device IP Configuration Wizard.
3. Run the executable file in the folder to which you downloaded it.

Use the Wizard

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

Launch the Wizard

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

Configure the Basic TCP/IP Settings Remotely

Prepare to Configure the Settings

Before you run the Wizard:

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

Run the Wizard to Perform the Configuration

To discover and configure unconfigured units over the network:

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

On the **Transmit Current Settings Remotely** screen, if you select the **Start a Web browser when finished** check box, the default Web browser connects to the cooling unit after the Wizard transmits the settings.

4. Click **Finish** to transmit the settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
5. If the Wizard finds another unconfigured cooling unit, it displays the screen to enter TCP/IP settings. Repeat this procedure beginning at step 3, or to skip the cooling unit whose MAC address is currently displayed, click **Cancel**.

Configure or Re-Configure the TCP/IP Settings Locally

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

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

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

How to Export Configuration Settings

Retrieve and Export the .ini File

Summary of the Procedure

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

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

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

Contents of the .ini File

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

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

Detailed Procedures

Retrieving

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

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

      `ftp> open ip_address`

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

      `ftp> get config.ini`

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

Customizing

You must customize the file before you export it.

1. Use a text editor to customize the file.
   - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   - Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
   - Enclose in quotation marks any values that contain leading or trailing spaces or are already enclosed in quotation marks.

- To export scheduled events, configure the values directly in the .ini file.
- To export a system time with the greatest accuracy, if the receiving cooling units can access a Network Time Protocol server, configure enabled for `NTPEnable`:

  `NTPEnable=enabled`

  Alternatively, reduce transmission time by exporting the `[SystemDate/Time]` section as a separate .ini file.
- To add comments, start each comment line with a semicolon (;).

2. Copy the customized file to another file name in the same folder:
   - The file name can have up to 64 characters and must have the .ini suffix.
   - Retain the original customized file for future use.

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

Transfer the File to a Single Unit

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

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

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

     `ftp> put filename.ini`

Export the File to Multiple Units

To export the .ini file to multiple units:

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

The Upload Event and Error Message

The Event and Its Error Messages

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

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

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

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

Messages in config.ini

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

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

Errors Generated by Overridden Values

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

See *Contents of the .ini File, page 54* for information about which values are overridden.

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

Related Topics

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



See *Device IP Configuration Wizard, page 52*.

File Transfers

Updating the Firmware

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

Updating here means placing the module files on the unit; there is no installation required. Check regularly on *www.schneider-electric.com* for any new updates.

NOTE: You will need to select the language pack if you require your display interface to be available in a language other than English.

Firmware Module Files

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

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

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

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

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

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

Troubleshooting

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

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.schneider-electric.com

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

© 2018 – 2018 Schneider Electric. All rights reserved.

990–2809C