

Contents

| | |
|---|-----------|
| Introduction | 1 |
| Product Description | 1 |
| Features of the InfraStruXure InRow SC management interface | 1 |
| Initial setup | 2 |
| Internal Management Features | 3 |
| Overview | 3 |
| Log-on control | 4 |
| Types of user accounts | 5 |
| How to Recover from a Lost Password | 5 |
| Display Interface LEDs | 7 |
| Status | 7 |
| Check Log | 8 |
| Warning Alarm | 8 |
| Critical Alarm | 8 |
| Watchdog Features | 9 |
| Overview | 9 |
| Network interface watchdog mechanism | 9 |
| Resetting the network timer | 9 |
| Control Console | 10 |
| How to Log On | 10 |
| Overview | 10 |
| Remote access to the control console | 10 |
| Local access to the control console | 11 |
| Main Screen | 12 |
| Example main screen | 12 |
| Information and status fields | 12 |
| Control Console Menus | 15 |
| Menu structure | 15 |
| Main menu | 16 |
| Device Manager option | 16 |
| Network option | 16 |
| System option | 17 |

Web Interface 18

| | |
|--------------------------------|-----------|
| How to Log On | 18 |
| Overview | 18 |
| Supported Web browsers | 18 |
| URL address formats | 20 |
| 21 | |
| Summary Page | 21 |
| Navigation tabs | 21 |
| Quick status | 22 |
| Status | 22 |
| Help | 22 |
| Select a tab to perform a task | 23 |

InRow SC Operation 25

| | |
|-------------------|-----------|
| Unit | 25 |
| Overview | 25 |
| Detailed Status | 25 |
| Identification | 26 |
| Run Hours | 26 |
| Service Intervals | 26 |
| Thresholds | 26 |
| Setpoints | 27 |
| Configuration | 28 |

Administration: Security 29

| | |
|---|-----------|
| Local Users | 29 |
| Permission levels | 29 |
| Setting user access (Administration>Security>Local Users> <i>options</i>) | 29 |
| Remote Users | 30 |
| Authentication (Administration>Security>Remote Users>Authentication) | 30 |
| RADIUS (Administration>Security>Remote Users>RADIUS) | 31 |
| Configuring the RADIUS Server | 32 |
| Summary of the configuration procedure | 32 |
| Configuring a RADIUS server on UNIX®, with shadow passwords | 33 |
| Supported RADIUS servers | 33 |
| Inactivity Timeout (Administration>Security>Auto Log Off) | 33 |

Administration: Network Features 34

| | |
|--|-----------|
| TCP/IP and Communication Settings | 34 |
| TCP/IP settings (Administration>Network>TCP/IP) | 34 |
| DHCP response options | 36 |
| Port Speed (Administration>Network>Port Speed) | 38 |
| DNS (Administration>Network>DNS>options) | 39 |
| Web (Administration>Network>Web>options) | 41 |
| Console (Administration>Network>Console>options) | 43 |
| SNMP (Administration>Network>SNMP>options) | 44 |
| FTP Server (Administration>Network>FTP Server) | 46 |

Administration: Notification and Logging 48

| | |
|---|-----------|
| Event Actions (Administration>Notification>Event Actions>options) | 48 |
| Types of notification | 48 |
| Configuring event actions | 49 |
| Active, Automatic, Direct Notification | 52 |
| E-mail notification | 52 |
| SNMP Traps | 55 |
| Syslog (Logs>Syslog>options) | 55 |
| Indirect Notification through Logs or Queries | 58 |
| Event log (Logs>Events>options) | 58 |
| Data log (Logs>Data>options) | 59 |
| How to use FTP or SCP to retrieve the log files | 61 |
| Queries (Modbus requests and SNMP GETs) | 63 |

Administration: General Options 64

| | |
|---|-----------|
| Information about the InRow SC | 64 |
| Information you configure | |
| (Administration>General>Identification) | 64 |
| Hardware and firmware information | |
| (Administration>General>Factory Info) | 64 |
| Date, Time, and Temperature | 65 |
| Date and time (Administration>General>Date & Time>options) | 65 |
| Temperature scale (Administration>General>Temp Scale) | 66 |
| Serial Modbus (Administration>General>Serial Modbus) | 67 |

Reset the Interface (Administration>General>Reset/Reboot) 68
Configuring Links (Administration>General>Quick Links) 69

APC Device IP Configuration Wizard 70

Purpose and Requirements 70
 How to use the Wizard to configure TCP/IP settings 70
 System requirements 70
 Installation 70
Use the Wizard 71
 Launch the Wizard 71
 Configure the basic TCP/IP settings remotely 71
 Configure or reconfigure the TCP/IP settings locally 72

How to Export Configuration Settings 73

Retrieving and Exporting the .ini File 73
 Summary of the procedure 73
 Contents of the .ini file 74
 Detailed procedures 75
The Upload Event and Error Messages 78
 The event and its error messages 78
 Errors generated by overridden values 79
Using the APC Device IP Configuration Wizard 79

File Transfers 80

Upgrading Firmware 80
 Benefits of upgrading firmware 80
 Firmware files (InRow SC) 80
 Obtain the latest firmware version 81
Firmware File Transfer Methods. 81
 Use FTP or SCP to upgrade one InRow SC 82
 How to upgrade multiple InRow SCs 83
 Use XMODEM to upgrade one InRow SC 83
Verifying Upgrades and Updates 85
 Verify the success or failure of the transfer 85

Last Transfer Result codes 85
Verify the version numbers of installed firmware 85

Product Information 86

Warranty and Service 86

Limited warranty 86
Warranty limitations 86
Obtaining service 87

Life-Support Policy 88

General policy 88
Examples of life-support devices 88

Index 89

Introduction

Product Description

Features of the InfraStruXure InRow SC management interface

The American Power Conversion (APC®) InfraStruXure InRow SC air conditioner is a modular DX air conditioning unit. It is one-half the width of a standard enclosure, and can be placed in a data-center row. It provides full management capabilities over a network using Telnet, Secure Shell (SSH), HTTP, HTTPS, FTP, Secure Copy (SCP), and SNMP. The InRow SC provides the following features:

- Temperature monitoring
- Remote shutdown input contact which, when active, halts cooling operations of the unit
- Output contact monitoring for use with a discrete sensor
- Event log accessible by Telnet, FTP, SSH, SCP, serial connection, the display interface, or a Web browser
- SNMP traps and e-mail notification sent in response to events
- Syslog events sent to configured Syslog servers
- Security protocols for authentication and encryption

Initial setup

You must define the following three TCP/IP settings for the InRow SC management interface before it can operate on the network:

- IP address of the InRow SC
- Subnet mask
- IP address of the default gateway



Note

Do not use the loopback address (127.0.0.1) as the default gateway address for the InRow SC management interface. Doing so disables the InRow SC management interface and will require you to reset TCP/IP settings to their defaults using a local serial login.



To use a DHCP server to configure the TCP/IP settings at the InRow SC, see [TCP/IP settings \(Administration>Network>TCP/IP\)](#).



See also

To configure the TCP/IP settings, see the InfraStruXure InRow SC *Operation and Maintenance* manual, provided in printed form and in PDF on either the *Utility* CD or on the APC Web site, www.apc.com.

Internal Management Features

Overview

You can manage the InRow SC through the Web management interface, display interface, control console, Modbus, or SNMP. SNMP requires the PowerNet[®] MIB, available on the *Utility* CD or from the APC Web site, www.apc.com.



For more information about the menu-driven InRow SC management interface, see [Web Interface](#) and [Control Console](#).



See also

For more information about the display interface, see the *InfraStruXure InRow SC Operation and Maintenance* manual, available on the *Utility* CD or on the APC Web site, www.apc.com.



See also

To download the latest version of the Modbus register map go to the APC Web site, www.apc.com, search by part number, and click the link to the register map in the list of documentation. Check the publication date at the start of the file.

For more information about Modbus, see the Modbus Standard Library at www.modbus.org.



See also

To use the PowerNet MIB with an SNMP browser, see the *PowerNet SNMP Management Information Base (MIB) Reference Guide*, provided on the *Utility* CD.

Log-on control

Only one user at a time can log on to the InRow SC to use its internal user interface features. The priority for access is as follows:

- Local access to the control console from a computer with a direct serial connection to the InRow SC always has the highest priority.
- Telnet or Secure SHell (SSH) access to the control console from a remote computer has the next highest priority.
- Web access, either directly or through the InfraStruXure Manager, has the lowest priority.



For information on how SNMP access to the InRow SC is controlled, see [SNMP \(Administration>Network>SNMP>options\)](#).

Types of user accounts

The InRow SC has three levels of access (Administrator, Device User, and Read-Only user), all of which are protected by user name and password requirements.

- An Administrator can use all of the management menus available in the control console and the Web interface. The Administrator's default user name and password are both **apc**.
- A Device User (Device Manager in the control console) can access only the **Log** option in the **Events** menu and use the **Unit** and **Alarms** menus. The Device User's 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.
 - Access to the same menus as a Device User, but without the capability to change configurations, control devices, or delete data. Links to configuration options may be visible but are disabled, and the event log displays no **Clear Log** button.

The default user name is **readonly**, and the default password is **apc**.



To set **User Name** and **Password** values for the Administrator, Device User, and Read-Only user accounts, see [Setting user access \(Administration>Security>Local Users>options\)](#). You must use the Web interface to configure values for the Read-Only user.

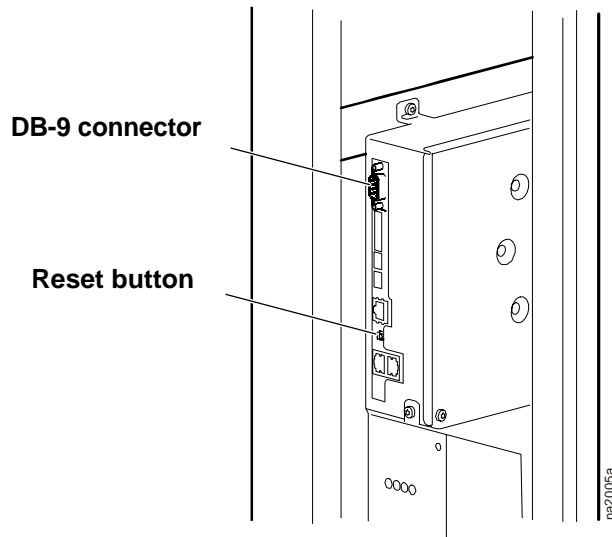
How to Recover from a Lost Password

Use a local computer, a computer that connects to the InRow SC or other device through the serial port to access the control console.



Note

To access the serial port, remove the rear panel and lower air filter of the InRow SC.



1. Select a serial port at the local computer, and disable any service that uses that port.
2. Connect the APC modem cable (APC part number 940-0103) to the selected port on the computer and to the serial port at the InRow SC (use the DB-9 connector on the back of the electrical panel).
3. Run a terminal program (such as HyperTerminal[®]) and configure the selected port as follows:
 - 9600 bps
 - 8 data bits
 - no parity
 - 1 stop bit
 - no flow control

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.

4. Press the **Reset** button on the motherboard. Immediately press ENTER, repeatedly if necessary, to display the **User Name** prompts. Press the **Reset** button on the back of the electrical panel. The Status LED will flash green. Immediately press the **Reset** button on the back of the electrical panel a second time while the LED is flashing to reset the user name and password to their defaults temporarily.
5. Press ENTER as many times as necessary to redisplay the **User Name** prompt, then use the default, **apc**, for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is redisplayed, you must repeat step 4 and log on again.)
6. From the **Control Console** menu, select **System**, then **User Manager**.
7. Select **Administrator**, and change the **User Name** and **Password** settings, both of which are now defined as **apc**. Select **Accept Changes** to store the new user name and password values.
8. Press CTRL+C, log off, reconnect any serial cable you disconnected, restart any service you disabled, reinstall the lower air filter, and replace the rear panel.

Display Interface LEDs

Status

This LED indicates the status of the InRow SC.

| Condition | Description |
|----------------|---|
| Off | The InRow SC has no power. |
| Solid Green | The InRow SC is receiving power. |
| Flashing Green | The InRow SC is receiving a firmware upgrade. |

Check Log

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

Warning Alarm

When yellow, this LED indicates that a warning alarm condition exists and requires 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

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 still blinks and shows a critical status.

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the InRow SC uses internal, system-wide watchdog mechanisms. When it reboots to recover from an internal problem, a **System: Warmstart** event is recorded in the event log.

Network interface watchdog mechanism

The InRow SC implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the InRow SC 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 InRow SC does not restart if the network is quiet for 9.5 minutes, the InRow SC attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the InRow SC, 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 most of the time and is on the same subnet. The network traffic of that computer will reset the 9.5-minute timer frequently enough to prevent the InRow SC from restarting.

Control Console

How to Log On

Overview

You can use either a local (serial) connection, or a remote (Telnet or SSH) connection to access the control console.

Use case-sensitive user name and password entries to log on (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device User). A Read-Only user cannot access the control console.



If you cannot remember your user name or password, see [How to Recover from a Lost Password](#).

Remote access to the control console

You can access the control console through Telnet or Secure SHell (SSH), depending on which is enabled. (An Administrator can enable these access methods through the **Telnet/SSH** option of the **Network** menu.) By default, Telnet is enabled. Enabling SSH automatically disables Telnet.

Telnet for basic access. Telnet provides the basic security of authentication by user name and password, but not the high-security benefits of encryption. To use Telnet to access the control console:

1. At a command prompt, type **telnet** and the System IP address for the InRow SC (when the InRow SC uses the default Telnet port of 23), and press ENTER. For example: **telnet 139.225.6.133**



Note

If the InRow SC uses a non-default port number (between 5000 and 32767), you need to include a colon or a space (depending on your Telnet client) between the IP address and the port number.

2. Enter the user name and password (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device User).

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

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

Local access to the control console

You can use a local computer that connects to the InRow SC through the serial port on the controller board on the electrical panel (connector J2) of the unit.



Note

To access the serial port, remove the rear panel and lower air filter of the InRow SC.

1. Select a serial port at the local computer, and disable any service which uses that port.
2. Use the supplied RS232 configuration cable (APC part number 940-0103) to connect the selected port to the serial port at the InRow SC (use the DB-9 connector on the back of the electrical panel).
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. Save the changes.
4. **PRESS ENTER**, repeatedly if necessary, to display the **User Name** prompt.
5. Enter the user name and password for the access desired (Administrator or Device User).

Main Screen

Example main screen

The following is an example of the screen that appears when you log on to the control console at the InRow SC.

```
American Power Conversion                Network Management Card AOS vx.x.x
(c) Copyright 2005 All Rights Reserved    InRow SC APP                      vx.x.x
-----
Name      : InRow SC                    Date : 05/29/2006
Contact   : Bill Cooper                 Time : 10:16:58
Location  : Testing Lab                 User : Administrator Stat : P+ N+ A+
Up Time   : 21 Days 21 Hours 21 Minutes

Communication Established

----- Control Console -----

    1- Device Manager
    2- Network
    3- System
    4- Logout

<ESC>- Main Menu, <ENTER>- Refresh, <CTRL-L>- Event Log>
```

Information and status fields

Main screen of control console.

- Two fields identify the APC operating system (AOS) and application (APP) firmware versions. The application firmware name identifies the type of device that connects to the network. On the example main screen, the application firmware for the InRow SC is displayed.

```
InRow SC AOS      vx.x.x
InRow SC APP      vx.x.x
```

- Three fields identify the system **Name**, **Contact**, and **Location** values.

```
Name:      InfraStruXure InRow SC
Contact:   Bill Cooper
Location:  Testing Lab
```



To set the **Name**, **Contact**, and **Location** values, see [Information you configure \(Administration>General>Identification\)](#).

- An **Up Time** field reports how long the InRow SC has been running since it was last reset or since power was applied.

```
Up Time: 21 Days 21 Hours 21 Minutes
```

- Two fields identify the date and time at which the screen most recently refreshed.

```
Date : 05/29/2006
Time : 5:58:30
```

- A **User** field identifies whether you logged on as Administrator or Device-Only User.

```
User : Administrator
      or
User : Device Manager
```

Main screen status fields.

- A **Stat** field reports the InRow SC status.

Stat : P+ N+ A+

| | |
|-----------|---|
| P+ | The APC operating system (AOS) is functioning properly. |
| N+ | The network is functioning properly. |
| N? | A BOOTP or DHCP request cycle is in progress. |
| N- | The InRow SC failed to connect to the network. |
| N! | Another device is using the IP address of the InRow SC. |
| A+ | The application is functioning properly. |
| A- | The application has a bad checksum. |
| A? | The application is initializing. |
| A! | The application is not compatible with the AOS. |



Note

If the AOS status is not P+, contact [APC Worldwide Customer Support](#), even if you can still access the InRow SC.

InRow SC air conditioner status field.

The **Status** field displays the status of the devices that are connected to the InRow SC air conditioner.

Cooling Unit Status: None

Control Console Menus

Menu structure

The menus in the control console list options by number and name. To use an option, type the option's number and press ENTER, then follow any on-screen instructions.

For menus that allow you to change a setting you must use the **Accept Changes** option to save the changes you made. Some changes may only take effect after you log off.

While in a menu, you can also do the following:

- Type ? and press ENTER to access brief menu option descriptions (if the menu has help available).
- Press ENTER to refresh the menu.
- Press ESC to return to the menu from which you accessed the current menu.
- Press CTRL+C to return to the main (control console) menu.
- Press CTRL+L to access the event log.
- Press CTRL+D to move through the UPS, sensor, input and beacon menus.



For more information, see [Event log \(Logs>Events>options\)](#).

Main menu

The main control console menu has options that provide access to the management features of the control console.

- 1- Device Manager (equivalent to Device User in the Web interface)
- 2- Network
- 3- System
- 4- Logout



Note

When you log on as Device Manager, you do not have access to the **Network** or **System** menus.

Device Manager option

This option accesses the **Device Manager** menu, which displays information about the unit. Select the components you want to manage. For example:

- 1- View Active Alarms
- 2- Cooling Unit

Network option

Use this option to perform any of the following tasks:

- Configure the TCP/IP settings for the InRow SC.
- Configure the settings for the type of server (DHCP or BOOTP) used to provide the TCP/IP settings to the InRow SC.
- Use the Ping utility.
- Define settings that affect the FTP, Telnet/SSH, Web/SSL, SNMP, Syslog, Serial Modbus, E-mail, and DNS features of the InRow SC.

System option

Use this option to perform any of the following tasks:

- Control **Administrator** and **Device Manager** access.
- Define the system **Name**, **Contact**, and **Location** values.
- Set the date and time used by the InRow SC.
- Restart the InRow SC
- Reset control console settings to their default values.
- Access group information about the InRow SC.
- Define RADIUS access and set primary and secondary servers.

Web Interface

How to Log On

Overview

You can use the InRow SC DNS name or System IP address for the URL address of the Web interface. Use your case-sensitive **User Name** and **Password** settings to log on. The default user name differs by account type:

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

The default password is **apc** for all three account types.



Note

If you are using HTTPS as your access protocol, your login credentials are compared with information in a server certificate. If the certificate was created with the APC Security Wizard, and an IP address was specified as the common name in the certificate, you must use an IP address to log on to the InRow SC. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.



For information about the Web page that appears when you log on to the Web interface, see [Summary Page](#).

Supported Web browsers

You can use Microsoft® Internet Explorer (IE) 5.5 and higher (on Windows® operating systems only), Firefox, version 1.x, by Mozilla Corporation (on all operating systems), or Netscape® 7.x and higher (on all operating systems) to access the InRow SC through its Web interface. Other commonly available browsers also may work but have not been fully tested by APC.



Note

For optimal functioning of the Web interface, enable JavaScript® for your Web browser.

In addition, the InRow SC cannot work with a proxy server. Therefore, before you can use a Web browser to access its Web interface, you must do one of the following:

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

URL address formats

Type the InRow SC's DNS name or IP address in the Web browser's URL address field and press ENTER. When you specify a non-default Web server port in Internet Explorer, you must include `http://` or `https://` in the URL.

Common browser error messages at log-on.

| Cause of the Error | Browser | Error Message |
|--|--------------------------------------|---|
| Someone else is logged on. | Internet Explorer, Netscape, Firefox | "You are not authorized to view this page" or "Someone is currently logged in..." |
| Web access is disabled, or the URL was not correct | Netscape | "The connection was refused..." |
| | Internet Explorer | "This page cannot be displayed." |
| | Firefox | "Unable to connect." |

URL format examples.

- For a DNS name of Web1:
 - `http://Web1` if HTTP is your access mode
 - `https://Web1` if HTTPS (SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133 and the default Web server port (80):
 - `http://139.225.6.133` if HTTP is your access mode
 - `https://139.225.6.133` if HTTPS (SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133 and a non-default Web server port (5000):
 - `http://139.225.6.133:5000` if HTTP is your access mode
 - `https://139.225.6.133:5000` if HTTPS (SSL/TLS) is your access mode.

Summary Page

When you log on to the Web interface at the InRow SC, navigation tabs are displayed at the top of the screen. Below the navigation tabs, a top menu bar lists options related to the selected tab. The status field displays information about the selected tab or top menu bar option.




Navigation tabs

Icons indicate the status of the InRow SC (and the number of alarms, if applicable).

- **Home**—View any active alarm or warning conditions and clear active alarms; this tab is displayed at logon.
- **Unit**—View cooling settings, unit properties and identification information; view or reset run hours and setpoints and configure service intervals.
- **Logs**—View and configure the event and data logs, and configure Syslog settings.
- **Administration**—Configure security, network connection, notification, and device settings.

Quick status

The quick status tab is displayed in the upper right of every screen in the Web interface. The tab displays a warning of any alarms.

| | |
|---|---|
|  | Click the green “device operating normally” icon to return to the status screen where the status for attached devices is displayed. |
|  | Click the “attention required” icon to return to the status screen where active warnings and alarms are displayed. |
|  | Click the “alarm detected” icon to return to the status screen where active alarms are displayed. |

Status

The **Active Alarms** field displays the states (No alarms present, Warning, or Critical) of both the unit and individual units. The **Recent Device Events** table displays the five most recent device events, and the dates and times they took place. Click **More Events** at the bottom of the **Recent Device Events** table to see the entire event log.

Help

Click **Help**, located in the upper right hand corner of the Web interface, to view context-sensitive information.

Select a tab to perform a task

To do the following, see [Unit](#):

- View the status overview and properties of the unit.
- Set unit delays.
- Change the unit identification values.
- View factory location and configure name and location
- Assign service intervals
- Configure the temperature setpoints.
- Assign the type of alarm that will activate the output sensor.
- Set the normal state of the input.
- Reset the unit run hours alarms.
- Set alarm threshold values.
- Setpoint works to achieve/maintain the air temperature.

To do the following, see [Administration: Notification and Logging](#):

- Access the data log.
- Configure the actions to be taken based on an event's severity level.
- Configure SNMP Trap Receiver settings for sending event-based traps.
- Define who will receive e-mail notifications of events.
- Test e-mail settings.

To do the following, see [Administration: Network Features](#):

- Configure new TCP/IP settings for the InRow SC.
- Identify the Domain Name System (DNS) Server and test the network connection to that server.
- Define settings for the FTP server, Telnet/SSH, SNMP, e-mail, Syslog, and Web.

Go do the following, see [Administration: General Options](#):

- Control Administrator, Device User, and Read-Only user access.
- Configure RADIUS access, servers, and server secret.
- Define the System **Name**, **Contact**, and **Location** values.
- Set the date and time used by the InRow SC.
- Restart the user interface of the InRow SC.
- Reset network interface settings to their default settings.
- Upload a user configuration file.
- Define the URL addresses of the user links in the Web interface.

InRow SC Operation

Unit

Overview

View information for the various components for the unit including the following:

- Operating mode—on, standby, or idle
- Cool output and demand—in kilowatts (kW)
- Temperature—Consist of the Rack Inlet temperature, Supply Air Temperature, Return Air Temperature, and Suction Temperature of air at the sensors
- Air flow—in cubic feet per minute (CFM) or Liters per second (L/s)
- 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 RPM of all condenser fans, given as a percentage of the maximum fan speed.

Detailed Status

View information for the components of the unit:

- Input and Output Relay—open or closed.
- Filter Differential Pressure—the difference in pressure on either side of the air filter. A high differential pressure indicates a clogged filter.
- Containment Differential Pressure—the difference in pressure between the hot side and cold side of the Racks Air Containment System (RACS) setup. A high differential pressure could indicate a clogged filter. This value affects fan speed control.
- Superheat Temperature—the difference between the suction line temperature and the evaporator saturation temperature.
- Suction Pressure—The pressure of the low pressure (suction) refrigerant line.
- Discharge Pressure—The pressure of the high pressure (discharge) refrigerant line.

Identification

The **Unit** tab's left navigation menu option **Identification** displays the following read-only information about the unit:

- Model number
- Serial number
- Controller firmware version
- Hardware revision
- Date of manufacture

At the **Unit** tab's left navigation menu option **Identification**, configure the following identification information:

- **Name**—Enter a name (up to 40 alphanumeric characters) for the unit
- **Location**—Enter the location (up to 40 alphanumeric characters) of the unit

Click **Apply** to save your changes.

Run Hours

View the run hours of each unit's components. To reset the run hours, select the unit components to set to zero and click **Apply**.

Service Intervals

Set the service interval for the air filter, in weeks. By default, the interval for the air filter service alarm is 18 weeks.

Enable or disable alarm generation for the air filter service interval, then click **Apply** to save your changes.

Thresholds

Configure high temperature thresholds of 32° to 212°F (0° to 100°C) for the rack inlet, supply air, and return air sensors. Click **Apply** to save your changes.

Setpoints

- **Cool Setpoint**—The air temperature setpoint the unit works to achieve/maintain during operation. In a Spot Cooling configuration, the unit will bring the Return Air Temperature to a Cool Setpoint. In an In-Row or RACS configuration the unit will bring the Rack Inlet Air Temperature to the Cool Setpoint.
- **Cool Deadband**—The air temperature must exceed the Cool Setpoint plus Cool Deadband before the unit turns on the compressor.
- **Supply Air Setpoint**—Assign the supply air setpoint, then click **Apply**.
- **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 and the air returned from the environment being cooled.

Configuration

Configure the following unit settings, then click **Apply** to save your changes:

- **Capacity Control**— Discrete and Proportional. Discrete mode is only available in Spot Cooling Configuration. Proportional Mode is available in any configuration.
- **Configuration Type**—There are three choices: **Spot Cooling, InRow** and **RACS**. Spot Cooling configuration, unit regulates the Return Air Temperature (the Rack Inlet Air Temperature sensor is ignored for control purposes). InRow and RACS configurations, the unit regulates the Rack Inlet Air Temperature using the remote temperature probe.
- **Startup Delay**—The delay that begins when power is applied. The unit starts when the delay period ends. This allows you to create a staged restart after a power loss. Valid values are 0 to 999 seconds.
- **Idle on Leak Detect**—Idle the unit when a leak is detected. By default, this feature is not activated; the default setting is **No**.
- **Input Normal State**—The normal state for the input contact, open or closed. When the input is not in its normal state, the unit will stop cooling.
- **Output Normal State**—The normal state for the Output contact, open or closed.
- **Output Source**—Defines the state of alarms that will change the state of the output.
- **Display Units**—The units (metric or English) displayed in the Web, console, and display interface, and in the data and event log.

Administration: Security

Local Users

Permission levels

Before you configure user access, be sure you understand the capabilities of each account type (Administrator, Device User, and Read-Only user) to use menus, view information, and change settings.



For information on user permission levels for each account type (Administrator, Device User, and Read-Only user), see [Types of user accounts](#).

Setting user access (**Administration>Security>Local Users>options**)

You set the user name and password for each of the account types in the same manner.

User name. The case-sensitive user name (maximum of 10 characters) is used by Administrator and Device Users to log on at the control console, local display, or Web interface and by the Read-Only User to log on at the Web interface. Default values are **apc** for Administrator, **device** for Device Users, and **readonly** for the Read-Only user.

Password. The case-sensitive password (maximum of 10 characters) is used to log on to the Web interface or (except for the Read-Only user) the control console or local display. The default setting for **Password** is **apc** for Administrators, Device Users, and Read-Only Users.

Remote Users

Authentication (Administration>Security>Remote Users>Authentication)

Use this option to select how to administer remote access to the InRow SC:



See also

For information about local authentication (authentication that can be administered without the centralized authentication provided by a RADIUS server), see the *Security Handbook* provided on the *Utility CD* and available on the APC Web site at www.apc.com.



Note

APC supports the authentication and authorization functions of RADIUS (Remote Authentication Dial-In User Service).

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

Select one of the following:

- **Local Authentication Only:** RADIUS is disabled. Local authentication is enabled.
- **RADIUS, then Local Authentication:** RADIUS is enabled, and local authentication is enabled. Authentication is requested from the RADIUS server first; local authentication is used only if RADIUS authentication fails.
- **RADIUS Only:** RADIUS is enabled. Local authentication is disabled.



Caution

If **RADIUS Only** is selected, and the RADIUS server is unavailable, improperly identified, or improperly configured, you must use a serial connection to the control console and change the Access setting to Local Authentication Only or RADIUS, then Local Authentication to regain access.

RADIUS (Administration>Security>Remote Users>RADIUS)

Use this option to do the following:

- Display a list of RADIUS servers identified as being available to the InRow SC and the time-out period for each server (the number of seconds the InRow SC will wait for a reply from the server before the request fails).
- Add a server to the list of identified RADIUS servers. Configure the following parameters for authentication by the new server, click a listed RADIUS server to display and modify its parameters.

| RADIUS Setting | Definition |
|------------------------|---|
| RADIUS Server | The server name or IP address of the RADIUS server. NOTE: RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address. |
| Secret | The shared secret between the RADIUS server and the InRow SC. |
| Timeout | The time, in seconds, that the InRow SC waits for a response from the RADIUS server. |
| Test Settings | Enter the Administrator user name and password to test the RADIUS server path that you have configured. |
| Skip Test and Apply | Do not test the RADIUS server path. |
| Switch Server Priority | Change which RADIUS server will authenticate users if two configured servers are listed and RADIUS, then Local Authentication or RADIUS Only is the enabled authentication method. |

Configuring the RADIUS Server

You must configure your RADIUS server to work with the InRow SC. The following procedure summarizes the steps to perform.



See also

For examples of the file entries needed to configure a RADIUS server for use with an InRow SC, see the *Security Handbook*, available on the *Utility CD* or from the APC Web site, www.apc.com.

Summary of the configuration procedure

1. Add the IP address of the InRow SC to the RADIUS server client list (file).



Note

RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.

2. The users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined instead. If no Service-Type attribute is configured, the user will have read-only access (to the Web interface only).



See also

See your RADIUS server documentation for information about the RADIUS users file, and see the *APC Security Handbook* for an example.

3. Vendor Specific Attributes (VSA) can be used instead of the Service-Type attributes provided by your RADIUS server. This method requires a dictionary entry and a RADIUS users file. In the dictionary file, you can define the names for the ATTRIBUTE and VALUE keywords, but not the numeric values. If you change the numeric values, RADIUS authentication and authorization will fail VSAs take precedence over standard RADIUS attributes.



See also

For examples of the RADIUS users file with VSAs and an example of an entry in the dictionary file on the RADIUS server, see the *APC Security Handbook*.

Configuring a RADIUS server on UNIX[®], with shadow passwords

If UNIX shadow password files are used (/etc/passwd) in conjunction 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.

```
DEFAULTAuth-Type = System
```

```
APC-Service-Type = Admin
```

To allow only Device-Users, change the value for APC-Service-Type to `Device`.

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

```
bconnersAuth-Type = System
```

```
APC-Service-Type = Admin
```

```
thawkAuth-Type = System
```

```
APC-Service-Type = Device
```

Supported RADIUS servers

APC supports FreeRADIUS, Microsoft Windows 2000 Server, and Microsoft Windows 2000 RADIUS Server. Other commonly available RADIUS applications may work but have not been fully tested by APC.

Inactivity Timeout (Administration>Security>Auto Log Off)

Use this option to configure the time (3 minutes by default) that the system waits before logging off an inactive user.

Administration: Network Features

TCP/IP and Communication Settings

TCP/IP settings (Administration>Network>TCP/IP)

The **TCP/IP** option on the left navigation menu, selected by default when you choose **Network** on the top menu bar, displays the current IP address, subnet mask, default gateway, and MAC address of the InRow SC.

On the same page, **TCP/IP Configuration** provides the following options for how the TCP/IP settings will be configured when the InRow SC turns on, resets, or restarts: **Manual**, **BOOTP**, **DHCP**, and **DHCP & BOOTP**.



See also

For information on DHCP and DHCP options, see **RFC2131** and **RFC2132**.

| Setting | Description |
|---|--|
| Manual | The IP address, subnet mask, and default gateway must be configured manually. Click Next>> , and enter the new values. |
| BOOTP | <p>A BOOTP server provides the TCP/IP settings. At 32-second intervals, the InRow SC requests a network assignment from any BOOTP server:</p> <ul style="list-style-type: none"> • If it receives a valid response, it starts the network services. • If it finds a BOOTP server, but a request to that server fails or times out, the InRow SC stops requesting, network settings until it is restarted. • By default, 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 so that it remains accessible. <p>Click Next>> to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail ¹:</p> <ul style="list-style-type: none"> • Maximum retries: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries. • If retries fail: Select Use prior settings (the default) or Stop BOOTP request. |
| DHCP | <p>At 32-second intervals, the InRow SC requests network assignment from any DHCP server, by default, the number of retries is unlimited.</p> <ul style="list-style-type: none"> • If it receives a valid response, by default it requires the APC cookie from the DHCP server in order to accept the lease and start the network services. • If it finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted. <p>To change these values, click Next>> for the DHCP Configuration page¹:</p> <ul style="list-style-type: none"> • Require vendor specific cookie to accept DHCP Address: Disable or enable the requirement that the DHCP server provide the APC cookie. • Maximum retries: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries. |
| <p>1. The default values for these three settings on the configuration pages generally do not need to be changed:</p> <ul style="list-style-type: none"> • Vendor Class: APC • Client ID: The MAC address of the InRow SC, which uniquely identifies it on the local area network (LAN) • User Class: The name of the application firmware module | |

| Setting | Description |
|--|--|
| DHCP & BOOTP | <p>The default setting. The InRow SC tries to obtain its TCP/IP settings from a BOOTP server first, and then, if it cannot discover a BOOTP server, from a DHCP server. If it obtains its TCP/IP settings from either server, it switches this setting to BOOTP or DHCP, depending on the type of server that supplied the TCP/IP settings to the InRow SC.</p> <p>Click Next>> to configure the same settings that are on the BOOTP Configuration and DHCP Configuration pages¹ and to specify that the DHCP and BOOTP setting be retained after either type of server provides the TCP/IP values.</p> |
| <p>1. The default values for these three settings on the configuration pages generally do not need to be changed:</p> <ul style="list-style-type: none"> •Vendor Class: APC •Client ID: The MAC address of the InRow SC, which uniquely identifies it on the local area network (LAN) •User Class: The name of the application firmware module | |

DHCP response options

Each valid DHCP response contains options that provide the TCP/IP settings that the InRow SC needs to operate on a network, and other information that affects the operation of the InRow SC.

Vendor Specific Information (option 43). The InRow SC uses this option in a DHCP response to determine whether the DHCP response is valid. This option contains up to two APC-specific options in a TAG/LEN/DATA format: the APC Cookie and the Boot Mode Transition.

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

Option 43 communicates to the InRow SC that a DHCP server is configured to service APC devices. By default, this DHCP response option must contain the APC cookie for the InRow SC to accept the lease.



To disable the requirement of an APC cookie, see [DHCP](#).

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
```

- **Boot Mode Transition. Tag 2, Len 1, Data 1/2**

This option 43 setting enables or disables **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**, which, by default, is disabled.

- A data value of 1 enables **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**. Whenever the In Row SC reboots, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.
 - A data value of 2 disables the option **Remain in DHCP & BOOTP mode after accepting TCP/IP settings** option. The **TCP/IP Configuration** setting option switches to **DHCP** when the accepts the DHCP response. Whenever the InRow SC reboots, it will request its network assignment from a DHCP server only.
- Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie and the disable Boot Mode Transition setting:

```
Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43 0x02 0x01 0x01
```

TCP/IP options. The **InRow SC** 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 InRow SC.
- **Subnet Mask** (option 1): The Subnet Mask value that the InRow SC needs to operate on the network.
- **Router**, i.e., Default Gateway (option 3): The default gateway address that the InRow SC needs to operate on the network.
- **IP Address Lease Time** (option 51): The time duration for the lease of the IP Address to the InRow SC.
- **Renewal Time, T1** (option 58): The time that the In Row SC 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 InRow SC must wait after an IP address lease is assigned before it can seek to rebind that lease.

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

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

Port Speed (Administration>Network>Port Speed)

The **Port Speed** setting defines the communication speed of the TCP/IP port.

- For **Auto-negotiation** (the default), Ethernet devices negotiate to transmit at the highest possible speed, but if the supported speeds of two devices are unmatched, the slower speed is used.
- Alternatively, you can choose 10 Mbps or 100 Mbps, each with the option of half-duplex (communication in only one direction at a time) or full-duplex (communication in both directions on the same channel simultaneously).

DNS (Administration>Network>DNS>options)

Use the options under **DNS** on the left navigation menu to configure and test the Domain Name System (DNS):

- Select **servers** to specify the IP addresses of the primary and optional secondary DNS server. For the InRow SC to send e-mail, at least the IP address of the primary DNS server must be defined.
 - The InRow SC waits up to 15 seconds for a response from the primary DNS server or the secondary DNS server (if a secondary DNS server is specified). If the InRow SC does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the InRow SC or on a nearby segment (but not across a wide-area network [WAN]).
 - After you define the IP addresses of the DNS servers, verify that DNS is working correctly by entering the DNS name of a computer on your network to look up the IP address for that computer.
- Select **naming** to define the host name and domain name of the InRow SC:
 - **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 InRow SC interface (except e-mail addresses) that accepts a domain name.
 - **Domain Name:** You need to configure the domain name here only. In all other fields in the InRow SC interface (except e-mail addresses) that accept domain names, the InRow SC adds this domain name when only a host name is entered.
 - To override all instances of the expansion of a specified host name by the addition of the domain name, set the 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 InRow SC 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.

- Select **test** to send a DNS query that tests the setup of your DNS servers:
 - As **Query Type**, select the method to use for the DNS query:
 - **by Host**: the URL name of the server
 - **by FQDN**: the fully qualified domain name
 - **by IP**: the IP address of the server
 - **by MX**: the Mail Exchange used by the server
 - As **Query Question**, identify the value to be used for the selected query type:

| Query Type Selected | Query Question to Use |
|---------------------|---|
| by Host | The URL |
| by FQDN | The fully qualified domain name, <i>my_server.my_domain.com</i> . |
| by IP | The IP address |
| by MX | The Mail Exchange address |

- View the result of the test DNS request in the **Last Query Response** field.

Web (Administration>Network>Web>options)

| Option | Description |
|-------------------|---|
| access | <p>To activate changes to any of these selections, log off from the InRow SC:</p> <ul style="list-style-type: none">• Disable: Disables access to the Web interface. (You must use the control console to re-enable access. Select Network and Web/SSL/TLS. Then for HTTP, select Access and Enabled. For HTTPS access, also select Web/SSL and Enabled.)• Enable HTTP (the default): Enables Hypertext Transfer Protocol (HTTP), which provides Web access by user name and password, but does not encrypt user names, passwords, and data during transmission.• Enable HTTPS: Enables Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer (SSL). SSL encrypts user names, passwords, and data during transmission, and authenticates the InRow SC by digital certificate. When HTTPS is enabled, your browser displays a small lock icon. <p>See “Creating and Installing Digital Certificates” in the <i>Security Handbook</i> on the <i>Utility</i> CD to choose among the several methods for using digital certificates.</p> <p>HTTP Port: The TCP/IP port (80 by default) used to communicate by HTTP with the InRow SC.</p> <p>HTTPS Port: The TCP/IP port (443 by default) used to communicate by HTTPS with the InRow SC.</p> <p>For either of these ports, you can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and the InRow SC IP address of 152.214.12.114:</p> <pre>http://152.214.12.114:5000 https://152.214.12.114:5000</pre> |
| ssl cipher suites | <p>Enable or disable any of the SSL encryption ciphers and hash algorithms:</p> <ul style="list-style-type: none">• DES: A block cipher that provides authentication by Secure Hash Algorithm.• RC4_MD5 (enabled by default): A stream cipher that provides authentication by MD5 hash algorithm.• RC4_SHA (enabled by default): A stream cipher that provides authentication by Secure Hash Algorithm.• 3DES: A block cipher that provides authentication by Secure Hash Algorithm. |

| Option | Description |
|-----------------|--|
| ssl certificate | <p>Add, replace, or remove a security certificate.</p> <p>Status:</p> <ul style="list-style-type: none"> • 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, /sec on the InRow SC. • Generating: The InRow SC is generating a certificate because no valid certificate was found. • Loading: A certificate is being activated on the InRow SC. • Valid certificate: A valid certificate was installed or was generated by the InRow SC. Click on this link to view the certificate's contents. <p>If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the InRow SC generates a default certificate, a process which delays access to the interface for up to five minutes. You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on.</p> <p>Add or Replace Certificate File: Enter or browse to the certificate file created with the Security Wizard.</p> <p>See "Creating and Installing Digital Certificates" in the <i>Security Handbook</i> on the <i>Utility</i> CD to choose a method for using digital certificates created by the Security Wizard or generated by the InRow SC.</p> <p>Remove: Delete the current certificate.</p> |

Console (Administration>Network>Console>options)

| Option | Description |
|----------------|--|
| access | <p>Choose one of the following for access by Telnet or Secure SHell (SSH):</p> <ul style="list-style-type: none">• Disable: Disables all access to the control console.• Enable Telnet (the default): Telnet transmits user names, passwords, and data without encryption.• Enable SSH v1 and v2: Do not enable both versions 1 and 2 of SSH unless you require both. They use extensive processing power.• Enable SSH v1 only: SSH version 1 encrypts user names, passwords, and data for transmission. There is little or no delay as you log on.• Enable SSH v2 only: SSH version 2 transmits user names, passwords, and data in encrypted form with more protection than version 1 from attempts to intercept, forge, or alter data during transmission. There is a noticeable delay as you log on. <p>Configure the ports to be used by these protocols:</p> <ul style="list-style-type: none">• Telnet Port: The Telnet port used to communicate with the InRow SC (23 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) or a space, as required by your Telnet client program, to specify the non-default port. For example, for port 5000 and the InRow SC IP address of 152.214.12.114, your Telnet client requires one of the these commands: <pre>telnet 152.214.12.114:5000 telnet 152.214.12.114 5000</pre>• SSH Port: The SSH port used to communicate with the InRow SC (22 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. See the documentation for your SSH client for the command line format required to specify a non-default port. |
| ssh encryption | <p>Enable or disable encryption algorithms (block ciphers) compatible with SSH version 1 or version 2 clients.</p> <p>If your SSH v1 client cannot use Blowfish, you must also enable DES.</p> <p>Your SSH v2 client selects the enabled algorithm that provides the highest security. If the client cannot use the default algorithms (3DES or Blowfish), enable an AES algorithm that it can use (AES 128 or AES 256)</p> |

| Option | Description |
|--------------|---|
| ssh host key | <p>Status indicates the status of the host key (private key):</p> <ul style="list-style-type: none"> • SSH Disabled: No host key in use: When disabled, SSH cannot use a host key. • Generating: The InRow SC is creating a host key because no valid host key was found. • Loading: A host key is being activated on the InRow SC. • Valid: One of the following valid host keys is in the /sec directory (the required location on the InRow SC): <ul style="list-style-type: none"> • A 1024-bit host key created by the APC Security Wizard • A 768-bit RSA host key generated by the InRow SC <p>Add or Replace: Browse to and upload a host key file created by the Security Wizard:</p> <p>If you use FTP or Secure CoPy (SCP) instead to transfer the host key file, you must specify the /sec directory as the target location in the command.</p> <p>To use the APC Security Wizard, see the <i>Security Handbook</i> on the <i>Utility CD</i>.</p> <p>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 InRow SC takes up to 5 minutes to create a host key, and the SSH server is not accessible during that time.</p> <p>Remove: Remove the current host key.</p> |



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

SNMP (Administration>Network>SNMP>options)

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 InfraStruXure Manager to manage an InRow SC on the public network of an InfraStruXure system, you must have SNMP enabled in the InRow SC. Read access will allow InfraStruXure Manager to receive traps from the InRow SC, but Write access is required while you use the interface of the InRow SC to set InfraStruXure Manager as a trap receiver.



See also

For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available on the *Utility CD* or from the APC Web site, www.apc.com.

| Option | Description |
|--------|--|
| access | <p>Enable or disable SNMP. With SNMP enabled (the default), the access control option controls how each of the four available SNMP communities is used.</p> <p>To define up to four NMSs as trap receivers, see Trap Receivers (Administration>Notification>SNMP Traps>trap receivers).</p> <p>To use SNMP to manage the InRow SC, see the <i>PowerNet Management Information Base (MIB) Reference Guide</i> on the <i>Utility CD</i>.</p> |

| Option | Description |
|----------------|---|
| access control | <p>Community Name: The password (maximum of 15 characters) that an NMS defined by the NMS IP/Host Name setting uses to access the community.</p> <p>NMS IP/Host Name: Access is granted only to the Network Management System (NMS) specified by the host name or only to the NMSs specified by one of the IP address formats in the following examples:</p> <ul style="list-style-type: none"> • 159.215.12.1: Only the NMS at the IP address 159.215.12.1. • 159.215.12.255: Any NMS on the 159.215.12 segment. • 159.215.255.255: Any NMS on the 159.215 segment. • 159.255.255.255: Any NMS on the 159 segment. • 0.0.0.0 or 255.255.255.255: Any NMS. <p>Access Type: Define how any NMS specified by NMS IP/Host Name and using the correct community name can access the community.</p> <ul style="list-style-type: none"> • Read: The NMS can use GETs at any time, but it can never use SETs. • Write: The NMS can use GETs at any time and can use SETs when no one is logged on to the InRow SC. • Disabled: The NMS cannot use GETs or SETs. • Write+: The NMS can use GETs and SETs at any time, even when someone is logged on to the InRow SC. |

FTP Server (Administration>Network>FTP Server)

The **FTP server** settings enable (by default) or disable access to the FTP server and specify the TCP/IP port (21 by default) that the FTP server uses to communicate with the InRow SC. The FTP server uses both the specified port and the port one number lower than the specified port.

You can change the **Port** setting to the number of any unused port from 5001 to 32768 for added security. Users must then use a colon (:) to specify the non-default port number. For example, for port 5001 and IP address 152.214.12.114, the command would be `ftp 152.214.12.114:5001`.



Note

FTP transfers files without encryption. For higher security, disable the FTP server, and transfer files with Secure CoPy (SCP). Selecting and configuring Secure SHell (SSH) enables SCP automatically.

At any time that you want the InRow SC to be accessible for management by InfraStruXure Manager, FTP Server must be enabled in the InRow RC interface.



See also

For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available on the *Utility* CD or from the APC Web site, www.apc.com.

Administration: Notification and Logging

Event Actions (Administration>Notification>Event Actions>options)

Types of notification

You can configure event actions to occur in response to an event or a group of events. These actions notify users of the event in any of several ways:

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



To set up additional methods of active notification that are not included in the **Event Action** options, see [Configuration](#) for information on configuring the output sensor.

- Indirect notification through the event log. If none of the direct notification methods are configured, users must check the log to determine which events have occurred.



Another method of indirect notification, not included in the **Event Action** options, is the use of informational queries. See [access control](#), under [SNMP \(Administration>Network>SNMP>options\)](#) for a description of SNMP access types that enable a Network Management System (NMS) to perform informational queries. Configuring the most restrictive SNMP access type, READ, enables informational queries without the risk of allowing remote configuration changes.

Configuring event actions

You can configure event actions for individual events or for pre-defined groups of events.

Configuring by event. To define event actions for an individual event:

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu.
2. Follow the on-screen instructions to list events by severity, either by main category or sub-category.
3. In the list of events, check the marked columns to see whether the action you want is already configured for the event. (By default, logging is configured for all events.)
4. For details of the current configuration, such as the recipients to be notified by e-mail or the Network Management Systems (NMSs) to be notified by SNMP traps, click on the event name.
5. Add to or change the event configuration.



Note

A Syslog server must be configured before you can display or use the Syslog option, and at least one e-mail recipient or trap receiver must be configured before you can display or use the detailed e-mail and trap notification options.

- Mark the check-boxes to enable (or unmark them to disable) event logging or Syslog for this event.
- Click on any e-mail recipient or trap receiver, and specify any value up to three digits to configure the following detailed options.
 - How long, in seconds or minutes, the InRow SC waits after the event occurs before sending e-mail to the selected e-mail recipient or a trap to the selected trap receiver. If the event clears during this delay period, no notification is sent. To configure a delay longer than 999 seconds (16 minutes, 39 seconds), use minutes.

- How frequently to send e-mail to the selected e-mail recipient or a trap to the selected trap receiver. E-mail or a trap repeats at the time interval specified here in seconds, minutes, or hours, unless the event has cleared.
- The number of times to send e-mail to the selected e-mail recipient or a trap to the selected trap receiver. Choose to send e-mail or a trap a specified number of times or to repeat the notification an unlimited number of times. In either case, notification stops if the event clears.



When configuring events, you can enable or disable notification to configured e-mail recipients, Syslog servers, or trap receivers, but you cannot add or remove any recipients, receivers, or Syslog servers. To add or remove recipients, receivers, or servers, see [Identifying Syslog Servers \(Logs>Syslog>servers\)](#), [E-mail recipients \(Administration>Notification>E-mail>recipients\)](#), and [Trap Receivers \(Administration>Notification>SNMP Traps>trap receivers\)](#).

Configuring by group. To configure a group of events simultaneously:

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by group** under **Event Actions** on the left navigation menu.
2. Choose how you want events to be grouped for configuration:
 - If you choose **Grouped by severity**, you can then select all events of one or more severity types.



Note

When configuring events by severity, you must use their existing severity. You cannot change the severity of an event.

- If you choose **Grouped by category**, you can then select all events in one or more pre-defined categories.

3. Select event actions for all events in the group.



Note

A Syslog server must be configured in order to display or use the Syslog option, and at least one e-mail recipient (for e-mail notification) or at least one trap receiver (for notification by SNMP traps) must be configured in order to display the detailed e-mail and trap receiver notification options.

- Click the **Logging** button to choose logging for all events in the group. Click **Next>>**, and then mark the check-boxes to enable (or unmark them to disable) event logging or Syslog for these events.
- Click the **E-mail Recipients** or **Trap Receivers** button, click **Next>>**, and select an e-mail recipient or trap receiver. Then specify any value up to three digits to configure the following detailed options.
 - How long, in seconds or minutes, the InRow SC waits after one of these events occurs before sending e-mail to the selected e-mail recipient or a trap to the selected trap receiver. If the event clears during this delay period, no notification is sent. To configure a delay longer than 999 seconds (16 minutes, 39 seconds), use minutes.
 - How frequently to send e-mail to the selected e-mail recipient or a trap to the selected trap receiver. E-mail or a trap repeats at the time interval specified here in seconds, minutes, or hours, unless the event has cleared.
 - The number of times to send e-mail to the selected e-mail recipient or a trap to the selected trap receiver. Choose to send e-mail or a trap a specified number of times or to repeat the notification an unlimited number of times. In either case, notification stops if the event clears.



To add or remove recipients or receivers, see [E-mail recipients \(Administration>Notification>E-mail>recipients\)](#) or [Trap Receivers \(Administration>Notification>SNMP Traps>trap receivers\)](#).

4. Click **Next>>**, and then click **Apply** to confirm the displayed selections.
5. Click **Finish** to return to the **by group** page, or select **Configure Additional Actions** to keep the selected event group and to configure the remaining **Logging**, **E-mail Recipients**, or **Trap Receivers** actions for this group.

Active, Automatic, Direct Notification

E-mail notification

Overview of setup. Use the 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, of the secondary Domain Name System (DNS) servers



See [DNS \(Administration>Network>DNS>options\)](#).

- The IP address or DNS name for **SMTP Server** and the **From Address** setting for SMTP



See [SMTP \(Administration>Notification>E-mail>server\)](#).

- The e-mail addresses for a maximum of four recipients



To configure recipients, see [E-mail recipients \(Administration>Notification>E-mail>recipients\)](#).



Note

You can use the **To Address** setting of the **recipients** option to send e-mail to a text-based pager.

SMTP (Administration>Notification>E-mail>server). Use this option to define the following settings:

| Setting | Description |
|-------------------|--|
| Local SMTP Server | <p>The IP address (or if DNS is configured, the DNS name) of the local SMTP server.</p> <p>NOTE:This definition is required only when SMTP Server is set to Local. See E-mail recipients (Administration>Notification>E-mail>recipients).</p> |
| From Address | <p>The contents of the From field in the format <i>user@ [IP_address]</i> (if an IP address is specified as Local SMTP Server) or <i>user@domain.com</i> (if DNS is configured and the DNS name is specified as Local SMTP Server) in the e-mail messages sent by the InRow SC.</p> <p>NOTE:The local SMTP server may require that you use a valid user account on the server for this setting. See the server's documentation for more information.</p> |

E-mail recipients (Administration>Notification>E-mail>recipients). Identify up to four e-mail recipients.

| Setting | Description |
|-------------------|---|
| To Address | <p>Defines the user and domain names of the recipient. To use e-mail for paging, use the e-mail address for that recipient's pager gateway account (for example, <code>myacct100@skytel.com</code>). The pager gateway will generate the page.</p> <p>You can bypass the DNS lookup of the mail server's IP address by using the IP address in brackets instead of the e-mail domain name. For example, use <code>jsmith@[xxx.xxx.x.xxx]</code> instead of <code>jsmith@company.com</code>. This is useful when DNS lookups are not working correctly.</p> <p>NOTE: The recipient's pager must be able to use text-based messaging.</p> |
| SMTP Server | <p>Select one of the following methods for routing e-mail:</p> <ul style="list-style-type: none"> • Local: Through the SMTP server of the InRow SC (the recommended setting). This option ensures that the e-mail is sent before the InRow SC's 20-second time-out, and, if necessary, is retried several times. Also do one of the following: <ul style="list-style-type: none"> • Enable forwarding at the InRow SC, so that the SMTP server can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Always check with the administrator of your SMTP server before changing its configuration to allow forwarding. • Set up a special e-mail account for the InRow SC to forward e-mail to an external mail account. • Recipient: Directly to the recipient's SMTP server. On a busy remote SMTP server, the time-out may prevent some e-mail from being sent because, with this option, the InRow SC tries to send the e-mail only once. <p>When the recipient uses the InRow SC SMTP server, this setting has no effect.</p> |
| E-mail Generation | Enables (by default) or disables sending e-mail to the recipient. |

E-mail test (Administration>Notification>E-mail>test). Use this option to send a test message to a configured recipient.

SNMP Traps

Trap Receivers (Administration>Notification>SNMP Traps>trap receivers).

Define the **Trap Receiver** settings that determine which Network Management Systems (NMSs) receive traps.

| Item | Definition |
|----------------------|--|
| Community Name | The password (maximum of 15 characters) used when traps are sent to the NMS identified by the NMS IP/Host Name setting. |
| NMS IP/Host Name | The IP address or host name of the NMS that will receive traps. 0.0.0.0 (the default value) causes traps not to be sent to any NMS. |
| Trap Generation | Enables (by default) or disables the sending of any traps to the NMS identified by the NMS IP/Host Name setting. |
| Authentication Traps | Enables or disables the sending of authentication traps to the NMS identified by the NMS IP/Host Name setting. |

SNMP Trap Test (Administration>Notification>SNMP Traps>test). Use this option to test the sending of a trap to a configured trap receiver.

Syslog (Logs>Syslog>options)

By default, the InRow SC can send messages to up to four Syslog servers whenever events occur. The Syslog servers, which must be specifically identified by their IP addresses or host names, record the events that occur at network devices in a log that provides a centralized record of events.



See also

This user's guide does not describe Syslog or its configuration values in detail. For more information about Syslog, see RFC3164, at www.ietf.org/rfc/rfc3164.txt?number=3164.

Identifying Syslog Servers (Logs>Syslog>servers). Use this option to identify one or more Syslog servers that will receive Syslog messages and to specify a port for each.

| Setting | Definition |
|---------------|--|
| Syslog Server | Uses specific IP addresses or host names to identify up to four servers that will receive Syslog messages sent by the InRow SC. NOTE: To use the Syslog feature, Syslog Server must be defined for at least one server. |
| Port | Identifies the user datagram protocol (UDP) port that the InRow SC will use to send Syslog messages. The default is 514 , the number of the UDP port assigned to Syslog. |

Syslog Settings (Logs>Syslog>settings). Leave the Syslog settings, except the **Server IP** settings, set to their defaults.

| Setting | Definition |
|--------------------|--|
| Message Generation | Enables (by default) or disables the Syslog feature. |
| Facility Code | Selects the facility code assigned to the InRow SC's Syslog messages (User , by default). NOTE: User is the selection that best defines the Syslog messages sent by the InRow SC. Do not change this selection unless advised to do so by the Syslog network or system administrator. |

| Setting | Definition |
|------------------|---|
| Severity Mapping | <p>Maps each of the severity levels assigned to InRow SC events to the available Syslog priorities. You should not need to change the default mappings.</p> <p>The following definitions are from RFC3164:</p> <ul style="list-style-type: none"> • 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 <p>Following are the default settings for the four Local Priority settings:</p> <ul style="list-style-type: none"> • Severe is mapped to Critical • Warning is mapped to Warning • Informational is mapped to Info • None (for events that have no severity level assigned) is mapped to Info <p>NOTE: To disable sending Syslog messages for Severe, Warning, or Informational events, see Configuring event actions.</p> |

Syslog Test and Format Example (Logs>Syslog>test). Send a test message to the Syslog servers configured through the **servers** option (**Logs>Syslog>servers**):

1. Select a severity to assign to the test message.
2. Define the test message, using any text that is formatted according to the required message (MSG) fields. The message fields, which you format, are one of the three parts of the Syslog message that will be sent: For example, **APC: Test Syslog** meets the formatting requirements.
 - The priority (PRI) identifies the Syslog priority assigned to the message's event and the facility code assigned to messages sent by the InRow SC.
 - The Header includes a time stamp and the IP address of the InRow SC.

- The message (MSG) part has two fields:
 - A TAG field, which is followed by a colon and a space, identifies the event type.
 - A CONTENT field provides the event text, followed (optionally) by a space and the event code.

Indirect Notification through Logs or Queries

Event log (Logs>Events>options)

Display and use the event log (Logs>Events>log). View or delete the contents of the event log. The event log displays all events recorded since the log was last deleted or since the log reached its maximum capacity and the older half was deleted automatically. Events are in reverse chronological order. By default, all events are logged:

- You can view the event log as a page of the Web interface (the default view) or click **Launch Log in New Window** from that page to display a full-screen view of the log, enabling you to see more of the listed events without scrolling.



Note

If your browser is Microsoft Internet Explorer, JavaScript must be enabled for you to use the **Launch Log in New Window** button.



Alternatively, you can use FTP or Secure CoPy (SCP) to view the event log. See [How to use FTP or SCP to retrieve the log files](#).

- To delete all events recorded in the log, click **Clear Event Log** on the Web page that displays the log. Deleted events cannot be retrieved.

To disable the logging of events based on their assigned severity level or their event category, configure event actions by group.



See [Configuring by group](#).

To access lists of all configurable events and how they are currently configured, select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu, and then click, in turn, on each major category of event.



See [Configuring by event](#).

Reverse Lookup (Logs>Events>reverse lookup). Reverse lookup is disabled by default. Enable this feature unless you have no DNS server configured or have poor network performance because of heavy network traffic.

With reverse lookup enabled, when a network-related event occurs, both the IP address and the domain name for the networked device associated 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 much less frequently than IP addresses, enabling reverse lookup can improve the ability to identify addresses of networked devices that are causing events to occur.

Data log (Logs>Data>options)

Displaying and using the data log (Logs>Data>log). Use this option to access a log that stores periodic measurements of the ambient temperature for each sensor managed by the InRow SC. Each entry is listed by the date and time the data was recorded and provides the data in a column format.

Click **Launch Log in New Window** to launch the data log in a new browser window that provides a full-screen view.



Note

If your browser is Microsoft Internet Explorer, JavaScript must be enabled for you to use the **Launch Log in New Window** button.



Alternatively, you can use FTP or Secure CoPy (SCP) to view the data log. See [How to use FTP or SCP to retrieve the log files](#).

Click **Clear Data Log** to delete all data recorded in the log. Deleted data cannot be retrieved.

Setting the data collection interval (Logs>Data>interval). Use this option to define, in the **Log Interval** setting, how frequently data is sampled and stored in the data log. This Web interface page also reports how many days of data the log can store, based on the interval you selected.

When the log is full, the older half of the log is deleted and the newer half is retained. To avoid automatic deletion of older data, enable and configure data log rotation, as described in the next section.

Configuring data log rotation (Logs>Data>rotation). Use this option to set up a password-protected data log repository on a specified FTP server. Enabling rotation causes a copy of any previously unsaved entries in the data log to be appended to the file you specify by name and location. Updates to this file occur either at the upload interval that you specify, in hours, or when the data log has reached its maximum size (if the maximum size is reached before the upload interval expires).

| Parameter | Description |
|--------------------|---|
| Data Log Rotation | Enable or disable (the default) data log rotation. |
| FTP Server Address | The location (IP address or host name) of the FTP server where the data repository file is stored. |
| User Name | The user name 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. |
| Password | The password required to send data to the repository file. |
| File Path | The path to the repository file. |
| File Name | The name of the repository ASCII text file. |

| Parameter | Description |
|------------------------------------|---|
| Delay <i>hours</i> between Uploads | The number of hours between uploads of data to the specified file. |
| Number of Retries | The number of times the upload will be attempted after an initial failure. |
| Retry Delay | The time that the system waits before retrying an upload after a failed attempt. You can specify that the upload will be retried repeatedly until it succeeds, or you can limit the number of retries. If you specify a limited number of retries, and the upload has been retried unsuccessfully the specified number of times (Number of Retries), the scheduled upload is skipped, and the system waits the number of hours specified as Delay hours between Uploads . |

To initiate the initial upload of data to the repository file immediately, click **Upload Now!**

How to use FTP or SCP to retrieve the log files

If you are an Administrator or Device-only User, you can use FTP or SCP to retrieve a tab-delineated event log file (*event.txt*) or data log file (*data.txt*) that you can import into a spreadsheet application.

- The file reports all of the events recorded since the log was last deleted.
- The file includes information that the event 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 InRow SC
 - The unique **Event Code** for each recorded event (event log only)



Note

The InRow SC 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 of the year.

If you are using the encryption-based security protocols for your system, use Secure CoPy (SCP) to retrieve the log file. (You should have FTP disabled.)

If you are using unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.



See also

See the *Security Handbook*, available on the *Utility CD* and on the APC Web site (www.apc.com) for information on the available protocols and methods for setting up the type of security appropriate for your needs.

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

```
scp username@hostname_or_ip_address:event.txt ./event.txt
```

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

```
scp username@hostname_or_ip_address:data.txt ./data.txt
```

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

1. At a command prompt, type `ftp` and the InRow SC's IP address, and press ENTER. If the **Port** setting for the **FTP Server** option (which you select on the **Network** menu of the **Administration** tab) has been changed from its default value (**21**), you must use the non-default value in the FTP command. For Windows 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 \(Administration>Network>FTP Server\)](#). You can specify any port from 5001 to 32768.

2. Use the case-sensitive **User Name** and **Password** for either an Administrator or a Device User to log on.
3. For Administrator, **apc** is the default for **User Name** and **Password**.
4. For the Device User, **device** is the default for **User Name**, and **apc** is the default for **Password**.

5. Use the **get** command to transmit the text-version of the event log or data log to your local drive.
ftp>get event.txt
or
ftp>get data.txt
6. You can use the **del** command to clear the contents of the event log or data 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 is created to record the deleted-log event.
7. Type `quit` at the `ftp>` prompt to exit from FTP.

Queries (Modbus requests and SNMP GETs)



See [Serial Modbus \(Administration>General>Serial Modbus\)](#) for information on configuring and using the request/response structure of building management systems using the Modbus protocol, and see [access control](#), under [SNMP \(Administration>Network>SNMP>options\)](#) for a description of SNMP access types that enable an NMS to perform informational queries. Configuring the most restrictive SNMP access type, READ, enables informational queries without the risk of allowing remote configuration changes.

Administration: General Options

Information about the InRow SC

Information you configure (Administration>General>Identification)

Use this option to define the System **Name**, **Location**, and **Contact** values used by the InRow SC SNMP agent. The option's settings provide the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifications (OIDs).

For example, you might configure **Name** as Test Lab, **Location** as Building 3, and **Contact** (whom to contact about the device) as Donald Adams.



For more information about the MIB-II OIDs, see the *PowerNet SNMP Management Information Base (MIB) Reference Guide* provided on the Utility CD and on the APC Web site, www.apc.com.

Hardware and firmware information (Administration>General>Factory Info)

The hardware information is especially useful to APC Customer Support in helping to troubleshoot problems with your InRow SC. The serial number and MAC address accessible through the **Factory Info** menu option are also available on the InRow SC itself.

Firmware information, listed under Application Module and APC OS (AOS), indicates the name, firmware version number, and the date and time each firmware module was created. This information may also be useful in troubleshooting and enables you to determine quickly if updated firmware is available to download from the APC Web site.

Date, Time, and Temperature

Date and time (Administration>General>Date & Time>options)

How date and time will be set (Administration>General>Date & Time>mode).

Use this option to set the time and date used by the InRow SC. The option displays the current settings, and allows you to change those settings manually, or through a Network Time Protocol (NTP) Server.

- **Manual:** Use this selection to do one of the following:
 - Enter the date and time for the InRow SC.
 - Mark the checkbox **Apply Local Computer Time** to match the date and time settings of the computer you are using, and click **Apply**.
- **Synchronize with NTP Server:** Use this selection to have an NTP Server define the date and time for the InRow SC.

| Setting | Definition |
|----------------------|---|
| 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. |
| Time Zone | Select a time zone. The number of hours preceding each time zone in the list is the offset from UTC (Coordinated Universal Time, Temps Universel Coordonné, formerly Greenwich Mean Time), the international time standard. |
| Update Interval | Define how often, in hours, the InRow SC accesses the NTP Server for an update. The minimum is 1 hour; the maximum is 8760 hours (1 year). |
| Update Using NTP Now | Initiate an immediate update of the date and time by the NTP Server. |

Enable and configure Daylight Saving Time (Administration>General>Date & Time>daylight saving). Use this option to enable either traditional United States Daylight Saving Time (DST) or to enable and configure a customized daylight saving time, with starting and ending dates and time that you specify to match how Daylight Saving Time is implemented in your local area. DST is disabled by default.

When customizing Daylight Saving Time:

- If the local Daylight Saving Time always starts or ends on the 4th occurrence of a specific weekday of a month (for example, the 4th Sunday), choose Fourth/Last. If a 5th Sunday occurs in that month in a subsequent year, the time setting will still change to or from Daylight Saving Time on the 4th Sunday.
- If the local Daylight Saving Time always starts or ends on the last occurrence of a specific weekday of a month, such as the last Sunday of that month, regardless of whether the last Sunday is the 4th or the 5th Sunday, choose Fifth/Last.

Selecting a date format (Administration>General>Date & Time>date format).

Select the numerical format in which to display all dates in this user interface. In the selections, each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.

Temperature scale (Administration>General>Temp Scale)

Select the temperature scale (Fahrenheit or Celsius) in which to display all temperature measurements in this user interface.



Note

Changing the temperature scale will also change other unit settings between metric and English. Settings that will be affected include flow rates and pressure measurements.

Serial Modbus (Administration>General>Serial Modbus)

To configure Modbus, select the **Administration** tab, **General** on the top menu bar, and **Serial Modbus** on the left navigation menu. You can enable or disable Modbus, choose a baud rate, and specify a unique identifier.

Modbus defines a request/response message structure for a client/server environment. The APC implementation of Modbus uses Remote Terminal Unit (RTU) mode. You can use Modbus to view the InRow SC through your building management system interface. It is read-only.

- The Modbus interface supports 2-wire RS-485.
- Modbus runs at 9600 or 19200 bps.

The Modbus register map for the InRow SC defines the data (type, location, and valid responses) available through Modbus. To download the latest Modbus register map, go to the APC Web site (www.apc.com), search by part number, and click the link to the register map in the list of documentation. Check the publication date at the start of the file.



See also

For more information on Modbus, see the Modbus Standard Library at www.modbus.org.

Reset the Interface (Administration>General>Reset/Reboot)

Use this option to perform any of the following actions:

| Action | Definition |
|-----------------------------|--|
| Reboot Management Interface | Restarts the management interface of the device without turning off and restarting the device itself. |
| Reset All | <p>Resets configuration settings as follows:</p> <p>Mark the Include TCP/IP checkbox to include the setting that determines how this device must obtain its TCP/IP settings. That setting will be reset to its default, DHCP & BOOTP.</p> <p>NOTE: To reset all settings except the TCP/IP settings of this device, do not mark the Include TCP/IP checkbox.</p> |
| Reset Only | <p>You can choose one or more of the following options by marking their check-boxes:</p> <p>TCP/IP: Resets only the setting that determines how this device must obtain its TCP/IP settings. That setting will be reset to its default, DHCP & BOOTP.</p> <p>Event Configuration: Resets only events to their default configuration. Any configuration changes, by event or by group, will revert to their default settings.</p> |

Configuring Links (Administration>General>Quick Links)

Select the **Administration** tab, the **General** option on the top menu bar, and the **Quick Links** option on the left navigation menu to view the three URL links displayed at the bottom left of each page of the interface.

By default, these links access the following Web pages:

- **APC's Web Site:** The APC home page.
- **Testdrive Demo:** A demonstration page where you can use samples of APC Web-enabled products.
- **APC Monitoring:** The home page of the APC Remote Monitoring Service.

To reconfigure a link, click on that link in the **Display** column, and change any of the following:

- **Display:** The short link name displayed on each interface page
- **Name:** A name that fully identifies the target or purpose of the link
- **Address:** Any URL—for example, the URL of another device and server

APC Device IP Configuration Wizard

Purpose and Requirements

How to use the Wizard to configure TCP/IP settings

The APC Device IP Configuration Wizard configures the IP address, subnet mask, and default gateway of one or more Network Management Cards or APC network-enabled devices (devices containing an embedded Network Management Card). You can use the Wizard in either of the following ways:

- Remotely over your TCP/IP network to discover and configure unconfigured Network Management Cards or devices on the same network segment as the computer running the Wizard.
- Through a direct connection from a serial port of your computer to a Network Management Card or device, to configure or reconfigure it.

System requirements

The Wizard runs on Windows 2000, Windows 2003, and Windows XP.

Installation

To install the Wizard from the *Utility* CD:

1. If autorun is enabled, the user interface of the CD starts when you insert the CD. Otherwise, open the file **contents.htm** on the CD.
2. Click **Device IP Configuration Wizard** and follow the instructions.

To install the Wizard from a downloaded executable file:

1. Go to www.apc/tools/download.
2. Download the Device IP Configuration Wizard
3. Run the executable file, the folder to which you downloaded it.

Use the Wizard

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 Network Management Cards or network-enabled devices, 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 Control Console settings.)
 - For a Network Management Card that you install, the MAC address is on a label on the bottom of the card.
 - For a network-enabled device (with an embedded Network Management Card), the MAC address is on a label on the device.

You can also obtain the MAC address from the Quality Assurance slip that came with the Network Management Card or device.

Run the Wizard to perform the configuration. To discover and configure, unconfigured Network Management Cards or network-enabled devices over the network:

1. From the **Start** menu, launch the Wizard. The Wizard detects the first Network Management Card or network-enabled device 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 Network Management Card or device identified by the MAC address. Click **Next >**.
On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the Network Management Card or device 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 Network Management Card or device, it displays the screen to enter TCP/IP settings. Repeat this procedure beginning with step 3, or to skip the Network Management Card or device whose MAC address is currently displayed, click **Cancel**.

Configure or reconfigure 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 Network Management Card or device) 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 Network Management Card or network-enabled device 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 Network Management Card or device, and click **Next>**.
7. On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the Network Management Card or device after the Wizard transmits the settings.
8. 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**.
9. If you selected **Start a Web browser when finished** in step 7, you can now configure other parameters through the Web interface of the card or device.

How to Export Configuration Settings

Retrieving and Exporting the .ini File

Summary of the procedure

As an Administrator, you can retrieve a dynamically generated .ini file of the current configuration of the InRow SC and export that file to another InRow SC or to multiple InRow SCs.

1. Configure the InRow SC to have the settings you want to export.
2. Retrieve the .ini file from that InRow SC.
3. Customize the .ini file (to change at least the TCP/IP settings) and make a copy to export.
4. Use any of the file transfer protocols supported by the InRow SCs to transfer the copied file to one or more additional InRow SCs. (To transfer the file to multiple InRow SCs simultaneously, write an FTP or SCP script that repeats the steps for transferring the file to a single InRow SC.)
5. Each receiving InRow SC stores the file temporarily in its flash memory, uses it to reconfigure its own settings, and then deletes the file.



To create batch files and use an APC utility to retrieve configuration settings from multiple InRow SCs and export them to other InRow SCs, see *Release Notes: ini File Utility, version 1.0* on the *Utility CD*.

Contents of the .ini file

The config.ini file that you retrieve from the InRow SC contains the following:

- *section headings*, which are category names enclosed in brackets ([]), and under each section heading, *keywords*, which are labels describing specific InRow SC settings.



Note

Only section headings and keywords supported for the specific device (in this case, the InRow SCs) from which you retrieve the file are included.

- Each keyword is followed by an equals sign and the current *value* for that parameter's setting, either the default value (if the value has not been specifically configured) or the configured value.
 - The **override** keyword, with its default value, prevents one or more keywords and their device-specific values from being exported. For example, in the **[NetworkTCP/IP]** section, the default value for **Override** (the MAC address of the InRow SCs) blocks the exporting of the values for the keywords **SystemIP**, **SubnetMask**, **DefaultGateway**, and **BootMode**.
 - You must edit the section **[SystemDate/Time]** to set the system date and time of a receiving InRow SC or cause that InRow SC to use an NTP Server to set its date and time.



See [Customizing](#) for configuration guidelines for date and time settings.

Detailed procedures

Use the following procedures to retrieve the settings of one InRow SC and export them to one or more InRow SC.

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

1. Configure the InRow SCs with the settings you want to export.



Note

To avoid errors, configure the InRow SC by using its user interface whenever possible. Directly editing the .ini file risks introducing errors.

2. Use FTP to retrieve the file *config.ini* from the InRow SC you configured:
 - a. Open a connection to the InRow SC, using its IP address. For example:
 - b. Log on, using the Administrator user name and password configured for the InRow SC.
 - c. Retrieve the config.ini file containing the InRow SCs current settings:

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

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



See also

To create batch files and use an APC utility to retrieve configuration settings from multiple InRow SCs and export them to other InRow SCs, see *Release Notes: ini File Utility, version 1.0* on the *Utility CD*.

Customizing. You must customize the file to change at least the TCP/IP settings 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.
 - To define values, opening and closing quotation marks are optional, except to enclose values that contain leading or trailing spaces or values which are already enclosed in quotation marks. (Leading or trailing spaces not within the opening and closing quotation marks are ignored.)
 - To export a specific system date and time or any scheduled events, you must configure the values directly in the .ini file.
 - To export a specific system time, export only the configured `[SystemDate/Time]` section as a separate .ini file. (The time necessary to export a large file would cause the configured time to be significantly inaccurate.)
 - For greater accuracy, if the InRow SCs receiving the file can access a Network Time Protocol (NTP) Server, set the value for the `NTPEnable` keyword as follows:
`NTPEnable=enabled`
 - Add comments about changes that you made. The first printable character of a comment line must be a semicolon (;).
2. Copy the customized file to another file name in the same folder:
 - The copy, which you will export to other InRow SCs, can have any file name up to 64 characters and must have the .ini file suffix.
 - Retain the original customized file for future use. **The file that you retain is the only record of your comments.** They are removed automatically from the file that you export.

Transferring the file to a single InRow SCs. To transfer the .ini file to one other InRow SC, do either of the following:

- From the Web interface of the receiving InRow SC, 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 .ini file to transfer or use the **Browse** button to identify the location of the .ini file.
- Use any of the file transfer protocols supported by InRow SC (including FTP, FTP Client, SCP, and TFTP). The following example uses FTP:

- a. From the folder containing the customized .ini file and its copy, use FTP to log in to the InRow SCs to which you are exporting the .ini file. For example:

```
ftp> open 158.165.4.135
```

- b. Export the copy of the customized .ini file. The receiving InRow SC accepts any file name that has the .ini suffix, is no more than 64 characters in length, and is exported to its root directory.

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

Exporting the file to multiple InRow SCs. To export the .ini file to multiple InRow SCs:

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



See also

To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* on the *Utility CD*.

The Upload Event and Error Messages

The event and its error messages

The following event occurs when the receiving InRow SC 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 event text is extended to include notification of the following errors.



Note

The export to and the subsequent upload by the receiving InRow SCs succeeds even if there are errors.

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

Errors generated by overridden values

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



See [Contents of the .ini file](#) for information about which values are overridden.

The overridden values are device-specific and not appropriate to export to other InRow SCs. Therefore, you can ignore these error messages. To prevent these error messages from occurring, 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.

Using the APC Device IP Configuration Wizard

On Windows operating systems, instead of using the preceding procedure for transferring .ini files, you can choose to update the basic TCP/IP settings of InRow SCs by using the APC Device IP Configuration Wizard.



See [APC Device IP Configuration Wizard](#)

File Transfers

Upgrading Firmware

Benefits of upgrading firmware

When you upgrade the firmware on the InRow SC:

- You obtain the latest bug fixes and performance improvements.
- New features become available for immediate use.

Keeping the firmware versions consistent across your network ensures that all InRow SCs support the same features in the same manner.

Firmware files (InRow SC)

A firmware version consists of two modules: An APC Operating System (AOS) module and an application module. Each module contains one or more Cyclical Redundancy Checks (CRCs) to protect its data from corruption during transfer.

The APC Operating System (AOS) and application module files used with the InRow SC share the same basic format:

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

- **apc**: Indicates that this is an APC file.
- **hardware-version**: **hw0x** identifies the version of the hardware on which you can use this binary file.
- **type**: Identifies whether the file is for the APC Operating System (AOS) or the application module for the InRow SC.
- **version**: The version number of the file.
- **bin**: Indicates that this is a binary file.

Obtain the latest firmware version

Automated upgrade tool for Microsoft Windows systems. An upgrade tool automates the transferring of the firmware modules on any supported Windows operating system. Obtain the latest version of the tool at no cost from www.apc.com/tools/download. At this Web page, find the latest firmware release for your APC product (in this case, your InRow SC) and download the automated tool, not the individual firmware modules. **Never** use the tool for one APC product to upgrade firmware of another.

Manual upgrades, primarily for Linux systems. If no computer on your network is running a Microsoft Windows operating system, you must upgrade the firmware of your InRow SCs by using the separate AOS and application firmware modules.

Obtain the individual firmware modules for your firmware upgrade from www.apc.com/tools/download.

Firmware File Transfer Methods

To upgrade the firmware of the InRow SC, use one of these methods:

- From a networked computer running a Microsoft Windows operating system, use the firmware upgrade tool downloaded from the APC Web site.
- From a networked computer on any supported operating system, use FTP or SCP to transfer the individual AOS and application firmware modules.
- For an InRow SC that is not on your network, use XMODEM through a serial connection to transfer the individual firmware modules from your computer to the InRow SC.



Note

When you transfer individual firmware modules, **you must** transfer the APC Operating System (AOS) module to the InRow SC before you transfer the application module.

Use FTP or SCP to upgrade one InRow SC

FTP. For you to use FTP to upgrade one InRow SC over the network:

- The InRow SC must be connected to the network, and its system IP, subnet mask, and default gateway must be configured
- The FTP server must be enabled at the InRow SC.

To transfer the files:

1. Open a command prompt window of a computer on the network. Go to the directory that contains the firmware files, and list the files:

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

For the listed files, *xxx* represents the firmware version number:

```
- apc_hw03_aos_xxx.bin  
- apc_hw03_application_xxx.bin
```

2. Open an FTP client session:

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

3. Type **open** and the IP address for the InRow SC, and press ENTER. If the **port** setting for the FTP Server has changed from its default of **21**, you must use the non-default value in the FTP command.

–For Windows FTP clients, separate a non-default port number from the IP address by a space. For example:

```
ftp> open 150.250.6.10 21000
```

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

4. Log on as Administrator; **apc** is the default user name and password.
5. Upgrade the AOS. (In the example, *xxx* is the firmware version number):

```
ftp> bin  
ftp> put apc_hw03_aos_xxx.bin
```

6. When FTP confirms the transfer, type **quit** to close the session.
7. After 20 seconds, repeat **step 2** through **step 5**. In **step 5**, use the application module file name.

SCP. To use Secure CoPy (SCP) to upgrade firmware for the InRow SC:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the InRow SC. The following example uses *xxx* to represent the version number of the AOS module:

```
scp apc_hw03_aos_xxx.bin apc@158.205.6.185:apc_hw03_aos_xxx.bin
```
3. Use a similar SCP command line, with the name of the application module, to transfer the second firmware module to the InRow SC.

How to upgrade multiple InRow SCs

Export configuration settings. You can create batch files and use an APC utility to retrieve configuration settings from multiple InRow SCs and export them to other InRow SCs.



See *Release Notes: ini File Utility, version 1.0*, available on the *Utility CD*.

See also

Use FTP or SCP to upgrade multiple InRow SCs. To upgrade multiple InRow SCs using an FTP client or using SCP, write a script which automatically performs the procedure.

Use XMODEM to upgrade one InRow SC

To upgrade the firmware for an InRow SC that is not on the network:

1. Obtain the individual firmware modules (the AOS module and the application module) from www.apc.com/tools/download.
2. Select a serial port at the local computer and disable any service that uses the port.
3. Connect the advanced signaling cable that came with the InRow SC to the selected port and to the serial port at the InRow SC.

4. 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.
5. Press ENTER to display the **User Name** prompt. Enter the Administrator user name and password (**apc** by default for both).
6. From the **Control Console** menu, select **System**, then **Tools**, then **File Transfer**, then **XMODEM**; and type **Yes** at the prompt to continue.
7. Select a baud rate, change the terminal program's baud rate to match your selection, and press ENTER. A higher baud rate causes faster upgrades.
8. From the terminal program's menu, select the binary AOS file to transfer using XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600. The InRow SC automatically restarts.
9. Repeat step 4 through step 8 to install the application module. In step 8, use the application module file name, not the AOS module file name.



For information about the format used for firmware modules, see [Firmware files \(InRow SC\)](#).

Verifying Upgrades and Updates

Verify the success or failure of the transfer

To verify whether a firmware upgrade succeeded, use the **Network** menu in the control console and select the **FTP Server** option to view **Last Transfer Result**, or use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

Last Transfer Result codes

| Code | Description |
|----------------------|--|
| Successful | The file transfer was successful. |
| Result not available | There are no recorded file transfers. |
| Failure unknown | The last file transfer failed for an unknown reason. |
| Server inaccessible | The TFTP or FTP server could not be found on the network. |
| Server access denied | The TFTP or FTP server denied access. |
| File not found | The TFTP or FTP server could not locate the requested file. |
| File type unknown | The file was downloaded but the contents were not recognized. |
| File corrupt | The file was downloaded but at least one Cyclical Redundancy Check (CRC) failed. |

Verify the version numbers of installed firmware

Use the Web interface to verify the versions of the upgraded firmware modules by selecting the **Administration** tab, **General** on the top menu bar, and **About** on the left navigation menu, or use an SNMP GET to the MIB II **sysDescr** OID.

Product Information

Warranty and Service

Limited warranty

APC warrants the InRow SC to be free from defects in materials and workmanship for a period of one year from the date of purchase. Its obligation under this warranty is limited to repairing or replacing, at its own sole option, any such defective products. This warranty does not apply to equipment that has been damaged by accident, negligence, or misapplication or has been altered or modified in any way. This warranty applies only to the original purchaser.

Warranty limitations

Except as provided herein, APC makes no warranties, expressed or implied, including warranties of merchantability and fitness for a particular purpose.

Some jurisdictions do not permit limitation or exclusion of implied warranties; therefore, the aforesaid limitation(s) or exclusion(s) may not apply to the purchaser.

Except as provided above, in no event will APC be liable for direct, indirect, special, incidental, or consequential damages arising out of the use of this product, even if advised of the possibility of such damage.

Specifically, APC is not liable for any costs, such as lost profits or revenue, loss of equipment, loss of use of equipment, loss of software, loss of data, costs of substitutes, claims by third parties, or otherwise. This warranty gives you specific legal rights and you may also have other rights, which vary according to jurisdiction.

Obtaining service

To obtain support for problems with your InRow SC:

1. Note the serial number. The serial number of the InRow SC is available by selecting the **Administration** tab, then **General** on the top menu bar and **Factory Info** on the left navigation menu.
2. Contact Customer Support at a phone number on the last page of this User's Guide. A technician will try to help you solve the problem by phone.
3. If you must return the product, the technician will give you a return material authorization (RMA) number. If the warranty expired, you will be charged for repair or replacement.
4. Pack the unit carefully. The warranty does not cover damage sustained in transit. Enclose a letter with your name, address, RMA number and daytime phone number; a copy of the sales receipt; and a check as payment, if applicable.
5. Mark the RMA number clearly on the outside of the shipping carton.
6. Ship by insured, prepaid carrier to the address provided by the Customer Support technician.

Life-Support Policy

General policy

American Power Conversion (APC) does not recommend the use of any of its products in the following situations:

- In life-support applications where failure or malfunction of the APC product can be reasonably expected to cause failure of the life-support device or to affect significantly its safety or effectiveness.
- In direct patient care.

APC will not knowingly sell its products for use in such applications unless it receives in writing assurances satisfactory to APC that (a) the risks of injury or damage have been minimized, (b) the customer assumes all such risks, and (c) the liability of American Power Conversion is adequately protected under the circumstances.

Examples of life-support devices

The term *life-support device* includes but is not limited to neonatal oxygen analyzers, nerve stimulators (whether used for anesthesia, pain relief, or other purposes), autotransfusion devices, blood pumps, defibrillators, arrhythmia detectors and alarms, pacemakers, hemodialysis systems, peritoneal dialysis systems, neonatal ventilator incubators, ventilators (for adults and infants), anesthesia ventilators, infusion pumps, and any other devices designated as “critical” by the U.S. FDA.

Hospital-grade wiring devices and leakage current protection may be ordered as options on many APC UPS systems. APC does not claim that units with these modifications are certified or listed as hospital-grade by APC or any other organization. Therefore these units do not meet the requirements for use in direct patient care.

Index

A

- Access
 - enabling or disabling methods of access
 - to the control console 43
 - to the Web interface 41
 - SNMP access control 46
 - to stored data log 60
- Administration
 - Network menu 34
- Air filter
 - enable/disable alarm generation 26
 - reset service intervals 26
- Apply Local Computer Time 65
- Authenticating users through RADIUS 30
- Authentication Traps setting 55
- Automatic log-off for inactivity 33

B

- BOOTP
 - BOOTP server providing TCP/IP settings 34

C

- Community Name for trap receivers 55
- config.ini file. See User configuration files.
- Contact identification (whom to contact) 64
- Control console
 - configuring access 43
 - Device Manager menu 16
 - navigating menus 15
 - refreshing menus 15
- Cooling unit settings, configuring 28

D

- Data log
 - disable sending authentication traps to an NMS 55
 - displaying and using 59
 - enable sending authentication traps to an NMS 55
 - Log Interval setting 60
 - rotation 60
- data.txt file
 - contents 61
 - importing into spreadsheet 61
- Date & Time settings 65
- Date format 66
- Daylight Saving Time configuration 66
- Device IP Configuration Wizard
 - system requirements 70
 - using the Wizard 71
- Device Manager menu
 - control console 16
- DHCP
 - APC cookie 36
 - DHCP server providing TCP/IP settings 34
 - response options 36
- Differential pressure (HACS/RACS only) 25
- Disable
 - data log rotation 60
 - e-mail to a recipient 54
 - encryption algorithms for SSH 43
 - reverse lookup 59
 - sending any traps to an NMS 55
 - sending authentication traps to an NMS 55
 - SSL cipher suites 41
 - Telnet 43

- Display interface LEDs 7
- Display units 28
- DNS
 - defining host and domain names 39
 - query types 40
 - specifying DNS servers by IP address 39

E

- E-mail
 - configuring notification parameters 52
 - configuring recipients 54
 - test message 54
 - using for paging 54
- Enable
 - data log rotation 60
 - e-mail forwarding to external SMTP servers 54
 - e-mail to a recipient 54
 - encryption algorithms for SSH 43
 - reverse lookup 59
 - sending any traps to an NMS 55
 - sending authentication traps to an NMS 55
 - SSL cipher suites 41
 - Telnet 43
 - versions of SSH 43
- English units 28
- Error messages 20
 - for firmware file transfer 85
 - from overridden values during .ini file transfer 79
- Ethernet port speed 38
- Event actions 48
 - configuring by event 49
 - configuring by group 50
- Event log
 - accessing 15
 - errors from overridden values during .ini file transfer 79

- using FTP del command 63
 - using FTP or SCP to retrieve 61
- event.txt file
 - contents 61
 - importing into spreadsheet 61

F

- Facility Code (Syslog setting) 56
- Factory information 26, 64
- File transfers
 - verification 85
- Firmware
 - benefits of upgrading 80
 - file transfer methods
 - automated upgrade tool 81
 - FTP or SCP 82
 - XMODEM 83
 - files for the InRow SC 80
 - information in Factory Info 64
 - obtaining the latest version 81
 - upgrading multiple InRow SC 83
 - verifying upgrades and updates 85
 - versions displayed on main screen 12
- From Address (SMTP setting) 53
- FTP
 - server settings 46
 - transferring firmware files 82
 - using to retrieve text version of event log or data log 61

H

- Hardware information 64
- Help on control console 15
- Host keys
 - adding or replacing 44
 - status 44
- Host name of trap receivers 55

I

- Identification 26
 - fields on main screen 13
 - Name, Location, and Contact 64
- Idle on leak detect 28
- Inactivity timeout 33
- ini files, See User configuration files
- Input sensor 28

K

- Keywords in user configuration file 74

L

- Last Transfer Result codes 85
- Links, configuration 69
- Local SMTP Server
 - defining by IP address or DNS name 53
 - recommended option for routing e-mail 54
- Location (system value) 64
- Log
 - data 59
 - event 58
- Logging on
 - Web interface 18
 - error messages 20
- Login date and time, control console 13

M

- Main screen
 - displaying identification 13
 - firmware values displayed 12
 - login date and time 13
 - status 14
 - Up Time 13

- User access identification 13

Menus

- Control Console 16
 - Events 23
 - General 24
 - Help 22
 - Network 23, 34
 - Notification 23
 - Unit 25
- ## Message Generation (Syslog setting) 56
- Metric units 28
 - MIB-II Identification variables 64
 - Modbus
 - configuration 67
 - register map 67
 - Modules, Factory information 28

N

- Name, Location, and Unit ID 26
- Network menu 34
- Network Time Protocol (NTP) 65
- NMS IP/Host Name for trap receivers 55
- Notification 48

O

- OS, APC 12, 28
- Output relay
 - defining activation source 28
 - normal state 28
- Override keyword, in user configuration file 74

P

- Paging by using e-mail 54
- Passwords
 - default for each account type 18

- defining for each account type 29
- for NMS that is a trap receiver 55
- to send data to stored data log 60
- Port (Syslog setting) 56
- Port speed, configuring for Ethernet 38
- Ports
 - FTP server 46
 - HTTP and HTTPS 41
 - RADIUS server 31
 - Telnet and SSH 43
- Primary NTP Server 65

Q

- Quick Links, configuration 69

R

- Reboot
 - preventing reboot for inactivity 9
 - Reboot Management Interface 68
- Recipient SMTP server 54
- Remote Monitoring Service 69
- Remote users, authentication 30
- Reset only events to defaults 68
- Reset only TCP/IP to defaults 68
- Reset run hours 26
- restart, staged 27, 28
- Reverse lookup 59
- Rotation of data log 61

S

- SCP
 - for high-security file transfer 47
 - transferring firmware files 82
 - using to retrieve text version of event log or data log 61
- Secondary NTP Server 65

- Section headings, user configuration file 74

Sensor

- air temperature 25
- configure temperature thresholds 26

Serial Modbus. See Modbus

Service intervals, resetting 26

Severity Mapping (Syslog setting) 57

SMTP server

- selecting for e-mail recipients 54
- settings 53

SNMP

- authentication traps 55
- disabling SNMP for high-security systems 44

SSH

- encryption algorithms 43
- host keys 44

SSL

- Certificates, how to create, view, or remove 42
- cipher suites 41
- configuring cipher suites 41

Staged restart 27, 28

Startup delay 27, 28

Status

- on control console main screen 14

Synchronize with NTP Server, (Date & Time) 65

Syslog 55

- identifying the Syslog server 56
- mapping event severity to Syslog priorities 57
- settings 56
- test 57

System Name 64

T

TCP/IP

- restoring default settings 68

- TCP/IP configuration 34
- Temperature scale (Fahrenheit or Celsius) 66
- Temperature sensor thresholds 26
- Test
 - DNS query 40
 - e-mail recipient settings 54
 - RADIUS server path 31
 - Syslog 57
 - trap receiver 55
- Time setting 65
- Time Zone, for synchronizing with NTP server 65
- To Address, E-mail Recipients 54
- Trap Generation 55
- Trap Receivers 55

U

- Up Time
 - control console main screen 13
- Update Interval, Date & Time setting 65
- Update Using NTP Now, Date & Time setting 65
- Upgrading firmware 80
- URL address formats 20
- User access identification, control console interface 13
- User configuration files
 - contents 74
 - customizing 76
 - exporting system time separately 76
 - retrieving and exporting 73
 - the upload event and error messages 78
 - using the APC utility to retrieve and transfer the files 73, 75

- User configuration files
 - overriding device-specific values 74
- User names
 - default for each account type 18
 - defining for each account type. 29
 - maximum number of characters for RADIUS 30
 - to send data to stored data log 60

V

- Verifying firmware upgrades and updates 85

W

- Web interface
 - configuring access 41
 - logging on 18
 - logon error messages 20
 - URL address formats 20

X

- XMODEM to transfer firmware files 83

APC Worldwide Customer Support

Customer support for this or any other APC product is available at no charge in any of the following ways:

- Visit the APC Web site to access documents in the APC Knowledge Base and to submit customer support requests.
 - www.apc.com (Corporate Headquarters)
 Connect to localized APC Web sites for specific countries, each of which provides customer support information.
 - www.apc.com/support/
 Global support searching APC Knowledge Base and using e-support.
- Contact an APC Customer Support center by telephone or e-mail.
 - Regional centers:

| | |
|--|--------------------------------|
| Direct InfraStruXure Customer Support Line | (1)(877)537-0607 (toll free) |
| APC headquarters U.S., Canada | (1)(800)800-4272 (toll free) |
| Latin America | (1)(401)789-5735 (USA) |
| Europe, Middle East, Africa | (353)(91)702000 (Ireland) |
| Japan | (0) 35434-2021 |
| Australia, New Zealand, South Pacific area | (61) (2) 9955 9366 (Australia) |

- Local, country-specific centers: go to www.apc.com/support/contact for contact information.

Contact the APC representative or other distributor from whom you purchased your APC product for information on how to obtain local customer support.

Copyright

Entire contents copyright 2006 American Power Conversion Corporation. All rights reserved. Reproduction in whole or in part without permission is prohibited. APC, the APC logo, InfraStruXure, and PowerNet are trademarks of American Power Conversion Corporation. All other trademarks, product names, and corporate names are the property of their respective owners and are used for informational purposes only.

990-2809

6/2006

