

# User Guide

## InRow<sup>™</sup> RC

**ACRC100  
ACRC101  
ACRC103**





# Contents

---

- Introduction ..... 1**
- Product Description ..... 1**
  - Features of the InRow™ RC ..... 1
  - Initial setup ..... 1
- Internal Management Features ..... 2**
  - Overview ..... 2
  - Log on control ..... 2
  - Types of user accounts ..... 3
- How to Recover a Lost Password ..... 3**
- Display Interface LEDs ..... 4**
  - Status ..... 4
  - Check log ..... 4
  - Warning alarm ..... 4
  - Critical alarm ..... 4
- Watchdog Features ..... 5**
  - Overview ..... 5
  - Network interface watchdog mechanism ..... 5
  - Resetting the network timer ..... 5
- Control Console ..... 6**
- How to Log On ..... 6**
  - Overview ..... 6
  - Remote access to the control console ..... 6
  - Local access to the control console ..... 7
- Main Screen ..... 7**
  - Example main screen ..... 7
  - Information and status fields ..... 8

<b>Control Console Menus</b> .....	<b>9</b>
Menu structure .....	9
Main menu .....	9
Device Manager option .....	10
Network option .....	10
System option .....	10
Logout option .....	10

## **Web Interface .....** **11**

<b>How to Log On</b> .....	<b>11</b>
Overview .....	11
Supported Web browsers .....	11
URL address formats .....	12

<b>Summary Page</b> .....	<b>12</b>
Navigation tabs .....	12
Quick status .....	13
Status .....	13
Help .....	13
Select a tab to perform a task .....	13

## **InRow RC Operation.....** **16**

<b>Home</b> .....	<b>16</b>
Overview .....	16
Alarm status .....	16

<b>Group</b> .....	<b>16</b>
Overview .....	16
Setpoints .....	17
Configuration .....	17

<b>Unit</b> .....	<b>18</b>
Overview .....	18
Detailed status .....	18
Identification .....	19
Run hours .....	19
Service intervals .....	19
Thresholds .....	19
Configuration .....	20

**Logs ..... 21**

**Events ..... 21**

- Log ..... 21
- Reverse lookup ..... 21

**Data ..... 22**

- Log ..... 22
- Graphing ..... 22
- Interval ..... 22
- Rotation ..... 23

**Syslog ..... 24**

- Servers ..... 24
- Settings ..... 25
- Test ..... 25
- How to use FTP or SCP to retrieve the log files ..... 26
- Queries (Modbus requests and SNMP GETs) ..... 27

**Administration: Security ..... 28**

**Local Users ..... 28**

- Permission levels ..... 28
- Setting user access ..... 28

**Remote Users ..... 28**

- Authentication ..... 28
- RADIUS ..... 29

**Configuring the RADIUS Server ..... 30**

- Summary of the configuration procedure ..... 30
- Configuring a RADIUS server on UNIX®, with shadow passwords 31
- Supported RADIUS servers ..... 31

**Auto Log Off ..... 31**

## **Administration: Network..... 32**

### **TCP/IP and Communication Settings ..... 32**

TCP/IP settings	32
DHCP response options	34
Port speed	35
DNS (Administration>Network>DNS>servers)	35
Web	37
Console	39
SNMP	40
FTP server	43

### **Related Topics ..... 43**

## **Administration: Notification ..... 44**

### **Event Actions ..... 44**

Types of notification	44
Configuring event actions	44

### **Active, Automatic, Direct Notification ..... 47**

E-mail	47
SNMP traps	49

## **Administration: General..... 50**

### **Information about the InRow RC ..... 50**

Identification	50
Date & time	50
User configuration file (ini)	51
Unit preference	51
Reset/reboot	52
Serial Modbus	52
Quick links	53
About	53

<b>APC Device IP Configuration Wizard.....</b>	<b>54</b>
<b>Purpose and Requirements .....</b>	<b>54</b>
Purpose: configure basic TCP/IP settings .....	54
System requirements .....	54
<b>Install the Wizard.....</b>	<b>54</b>
<b>Use the Wizard.....</b>	<b>55</b>
Launch the Wizard .....	55
Configure the basic TCP/IP settings remotely .....	55
Configure or reconfigure the TCP/IP settings locally .....	56
<b>How to Export Configuration Settings.....</b>	<b>57</b>
<b>Retrieving and Exporting the .ini File .....</b>	<b>57</b>
Summary of the procedure .....	57
Contents of the .ini file .....	57
Detailed procedures .....	58
<b>The Upload Event and Error Messages.....</b>	<b>60</b>
The event and its error messages .....	60
Errors generated by overridden values .....	60
<b>Using the APC Device IP Configuration Wizard .....</b>	<b>61</b>
<b>File Transfers .....</b>	<b>62</b>
<b>Overview.....</b>	<b>62</b>
<b>Upgrading Firmware .....</b>	<b>62</b>
Benefits of upgrading firmware .....	62
Firmware files (InRow RC) .....	62
Obtain the latest firmware version .....	63
Firmware file transfer methods .....	63
Use FTP or SCP to upgrade one InRow RC .....	64
Upgrade multiple InRow RCs .....	65
Use XMODEM to upgrade one InRow RC .....	65
<b>Verifying Upgrades and Updates.....</b>	<b>66</b>
Overview .....	66
Last transfer result codes .....	66





# Introduction

---

## Product Description

### Features of the InRow™ RC

The American Power Conversion (APC™) InRow RC is a chilled water modular air conditioning unit that is available in either a half-rack (ACRC100 series) or a full-rack (ACRC500 series) model. This user guide describes the features of the ACRC100-series cooling units. The ACRC100-series models are the widths of a standard enclosure, and can be placed in a data-center row. The InRow RC provides full management capabilities over a network using Telnet, Secure Shell (SSH), HTTP, HTTPS, FTP, Secure Copy (SCP), Modbus, and SNMP. The InRow RC provides the following features:

- Group control
- Temperature monitoring
- Remote shutdown
- Output contact monitoring
- Event log accessible by Telnet, FTP, SSH, SCP, serial connection, the display interface, or a Web browser
- SNMP traps and e-mail notifications sent in response to events
- Syslog events sent to configured Syslog servers
- Security protocols for authentication and encryption

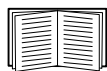
### Initial setup

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

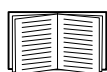
- IP address of the Management Card
- Subnet mask
- IP address of the default gateway



**Note:** Never use the loopback address (127.0.0.1) as the default gateway address for the InRow RC. Doing so will disable the unit 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 for an InRow RC, see “[TCP/IP settings](#)” on page 32.

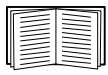


To configure the TCP/IP settings, see the InRow RC *Installation and Quick Start Manual*, provided in printed form and in PDF on either the *Utility CD* or on the APC Web site, [www.apc.com](http://www.apc.com).

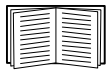
# Internal Management Features

## Overview

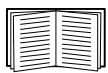
You can manage the InRow RC through the Web interface, display interface, control console, Modbus, or SNMP. SNMP requires the PowerNet<sup>®</sup> MIB, available on the CD or from the APC Web site, [www.apc.com](http://www.apc.com).



For more information about the menu-driven interfaces of the InRow RC, see “[Web Interface](#)” on page 11 and “[Control Console](#)” on page 6.

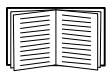


For more information about the display interface, see the InRow RC *Operation and Maintenance* manual, available on the CD or on the APC Web site, [www.apc.com](http://www.apc.com).



To download the latest version of the Modbus register map, go to the APC Web site, [www.apc.com](http://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](http://www.modbus.org).

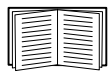


To use the PowerNet MIB with an SNMP browser, see the *PowerNet SNMP Management Information Base (MIB) Reference Guide*, provided on the APC Network Management Card utility CD.

## Log on control

Only one user at a time can log on to the InRow RC 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 RC 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 InfraStruXure Central or InfraStruXure Manager, has the lowest priority.



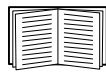
For information on how to control SNMP access to the InRow RC, see “[SNMP](#)” on page 40.

## Types of user accounts

The InRow RC has three levels of access (Administrator, Device-Only 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 default user name and password are both **apc**.
- A Device-Only User (Device Manager in the control console) can access only the **Log** option in the **Events** menu and use the **Group**, **Unit**, and **Alarms** menus. The Device-Only User 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-Only 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 Read-Only User default user name is **readonly**, and the default password is **apc**.



To set **User Name** and **Password** values for the Administrator, Device-Only User, and Read-Only User accounts, see “**Setting user access**” on page 28. You must use the Web interface to configure values for the Read-Only User.

## How to Recover a Lost Password

Use a local computer (a computer that connects to the InRow RC through the serial port) to access the control console.

1. Select a serial port at the local computer and disable any service that uses that port.
2. Connect the APC null-modem cable (APC part number 940-0103A) to the selected port on the computer and to the serial port at the InRow RC (use the DB-9 connector on the front of the electrical panel).



**Note:** Do not touch components on the electrical panel, other than the service port.

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
4. Press ENTER on the computer, repeatedly if necessary, to display the **User Name** prompt.

If you are unable to display the **User Name** prompt, verify the following:

  - The serial port is not in use by another application.
  - The terminal settings are correct as specified in step 3.
  - The correct cable is being used as specified in step 2.
5. Switch the main breaker to OFF. Wait one second. Switch the main breaker to ON.



**Note:** If you wait too long to return power to the InRow RC, you must repeat step 5.

6. 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 5 and log on again.)
7. From the **Control Console** menu, select **System**, then **User Manager**.
8. 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.
9. 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 RC.

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

### Check log

When yellow, this LED indicates that at least one new critical alarm, warning alarm, or 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 may require your attention to prevent it from deteriorating into a critical state. A new alarm will cause a beep every 30 seconds until you silence the alarm by pressing any function key.

### Critical alarm

When red, this LED indicates that a critical alarm condition exists and requires your immediate attention. An audible alarm beeps every 30 seconds. Press any function key to silence the audible alarm.

# Watchdog Features

## Overview

To detect internal problems and recover from unanticipated inputs, the InRow RC 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 RC implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the InRow RC 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 RC does not restart if the network is quiet for 9.5 minutes, the InRow RC attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the InRow RC, 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 RC from restarting.

# Control Console

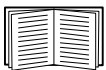
---

## 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-Only User). A Read-Only User cannot access the control console.



If you cannot remember your user name or password, see [“How to Recover a Lost Password”](#) on page 3.

### 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 from any computer on the same subnet:

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

```
telnet 139.225.6.133
```



**Note:** If the InRow RC uses a non-default port number (between 5000 and 32768), 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-Only 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 a SSH client program installed on your computer.

## Local access to the control console

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



**Note:** To access the serial port, remove the front panel and lower air filter of the InRow RC.

1. Select a serial port at the local computer and disable any service that uses that port.
2. Use the supplied RS-232 configuration cable (APC part number 940-0103A) to connect the selected port to the serial port at the InRow RC (use the DB-9 connector on the front 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. Enter the user name and password for the access desired (Administrator or Device-Only 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 RC.

```

                                User Name : apc
                                Password  : ***

American Power Conversion      Network Management Card AOS      vx.x.x
<c> Copyright 2008 All Rights Reserved  InRow RC APP              vx.x.x.x
-----
Name       : InRow RC                Date : 10/29/2008
Contact    : Bill Cooper              Time : 10:16:58
Location   : Testing Lab              User : Administrator
Up Time    : 0 Days 0 Hours 43 Minutes Stat : P+ N+ A+

Cooling Group Status : None
Cooling Unit  Status : None

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

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

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

## Information and status fields

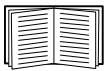
### Main screen information fields.

- 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 RC is displayed.

```
Network Management Card AOS      vx.x.x
InRow RC APP                     vx.x.x
```

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

```
Name       : InRow RC
Contact    : Bill Cooper
Location   : Testing Lab
```



To set the **Name**, **Contact**, and **Location** values, see “**Identification**” on page 50.

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

```
Up Time: 0 Days 0 Hours 43 Minutes
```

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

```
Date : 10/29/2008
Time : 10:16:58
```

- 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 status of the InRow RC.

```
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 RC failed to connect to the network.
N!	Another device is using the IP address of the InRow RC.
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 RC.

### InRow RC status field.

The **Status** field displays the status of the Cooling Units. Under normal operation this field will read:

Cooling Group Status : None

Cooling Unit Status : None

None will be replaced with `Warning` or `Critical` if an alarm condition exists.

## Control Console Menus

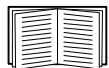
### Menu structure

The menus in the control console list options by number and name. To use an option, type the option 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.



For more information about the event log, see [“Events”](#) on page 21.

### Main menu

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

1- Device Manager

2- Network

3- System

4- Logout



**Note:** When you log on as Device User, 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 and the group. Select the components you want to manage. For example:

- 1- View Active Alarms
- 2- Cooling Group
- 3- Cooling Unit

## Network option

Use this option to perform any of the following tasks:

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

## 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 RC.
- Restart the InRow RC management interface.
- Reset control console settings to their default values.
- Define RADIUS access and set primary and secondary servers.

## Logout option

Use this option to log out of the Control Console.

# Web Interface

---

## How to Log On

### Overview

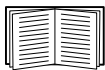
You can use the DNS name or System IP address of the InRow RC for the URL address of the Web interface. Use your case-sensitive **User Name** and **Password** settings to log on. The default user name differs by account type:

- **apc** for an Administrator
- **device** for a Device-Only 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 RC. 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” on page 12.](#)

### Supported Web browsers

You can use Microsoft® Internet Explorer 5.5 and higher (on Windows operating systems only), or Firefox, version 1.x and higher, by Mozilla Corporation (on all operating systems) to access the InRow RC 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 RC management interface cannot work with a proxy server. Therefore, before you can use a Web browser to access the InRow RC Web interface, you must do one of the following:

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

## URL address formats

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

### Common browser error messages at login. .

Cause of the Error	Browser	Error Message
Someone else is logged on.	Internet Explorer, 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		
	Internet Explorer	“This page cannot be displayed.”
	Firefox	“Unable to connect.”

- For a DNS name of Web1, the entry would be one of the following:
  - `http://Web1` if HTTP is your access mode
  - `https://Web1` if HTTPS is your access mode
- For a System IP address of 139.225.6.133, when the InRow RC uses the default port (80) at the Web server, the entry would be one of the following:
  - `http://139.225.6.133` if HTTP is your access mode
  - `https://139.225.6.133` if HTTPS is your access mode
- For a System IP address of 139.225.6.133, when the InRow RC uses a non-default port (5000, in this example) at the Web server, the entry would be one of the following:
  - `http://139.225.6.133:5000` if HTTP is your access mode
  - `https://139.225.6.133:5000` if HTTPS is your access mode

## Summary Page

When you log on to the Web interface at the InRow RC, 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

Five tabs are displayed at the top of the screen:

- **Home**—View any active alarm or warning conditions and clear active alarms; this tab is displayed at login.
- **Group**—View and configure group settings.
- **Unit**—View and configure cooling settings, unit properties, identification information, view or reset run hours, 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 summary of any alarms.

	Click the green “device operating normally” icon to return to the status screen where the status of the InRow RC 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 Cooling Group and individual Cooling 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 “**Home**” on page 16:

- View and clear alarms.

To do the following, see “**Group**” on page 16:

- View the status of the group.
- Set the number of units in the group.
- Define the configuration type used by the group.
- Set the cool and supply air setpoints.
- Set the fan speed preference.
- Set the cool PIDs.
- Set the percentage of glycol in the group.
- Configure active flow control settings (if equipped)

To do the following, see [“Unit”](#) on page 18:

- View the status and properties of each unit.
- Set unit delays.
- Change the unit identification values.
- Assign the type of alarm that will activate the output sensor.
- Set the normal state of the input and output.
- Reset the unit run hours alarms.
- Set alarm threshold values.
- Set service intervals.

To do the following, see [“Administration: Security”](#) on page 28:

- Access the event and data logs.
- Set the interval and rotation for the data log.
- Create data log graphs.
- Configure Syslog settings, add servers to the Syslog, and initiate Syslog server tests.

To do the following, see [“Administration: Security”](#) on page 28:

- Control Administrator, Device User, and Read-Only user access.
- Configure RADIUS access, servers, and server secret.
- Configure the minutes of inactivity required before Auto Log Off

To do the following, see [“Administration: Network”](#) on page 32:

- Configure new TCP/IP settings for the InRow RC.
- Select the port speed.
- Identify the Domain Name System (DNS) Server and test the network connection to that server.
- Define settings for the FTP server, SNMPv1, SNMPv3, Control Console/SSH, and Web/SSL.

To do the following, see [“Administration: Notification”](#) on page 44:

- Configure the actions to be taken based on the severity level of an event.
- Configure and test 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: General”](#) on page 50:

- Define the System name, contact, and location values.
- Set the date and time used by the InRow RC.
- Select the temperature scale used by the InRow RC.
- Restart the user interface of the InRow RC.
- Reset network interface settings to their default settings.
- Upload a user configuration file.
- Configure Modbus settings.
- View information about the InRow RC.
- Define the URL addresses of the user links in the Web interface.

# InRow RC Operation

---

## Home

### Overview

View a summary of the following:

- Active alarms
- Group status
- Unit status
- Recent device events

### Alarm status

View the following alarm information:

- Group alarm status showing alarm descriptions and severity level
- Unit alarm status showing alarm descriptions and severity level

You can also choose to clear active alarms.

## Group

### Overview

View the following properties that are group-level or common to each unit in the group:

- Cool setpoint—in degrees Celsius (C) or Fahrenheit (F)
- Supply air setpoint—in degrees Celsius (C) or Fahrenheit (F)
- Airflow—in cubic feet per minute (CFM) or liters per second (L/s)
- Active flow control status (if equipped)
- Maximum rack inlet temperature
- Minimum rack inlet temperature
- Cool output—in kW
- Cool demand—in kW



## Setpoints

Assign the group setpoints and then click **Apply**.

Assign Fan Speed Control and then click **Apply**. Options are:

- Automatic
- Manual

If manual fan speed control is selected, then assign Fan Speed Preference and then click **Apply**. Options are:

- **Low**
- **Medium-Low**
- **Medium**
- **Medium-High**
- **High**

Assign Active Flow Control Bias and then click **Apply (if equipped)**. Options are:

- Positive
- Slightly-Positive
- Zero
- Slightly-Negative
- Negative



**Note:** Automatic fan speed control must be selected for active flow control bias to work properly.

## Configuration

**Number of units in group.** Enter the number of units in the group, then click **Apply**. Up to twelve units can be configured to work as a group.

**Configuration type.** Select the configuration type, which is the air flow control strategy the group uses, then click **Apply**:

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

**Percent glycol.** Enter the percentage of glycol the group uses to cool the environment. This information is used to calculate the amount of energy (in kW) required by the unit.



**Note:** Only a qualified service technician should change the amount of glycol in the group.

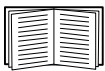
**Max fan speed.** Enter the percentage of available fan speed (60 to 100)

**Altitude.** Enter the altitude of installed Active Flow Controllers (mean sea level).

**PID control settings.** The Proportional + Integral + Derivative (PID) control loop is used to control the output of the group. Enter the settings for the Cool PIDs, then click **Apply**.



**Note:** The loops must be tuned after the room load is in place, and then tuned periodically if the room load changes. Only a qualified service technician should perform PID tuning.



For more information about PID tuning, see the *InRow RC Operation and Maintenance* manual, available on the *Utility* CD or on the APC Web site, [www.apc.com](http://www.apc.com).

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

**Active Flow Controller Lamp Test.** When enabled, lamps on all connected AFCs cycle through all three colors until the setting is set to OFF (this provides a way to verify connectivity).

## Unit

### Overview

View information for the various components of each unit in the group, including the following:

- Operating mode—On, Standby, or Idle.
- Cool output and demand—in kW.
- Rack Inlet Temperature—in degrees F or C.
- Supply and Return Air Temperatures—in degrees F or C.
- Air flow—in CFM or L/s.
- Fan speed—the average RPM of all fans, given as a percentage of the maximum fan speed.

### Detailed status

View information for the components of the units in the group:

- Input and output contact states—open or closed.
- Active power source—the power source supplying power to the unit, A or B.
- Filter differential pressure—the difference in pressure on either side of the air filter in WC or Pa.
- Fluid valve position—expressed as a percentage.
- Fluid flow in GPM or L/S.
- Entering and leaving fluid temperature in degrees F or C.

## Identification

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

- Model Number
- Serial Number
- Controller Firmware
- Hardware Revision
- Date of Manufacture

You can also configure the following identification information:

- **Unit ID**—Assign the unit a number from 1 to 12. The **Unit ID** may be unique for each cooling unit within the cooling group, but the same **Unit ID** can be assigned to multiple units.
- **Name**—Enter a name (up to 20 alphanumeric characters) for the unit.
- **Location**—Enter the location (up to 20 alphanumeric characters) of the unit.

Click **Apply** to save your changes.

## Run hours

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

## Service intervals

Set the service interval for the **Air Filter**, in weeks. The default service interval is 13 weeks.

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

## Thresholds

Configure high temperature thresholds for the rack inlet, supply air, return air, and entering fluid temperature sensors. If the respective temperature rises above the threshold, an alarm is activated. Click **Apply** to save your changes.

## Configuration

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

- **Startup Delay**—The delay, in seconds, 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.
- **Cool Capacity**—The setting used to determine chilled water flow to the unit. Use **Automatic** to have the Cooling Unit automatically control its output under normal (default) conditions. Use **Maximum** to run the Cooling Unit at full capacity.
- **Idle on Leak Detect**—When enabled, this setting causes the unit to idle when a leak is detected; the default setting is disabled.
- **Idle on Cool Fail**—When enabled, this setting causes the unit to idle when a cooling failure is detected; the default setting is enabled.
- **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 relay, open or closed.
- **Output Source**—The type of alarm that will activate the output relay: any alarm, or only critical alarms.
- **Power Source**—Select which power source supplies power to the unit.
- **Display Units**—The units (metric or US) displayed for each Cooling Unit.

# Logs

---

## Events

### Log

Use this option to 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”](#) on page 26.

- 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”](#) on page 45.

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; then click, in turn, on each major category of event.



See [“Configuring by event”](#) on page 44.

### 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

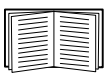
Use this option to access a log that periodically records InRow RC data. Each entry is listed by the date and time the data was recorded and provides the data in a column format.

To view the data log through the Web interface, click **log**.

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”](#) on page 26.

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

## Graphing

Use this option to create an interactive data graph. Select a maximum of four data parameters from the **Graph Data** drop-down list. Choose a time frame from the **Graph Time** drop-down list or enter a date range in the **From** and **To** fields. Click **Apply** to generate the graph.

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

Use the zoom tool above the graph to magnify the data shown on the screen. You can also click on any point in the graph to center and magnify that point on the screen. Use the left or right arrow bar to navigate through the data displayed in the magnified graph. Hover over any horizontal line in the graph to view the date, time, and Y-axis value for that data record.

## Interval

Use this option to define, in the **Data 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.

## Rotation

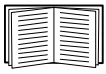
Use this option to set up a password-protected data log repository on a specified FTP server. Enabling rotation causes a copy of any previously unsaved entries in the data log to be appended to the file you specify by name and location. Updates to this file occur either at the upload interval that you 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
Last Upload Result	Indicates whether the last upload of the data file to the FTP server succeeded or failed, or displays "None Available."
Data Log Rotation	Enable or disable (the default) data log rotation.
FTP Server	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.
Unique File Name	Check the box to enable a unique file name.
Delay <i>hours</i> between Uploads	The number of hours between uploads of data to the specified file.
Upon failure, try uploading every <i>minutes</i>	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 ( <b>Number of Retries</b> ), the scheduled upload is skipped, and the system waits the number of hours specified as <b>Delay hours between Uploads</b> .

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

# Syslog

By default, the InRow RC 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.



This user 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](http://www.ietf.org/rfc/rfc3164.txt?number=3164).

## Servers

Use this option to identify one or more Syslog servers that will receive Syslog messages and to specify a port for each. Select the server address to edit existing server configurations or select **Add Server** to configure additional servers.

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 RC. Note: To use the Syslog feature, <b>Syslog Server</b> must be defined for at least one server.
Port	Identifies the user datagram protocol (UDP) port that the InRow RC will use to send Syslog messages. The default is <b>514</b> , the number of the UDP port assigned to Syslog.



## Settings

Leave the Syslog settings, except the **Server IP** settings, set to their defaults unless otherwise specified by the Syslog network or system administrator.

Setting	Definition
Message Generation	Enables (by default) or disables the Syslog feature.
Facility Code	Selects the facility code assigned to the InRow RC Syslog messages ( <b>User</b> , by default). Note: <b>User</b> is the selection that best defines the Syslog messages sent by the InRow RC. Do not change this selection unless advised to do so by the Syslog network or system administrator.
Severity Mapping	Maps each of the severity levels assigned to InRow RC events to the available Syslog priorities. You should not need to change the default mappings.  The following definitions are from RFC3164: <ul style="list-style-type: none"><li>• <b>Emergency</b>: The system is unusable</li><li>• <b>Alert</b>: Action must be taken immediately</li><li>• <b>Critical</b>: Critical conditions</li><li>• <b>Error</b>: Error conditions</li><li>• <b>Warning</b>: Warning conditions</li><li>• <b>Notice</b>: Normal but significant conditions</li><li>• <b>Info</b>: Informational messages</li><li>• <b>Debug</b>: Debug-level messages</li></ul> Following are the default settings for the four <b>Local Priority</b> settings: <ul style="list-style-type: none"><li>• <b>Critical</b> is mapped to <b>Critical</b></li><li>• <b>Warning</b> is mapped to <b>Warning</b></li><li>• <b>Informational</b> is mapped to <b>Info</b></li></ul> Note: To disable sending Syslog messages for <b>Critical</b> , <b>Warning</b> , or <b>Informational</b> events, see <a href="#">“Configuring event actions”</a> on page 44.

## Test

Use this option to send a test message to the Syslog servers configured through the **servers** option:

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 test message field. For example, `APC: Test Syslog`, meets the formatting requirements.

## 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-delimited event log file (*event.txt*) or data log file (*data.txt*) that you can import into a spreadsheet application.

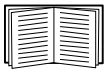
- The file reports all of the events recorded since the log was last deleted.
- The file includes information that the event log does not display.
  - The version of the file format (first field)
  - The date and time the file was retrieved
  - The **Name**, **Contact**, **Location** values, and IP address of the InRow RC
  - The unique **Event Code** for each recorded event (event log only)



**Note:** The InRow RC 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 the *Security Handbook*, available on the APC Network Management Card *utility* CD and on the APC Web site ([www.apc.com](http://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
```

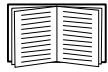
To use SCP to retrieve the *data.txt* file, use the following command:

```
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 RC 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](#)” on page 43. You can specify any port from 5001 to 32768.

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

3. You can use the **del** command to clear the contents of the event log or data log.

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

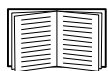
or

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

You will not be asked to confirm the deletion. If you clear the event log, a new *event.txt* file is created to record the event.

4. Type `quit` at the `ftp>` prompt to exit from FTP.

## Queries (Modbus requests and SNMP GETs)



See “[About](#)” on page 53 for information on configuring and using the request/response structure of building management systems using the Modbus protocol, and see “[access control](#)” on page 41 for a description of SNMP access types that enable an NMS to perform informational queries. Configuring the most restrictive SNMPv1 access type, `READ`, enables informational queries without the risk of allowing remote configuration changes.

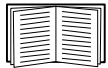
# Administration: Security

---

## Local Users

### Permission levels

Before you configure user access, be sure you understand the capabilities of each account type (Administrator, Device-Only 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-Only User, and Read-Only User), see “[Types of user accounts](#)” on page 3.

### Setting user access

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 Administrators and Device-Only Users to log on at the control console, display interface, 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-Only Users, and **readonly** for the Read-Only User.

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

## Remote Users

### Authentication

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



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](http://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 RC or another network-enabled device that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user permission level.
- RADIUS user names used with the InRow RC 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 the RADIUS server is not available.
- **RADIUS Only:** RADIUS is enabled. Local authentication is disabled.



**Note:** If **RADIUS Only** is selected, the only way to recover if the RADIUS server is unavailable, improperly identified, or improperly configured is to use a serial connection to the control console and change the **Authentication Method** setting to **Local Authentication Only** or **RADIUS, then Local Authentication**. See “[Local access to the control console](#)” on page 9 for information about how to access the serial port.

## RADIUS

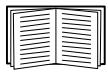
Use this option to do the following:

- Display a list of RADIUS servers identified as being available to the InRow RC and the time-out period for each server (the number of seconds the InRow RC will wait for a reply from the server before the request fails).
- Add a server to the list of identified RADIUS servers. Click **Add Server**, and configure the following parameters for authentication by the new server:

<b>RADIUS Setting</b>	<b>Definition</b>
<b>RADIUS Server</b>	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.
<b>Secret</b>	The shared secret between the RADIUS server and the InRow RC.
<b>Reply Timeout</b>	The time in seconds that the InRow RC waits for a response from the RADIUS server.
<b>Test Settings</b>	Enter the Administrator user name and password to test the RADIUS server path that you have configured.
<b>Skip Test and Apply</b>	Do not test the RADIUS server path.

# Configuring the RADIUS Server

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



For examples of the file entries needed to configure a RADIUS server for use with an InRow RC, see the *Security Handbook*, available on the *Utility CD* or from the APC Web site, [www.apc.com](http://www.apc.com).

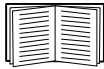
## Summary of the configuration procedure

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



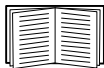
**Note:** RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.

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

3. VSAs 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 not work correctly. VSAs take precedence over standard RADIUS attributes.



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-Only 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 and Microsoft IAS 2003. Other commonly available RADIUS applications may work but have not been fully tested by APC.

## Auto Log Off

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

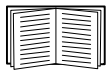
# Administration: Network

## TCP/IP and Communication Settings

### TCP/IP settings

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

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



For information on DHCP and DHCP options, see [RFC2131](#) and [RFC2132](#).

TCP/IP Setting	Description
Manual	The IP address, subnet mask, and default gateway must be configured manually. (The MAC address is not configurable.) Click <b>Next&gt;&gt;</b> and enter the new values.
BOOTP	<p>A BOOTP server provides the TCP/IP settings. At 32-second intervals, the InRow RC requests network assignment from any BOOTP server:</p> <ul style="list-style-type: none"><li>• If it receives a valid response, it starts the network services.</li><li>• If it finds a BOOTP server, but the request to that server fails or times out, the InRow RC stops requesting network settings until it is restarted.</li><li>• By default, If previously configured network settings exist, and it receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible if a BOOTP server is no longer available.</li></ul> <p>Click <b>Next&gt;&gt;</b> to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail to find a BOOTP server: <sup>1</sup></p> <ul style="list-style-type: none"><li>• <b>Maximum retries</b>: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.</li><li>• <b>If retries fail</b>: Select either <b>Use prior settings</b> (the default) or <b>Stop BOOTP request</b>.</li></ul>
<p>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"><li>• <b>Vendor Class</b>: APC</li><li>• <b>Client ID</b>: The MAC address of the InRow RC, which uniquely identifies it on the local area network (LAN)</li><li>• <b>User Class</b>: The name of the application firmware module</li></ul>	



TCP/IP Setting	Description
DHCP	<p>At 32-second intervals, the InRow RC requests network assignment from any DHCP server. By default, the number of retries is unlimited.</p> <ul style="list-style-type: none"> <li>• If the InRow RC 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.</li> <li>• If the InRow RC finds a DHCP server, but the request to that server fails or times out, the InRow RC stops requesting network settings until it is restarted.</li> <li>• If a DHCP server responds with an invalid offer (for example, the offer does not contain the APC Cookie), the InRow RC accepts the lease from that server on the last request of the sequence and then immediately releases that lease. This prevents the DHCP server from reserving the IP address associated with its invalid offer.</li> </ul> <p>For more information on what a valid response requires, see “<a href="#">DHCP response options</a>” on page 34</p> <p>To specify values other than the defaults, click <b>Next&gt;&gt;</b> to access the <b>DHCP Configuration</b> page.<sup>1</sup></p> <ul style="list-style-type: none"> <li>• <b>Require vendor specific cookie to accept DHCP Address:</b> To disable the requirement that the DHCP server provide the APC cookie, unmark this check-box.</li> <li>• <b>Maximum retries:</b> Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.</li> </ul>
DHCP and BOOTP	<p>The default setting. The InRow RC 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 from the default to <b>BOOTP</b> or <b>DHCP</b>, depending on the type of server that supplied the TCP/IP settings to the InRow RC.</p> <p>Click <b>Next&gt;&gt;</b> to access and configure the same settings that are available on the <b>BOOTP Configuration</b> and <b>DHCP Configuration</b> pages<sup>1</sup> and to specify that the <b>DHCP and BOOTP</b> setting be retained after either type of server provides the TCP/IP values.</p>
<p>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"> <li>• <b>Vendor Class:</b> APC</li> <li>• <b>Client ID:</b> The MAC address of the InRow RC, which uniquely identifies it on the local area network (LAN)</li> <li>• <b>User Class:</b> The name of the application firmware module</li> </ul>	

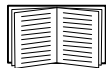
## DHCP response options

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

**Vendor specific information (option 43).** The InRow RC 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 RC that a DHCP server is configured to service APC devices. By default, this DHCP response option must contain the APC Cookie for the InRow RC to accept the lease.



To disable the requirement of an APC cookie, see “DHCP” on page 33.

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 InRow RC 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 **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**. The **TCP/IP Configuration** setting switches to **DHCP** when the InRow RC accepts the DHCP response. Whenever the InRow RC 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 RC 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 RC.
- **Subnet Mask** (option 1): The Subnet Mask value that the InRow RC needs to operate on the network.
- **Default Gateway** (option 3): The default gateway address that the InRow RC 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 RC.
- **Renewal Time, T1** (option 58): The time that the InRow RC 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 RC must wait after an IP address lease is assigned before it can seek to rebind that lease.

**Other options.** The InRow RC also uses the following 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 RC can use.
- **Time Offset** (option 2): The offset of the InRow RC'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 RC can use.
- **Host Name** (option 12): The host name that the InRow RC will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the InRow RC 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 an 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 RC will download the .ini file. After the download, the InRow RC uses the .ini file as a boot file to reconfigure its settings.

## 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 either 10 Mbps or 100 Mbps, each with the option of half-duplex (for communication in only one direction at a time) or full-duplex (for communication simultaneously in both directions on the same channel).

## DNS (Administration>Network>DNS>servers)

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 Domain Name System server. The InRow RC cannot send any e-mail messages unless at least the IP address of the primary DNS server is defined.
  - The InRow RC waits a maximum of 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 RC does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the InRow RC 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 RC:
  - **Host Name:** When an Administrator configures a host name here and a domain name in the **Domain Name** field, users can then enter a host name in any field in the InRow RC interface (except e-mail addresses) that accepts a domain name as input.


- **Domain Name:** An Administrator must configure the domain name here only. In all other fields in the InRow RC interface (except e-mail addresses) that accept domain names, the InRow RC 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, `example.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 RC 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
  - In the **Query Question** field, 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, formatted as <code>my_server.my_domain.com</code> .
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

Use the options under **Web** on the left navigation menu to configure the following:

Option	Description
access	<p>To activate changes to any of the following access selections, log off from and back on to the InRow RC:</p> <ul style="list-style-type: none"> <li>• <b>Disable</b>: Disables all access to the Web interface. (You must use the control console to re-enable access to the Web interface. Select <b>Network</b> and <b>Web/SSL/TLS</b>. Then for HTTP access, select <b>Access</b> and <b>Enabled</b>, and for HTTPS access, also select <b>Web/SSL</b> and <b>Enabled</b>.)</li> <li>• <b>Enable HTTP</b> (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.</li> <li>• <b>Enable HTTPS</b>: Enables Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) to provide Web access. Secure Sockets Layer (SSL) encrypts user names, passwords, and data during transmission, and provides authentication of the InRow RC by digital certificate.</li> </ul> <p>See “Creating and Installing Digital Certificates” in the <i>Security Handbook</i> on the APC Network Management Card <i>utility</i> CD to choose among the several methods for using digital certificates.</p> <p>When HTTPS is enabled, your browser displays a lock icon, usually at the bottom of the screen:</p>  <p><b>HTTP Port</b>: Identifies the TCP/IP port used for communication by HTTP with the InRow RC. The default is 80.</p> <p><b>HTTPS Port</b>: Identifies the TCP/IP port used for communication by HTTPS with the InRow RC. The default is 443.</p> <p>You can change either port setting to the number of any unused port from 5000 to 32768 to enhance the protection provided by User Name and Password settings. You must then use a colon (:) in the address field of the browser to specify the non-default port number. For example, for port 5000 and the InRow RC IP address of 152.214.12.114, you would use one of these Web addresses:</p> <pre style="text-align: center;">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"> <li>• <b>DES</b>: A block cipher that provides authentication by Secure Hash Algorithm.</li> <li>• <b>RC4_MD5</b> (enabled by default): A stream cipher, providing authentication by MD5 hash algorithm.</li> <li>• <b>RC4_SHA</b> (enabled by default): A stream cipher that provides authentication by Secure Hash Algorithm.</li> <li>• <b>3DES</b>: A block cipher that provides authentication by Secure Hash Algorithm.</li> </ul>

Option	Description
ssl certificate	<p>Add, replace, or remove a security certificate.</p> <p><b>Status:</b></p> <ul style="list-style-type: none"> <li>• <b>Not installed:</b> A certificate is not installed, or a certificate was installed by FTP or SCP to an incorrect location. Using <b>Add or Replace Certificate File</b> installs the certificate to the correct location, /sec on the InRow RC.</li> <li>• <b>Generating:</b> The InRow RC is generating a certificate because no valid certificate was found.</li> <li>• <b>Loading:</b> A certificate is being activated on the InRow RC.</li> <li>• <b>Valid certificate:</b> A valid certificate was installed or was generated by the InRow RC. Click on this link to view the certificate contents.</li> </ul> <p><b>If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the InRow RC generates a default certificate, a process which delays access to the interface for up to five minutes.</b> You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on.</p> <p><b>Add or Replace Certificate File:</b> 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 APC Network Management Card <i>utility</i> CD to choose a method for using digital certificates, including certificates created by the Security Wizard or generated by the InRow RC.</p> <p><b>Remove:</b> Delete the current certificate.</p>

## Console

Use the options under **Console** on the left navigation menu to configure the following:

Option	Description
access	<p>Choose one of the following:</p> <ul style="list-style-type: none"> <li>• <b>Disable:</b> Disables all access to the control console.</li> <li>• <b>Enable Telnet</b> (the default setting): Telnet transmits user names, passwords, and data without encryption.</li> <li>• <b>Enable SSH v1 and v2:</b> Do not enable both versions 1 and 2 of Secure SHell (SSH) unless you require that both be activated at the same time. (Security protocols use extensive processing power.)</li> <li>• <b>Enable SSH v1 only:</b> Secure SHell (SSH) version 1 transmits user names, passwords, and data in encrypted form. There is little or no delay as you log on.</li> <li>• <b>Enable SSH v2 only:</b> Secure SHell (SSH) version 2 transmits user names, passwords, and data in encrypted form with somewhat more protection than version 1 from attempts to intercept, forge, or alter data during transmission. There is a noticeable delay as you log on.</li> </ul> <p>Identify the TCP/IP port used for communications with the Network Management Card of the InRow RC by Telnet and Secure SHell (SSH).</p> <ul style="list-style-type: none"> <li>• <b>Telnet Port:</b> The default is 23.</li> <li>• <b>SSH Port:</b> The default is 22.</li> </ul> <p>You can change the Port setting to the number of any unused port from 5000 to 32768 to enhance the protection provided by User Name and Password settings.</p> <ul style="list-style-type: none"> <li>• For Telnet, you must use either a colon (:) or a space in the command line, according to the requirements of your Telnet client program, to specify the non-default port number. For example, for a port number of 5000 and the InRow RC IP address of 152.214.12.114, your Telnet client requires one of the following commands:           <pre style="margin-left: 40px;">telnet 152.214.12.114:5000 telnet 152.214.12.114 5000</pre> </li> <li>• For SSH, see the documentation for your SSH client for the command line format required to specify a non-default port when starting SSH.</li> </ul>
ssh encryption	<p>Enable or disable encryption algorithms (block ciphers) compatible with SSH version 1 or version 2 clients:</p> <p>SSH v1 algorithms:</p> <ul style="list-style-type: none"> <li>• <b>DES</b></li> <li>• <b>Blowfish:</b> If your SSH v1 client cannot use Blowfish, which is always enabled, you must also enable DES.</li> </ul> <p>SSH v2 algorithms:</p> <ul style="list-style-type: none"> <li>• <b>3DES:</b> (enabled by default)</li> <li>• <b>Blowfish:</b> (enabled by default)</li> <li>• <b>AES 128</b></li> <li>• <b>AES 256</b></li> </ul> <p>Your SSH v2 client selects the enabled algorithm that provides the highest security. If your SSH client cannot use the default algorithms, you must enable an AES algorithm that it can use.</p>

Option	Description
ssh host key	<p><b>Status</b> indicates the status of the host key (private key):</p> <ul style="list-style-type: none"> <li>• <b>SSH Disabled: No host key in use:</b> SSH is disabled and is not using a host key even if one is loaded.</li> <li>• <b>Generating:</b> The InRow RC is creating a host key because no valid host key was found.</li> <li>• <b>Loading:</b> A host key is being activated on the InRow RC.</li> <li>• <b>Valid:</b> One of the following valid host keys is in the <code>/sec</code> directory (the required location on the InRow RC): <ul style="list-style-type: none"> <li>• A 1024-bit host key created by the APC Security Wizard.</li> <li>• A 768-bit RSA host key generated by the InRow RC.</li> </ul> </li> </ul> <p><b>Add or Replace:</b> Upload a host key file created by the APC Security Wizard to the <code>/sec</code> directory:</p> <ol style="list-style-type: none"> <li>1. Click <b>Browse</b>.</li> <li>2. Locate the file.</li> <li>3. Click <b>Apply</b>.</li> </ol> <p>If you use FTP or Secure CoPy (SCP) instead to transfer the host key file, you must specify the <code>/sec</code> directory as the target location in the command.</p> <p>To use the APC Security Wizard, see the <i>Security Handbook</i> on the APC Network Management Card <i>utility</i> CD.</p> <p>Note: To reduce the time required to enable SSH, create and upload a host key in advance. <b>If you enable SSH with no host key loaded, the InRow RC takes up to 5 minutes to create a host key, and the SSH server is not accessible during that time.</b></p> <p><b>Remove:</b> Remove the current host key.</p>



**Note:** To use SSH, you must have a SSH client installed. Most Linux and other UNIX<sup>®</sup> platforms include a SSH client, but Microsoft Windows operating systems do not. SSH clients are available from various vendors.

## SNMP

**SNMPv1.** 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 Central or InfraStruXure Manager to manage an InRow RC on the public network of an InfraStruXure system, you must have SNMP enabled in the InRow RC. Read access will allow InfraStruXure Central or InfraStruXure Manager to receive traps from the InRow RC, but Write access is required while you use the interface of the InRow RC to set InfraStruXure Central or InfraStruXure Manager as a trap receiver.



For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available on the APC Network Management Card *utility* CD or from the APC Web site, [www.apc.com](http://www.apc.com).



Use the options under **SNMP** on the left navigation menu to configure the following:

Option	Description
access	<p><b>Enable SNMPv1 Access:</b> Enables SNMP version 1 as a method of communication with this device.</p>
access control	<p>You can configure up to four access control entries to specify which Network Management Systems (NMS) have access to this device. The opening page for access control, by default, assigns one entry to each of the four available SNMPv1 communities, but you can edit these settings to apply more than one entry to any community to grant access by several specific IP addresses, host names, or IP address masks. To edit the access control settings for a community, click its community name.</p> <ul style="list-style-type: none"> <li>• If you leave the default access control entry unchanged for a community, that community has access to this device from any location on the network.</li> <li>• If you configure multiple access control entries for one community name, the limit of four entries requires that one or more of the other communities must have no access control entry. If no access control entry is listed for a community, that community has no access to this device.</li> </ul> <p><b>Community Name:</b> The name that a NMS must use to access the community. The maximum length is 15 ASCII characters, and the default community names for the four communities are "public," "private," "public2," and "private2."</p> <p><b>NMS IP/Host Name:</b> The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows:</p> <ul style="list-style-type: none"> <li>• 149.225.12.255: Access only by a NMS on the 149.225.12 segment.</li> <li>• 149.225.255.255: Access only by a NMS on the 149.225 segment.</li> <li>• 149.255.255.255: Access only by a NMS on the 149 segment.</li> <li>• 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.</li> </ul> <p><b>Access Type:</b> The actions an NMS can perform through the community.</p> <ul style="list-style-type: none"> <li>• <b>Read:</b> GETS only, at any time.</li> <li>• <b>Write:</b> GETS at any time, and SETS when no user is logged onto the Web interface or Control Console.</li> <li>• <b>Write+:</b> GETS and SETS at any time.</li> <li>• <b>Disabled:</b> No GETS or SETS at any time.</li> </ul>

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



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

The InRow RC supports only MD5 authentication and DES encryption.

Option	Description
access	<p><b>SNMPv3 Access:</b> Enables SNMPv3 as a method of communication with this device.</p>
user profiles	<p>By default, lists the settings of four user profiles, configured with the user names "apc snmp profile1" through "apc snmp profile 4," and no authentication and no privacy (no encryption of data). To edit the following settings for a user profile, click a user name in the list.</p> <p><b>User Name:</b> The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters.</p> <p><b>Authentication Passphrase:</b> A phrase of 15 to 32 ASCII characters that verifies that the NMS communicating with this device through SNMPv3 is the NMS it claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time.</p> <p><b>Privacy Passphrase:</b> A phrase of 15 to 32 ASCII characters that ensures the privacy of the data (by means of encryption) that a NMS is sending to this device or receiving from this device through SNMP v3.</p> <p><b>Authentication Protocol:</b> The APC implementation of SNMPv3 supports MD5 authentication. Authentication will not occur unless MD5 is selected here.</p> <p><b>Privacy Protocol:</b> The APC implementation of SNMPv3 supports DES as the protocol for encrypting and decrypting data. Privacy of transmitted data requires that DES is selected here.</p> <p><b>Note:</b> You cannot select the privacy protocol if no authentication protocol is selected.</p>
access control	<p>You can configure up to four access control entries to specify which NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four user profiles, but you can edit these settings to apply more than one entry to any user profile to grant access by several specific IP addresses, host names, or IP address masks.</p> <ul style="list-style-type: none"> <li>• If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device.</li> <li>• If you configure multiple access entries for one user profile, the limit of four entries requires that one or more of the other user profiles must have no access control entry. If no access control entry is listed for a user profile, no NMS that uses that profile has any access to this device.</li> </ul> <p>To edit the access control settings for a user profile, click its user name.</p> <p><b>Access:</b> Mark the Enable checkbox to activate the access control specified by the parameters in this access control entry.</p> <p><b>User Name:</b> Select from the drop-down list the user profile to which this access control entry will apply. The choices available are the four user names that you configure through the <b>user profiles</b> option on the left navigation menu.</p> <p><b>NMS IP/Host Name:</b> The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. An IP address mask that contains 255 restricts access as follows:</p> <ul style="list-style-type: none"> <li>• 149.225.12.255: Access only by a NMS on the 149.225.12 segment.</li> <li>• 149.225.255.255: Access only by a NMS on the 149.225 segment.</li> <li>• 149.255.255.255: Access only by a NMS on the 149 segment.</li> <li>• 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.</li> </ul>

## 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 for communication with the InRow RC. 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 32767 to enhance the protection provided by User Name and Password settings. You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 5001 and the InRow RC IP address of 152.214.12.114, you would use this command:

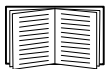
```
ftp 152.214.12.114:5001
```



**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 RC to be accessible for management by InfraStruXure Central or InfraStruXure Manager, FTP Server must be enabled in the InRow RC interface.

## Related Topics



See these related topics:

- [“Console”](#) on page 39 to configure SSH.
- [“How to use FTP or SCP to retrieve the log files”](#) on page 26 to obtain a text version of the event log.

# Administration: Notification

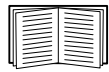
---

## Event Actions

### Types of notification

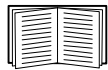
You can configure event actions to occur in response to an event or a group of events. These actions notify users of the event in any of several ways:

- 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](#)” on page 20 for information on configuring the output contact.

- 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](#)” on page 41 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, or using Serial Modbus enables informational queries without the risk of allowing remote configuration changes.

### Configuring event actions

You can configure event actions for individual events or for predefined groups of events.

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

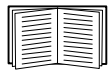
1. Select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu.
2. Follow the on-screen instructions to list events by severity, either by main category or sub-category.
3. In the list of events, check the marked columns 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 checkboxes 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 RC 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 “[Syslog](#)” on page 24, “[Recipients](#)” on page 48, and “[Trap receivers.](#)” on page 49.

**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 and select **Next**:
  - If you choose **Events 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 **Events by category**, you can then select all events in one or more predefined categories.

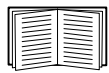
3. Select event actions for all events in the group.



**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 checkboxes 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 RC 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 [“Recipients”](#) on page 48 or [“Trap receivers.”](#) on page 49.

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.

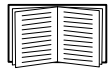
# Active, Automatic, Direct Notification

## E-mail

**Overview of setup.** Use the Simple Mail Transfer Protocol (SMTP) to send e-mail to up to four recipients when an event occurs.

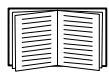
To use the e-mail feature, you must define the following settings:

- The IP addresses of the primary and, optionally, of the secondary Domain Name System (DNS) servers



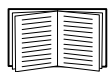
See “[DNS \(Administration>Network>DNS>servers\)](#)” on page 35.

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



See “[SMTP \(Administration>Notification>E-mail>server\)](#)” on page 47.

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



To configure recipients, see “[Recipients](#)” on page 48.



**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	The IP address (or if DNS is configured, the DNS name) of the local SMTP server. Note: This definition is required only when <b>SMTP Server</b> is set to <b>Local</b> when e-mail recipients are being configured. See “ <a href="#">Recipients</a> ” on page 48.
From Address	The contents of the <b>From</b> field in the format <i>user@[IP_address]</i> (if an IP address is specified as <b>Local SMTP Server</b> ) or <i>user@domain.com</i> (if DNS is configured and the DNS name is specified as <b>Local SMTP Server</b> ) in the e-mail messages sent by the InRow RC. Note: The local SMTP server configuration may require that you use a valid user account on the server for this setting. See the server documentation for more information.

**Recipients.** Use this option to identify up to four e-mail recipients. Click a recipient **To Address** to edit that configuration. Select **Add Recipient** to add a new recipient.

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 pager gateway account (for example, myacct100@skytel.com). The pager gateway will generate the page.</p> <p>You can bypass the DNS lookup of the mail server IP address by using the IP address in brackets instead of the e-mail domain name. For example, use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly.</p> <p>Note: The recipient pager must be able to use text-based messaging.</p>
E-mail Generation	Enables (by default) or disables sending e-mail to the recipient.
SMTP Server	<p>Selects one of the following methods for routing e-mail:</p> <ul style="list-style-type: none"> <li>• <b>Local:</b> Through the SMTP server of the InRow RC (the recommended setting). This option ensures that the e-mail is sent before the InRow RC 20-second time-out, and, if necessary, is retried several times. Also do one of the following: <ul style="list-style-type: none"> <li>• Enable forwarding at the InRow RC SMTP server so that it 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.</li> <li>• Set up a special e-mail account for the InRow RC to forward e-mail to an external mail account.</li> </ul> </li> <li>• <b>Recipient:</b> Directly to the recipient 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 RC tries to send the e-mail only once.</li> </ul> <p>When the recipient uses the InRow RC SMTP server, this setting has no effect.</p>
Format	Select <b>Long</b> or <b>Short</b> . The <b>Long</b> format contains Name, Location, Contact, IP address, serial number of the device, date, time, event code, and event description. The <b>Short</b> format provides only the event description.

**Test.** Use this option to send a test message to a configured recipient.



## SNMP traps

**Trap receivers.** This option lists, by NMS IP/Host Name, up to the maximum number (six) of trap receivers allowed.

- To open the page for configuring a new trap receiver, click **Add Trap Receiver**.
- To modify or delete a trap receiver, first click its IP address or host name to access its settings. (If you delete a trap receiver, all notification settings configured under Event Actions for the deleted trap receiver are set to their default values.)
- To specify the trap type for a trap receiver, select either the SNMPv1 or SNMPv3 radio button. For an NMS to receive both types of traps, you must configure two trap receivers for that NMS, one for each trap type.

Item	Definition
Trap Generation	Enable (the default) or disable trap generation for this trap receiver.
NMS IP/Host Name	The IP address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.

### SNMPv1 option.

Community Name	The name ("public" by default) used as an identifier when SNMPv1 traps are sent to this trap receiver.
Authenticate Traps	When this option is enabled (the default), the NMS identified by the NMS IP/Host Name setting will receive authentication traps (traps generated by invalid attempts to log on to this device). To disable that ability, unmark the checkbox.

**SNMPv3 option.** Select the identifier of the user profile for this trap receiver. (To view the settings of the user profiles identified by the user names selectable here, choose **Network** on the top menu bar and **user profiles** under **SNMPv3** on the left navigation menu.)

**Test.** Use this option to test the sending of a trap to a configured trap receiver.

**Last test result**—The result of the most recent SNMP trap test. A successful SNMP trap test verifies only that a trap was sent; it does not verify that the trap was received by the selected trap receiver. A trap test succeeds if all of the following are true:

- The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
- The trap receiver is enabled.
- If a host name is selected for the **To** address, that host name can be mapped to a valid IP address.

**To**—Select the IP address or host name to which a test SNMP trap will be sent. If no trap receiver was ever configured, a link to the **Trap Receiver** configuration page is displayed. (If a trap receiver was deleted, or was reset to its default values by this or any other management application, the default values for its trap type are listed.)

# Administration: General

---

## Information about the InRow RC

### Identification

Use this option to define the System **Name**, **Contact**, and **Location** values used to identify the InRow RC. For example, you might configure **Name** as Test Lab, **Contact** (whom to contact about the device) as Donald Adams, and **Location** as Building 3.

### Date & time

**Mode.** Use this option to set the time and date used by the InRow RC. 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 RC.
  - 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 RC.

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 RC accesses the NTP Server for an update. The minimum is 1 hour; the maximum is 8760 hours (1 year).
Update Using NTP Now	Mark this checkbox and click <b>Apply</b> to initiate an immediate update of the date and time by the NTP Server.

**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:

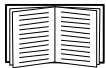
- If the local Daylight Saving Time always starts or ends on the 4th occurrence of a specific weekday of a month (for example, the 4th Sunday), choose Fourth/Last. If a 5th Sunday occurs in that month in a subsequent year, the time setting will still change to or from Daylight Saving Time on the 4th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

**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.

### User configuration file (.ini)

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

Use the **Browse** button to upload an .ini file.



For further detail, see [“How to Export Configuration Settings”](#) on page 57.

### Unit preference

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.

## 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	Resets Security, Network, Notification, General, and Logs configuration settings. It does not reset Cooling Group and Cooling Unit configuration settings.  Mark the <b>Exclude TCP/IP</b> checkbox to reset all device settings except the TCP/IP settings. Note: To reset all device settings leave the <b>Exclude TCP/IP</b> checkbox unchecked.
Reset Only	You can choose one or more of the following options by marking their checkboxes:  <b>TCP/IP:</b> 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.  <b>Event Configuration:</b> Resets only events to their default configuration. Any configuration changes, by event or by group, will revert to their default settings.

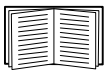
## Serial Modbus

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 RC 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 RC 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](http://www.apc.com)), search for your product, 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 on Modbus, see the Modbus Standard Library at [www.modbus.org](http://www.modbus.org).

## 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 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.

## About

The hardware information is especially useful to APC Customer Support in helping to troubleshoot problems with your InRow RC. The serial number and MAC address accessible through the **About** menu option are also available on the InRow RC itself. Management Uptime shows the time that has elapsed since the last reset or reboot.

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.

# APC Device IP Configuration Wizard

---

## Purpose and Requirements

### Purpose: configure basic TCP/IP settings

You can use the APC Device IP Configuration Wizard to configure the basic TCP/IP settings (IP address, subnet mask, and default gateway) of the following:

- Network Management Cards
- Network-enabled devices (devices that contain embedded Network Management Cards)

Using the Wizard, you can configure the basic TCP/IP settings of installed or embedded Network Management Cards in either of the following ways:

- Automatically discover and configure unconfigured Network Management Cards or network-enabled devices remotely over your TCP/IP network.
- Configure or reconfigure a Network Management Card or network-enabled device through a direct connection from the serial port of your computer to the device that contains the card.



**Note:** The Wizard can discover and configure Network Management Cards or devices only if they are on the same network segment as the computer that is running the Wizard.

### System requirements

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

## Install the Wizard

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.com/tools/download](http://www.apc.com/tools/download).
2. Download the Device IP Configuration Wizard.
3. Run the executable file in the folder to which you downloaded it.

# Use the Wizard

## Launch the Wizard

The installation creates a shortcut link in the **Start** menu that you can use to launch the Wizard.

## Configure the basic TCP/IP settings remotely

**Prepare to configure the settings.** Before you run the Wizard, be sure that you have the information you will need during the configuration procedure:

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 so that you can identify each Network Management Card or device that the Wizard discovers. (The Wizard displays the MAC address for a discovered card or device on the same screen on which you then enter the TCP/IP settings.)
  - For Network Management Cards 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 — for example, usually on the side of a device that you mount in a rack.

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, over the network, Network Management Cards or network-enabled devices that are not configured:

1. From the **Start** menu, launch the Wizard. The Wizard automatically 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 TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the unconfigured Network Management Card or network-enabled device identified by the MAC address at the top of the screen. Then 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 you transmit the settings.

4. 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**.
5. The Wizard searches for another unconfigured Network Management Card or device. If it finds one, it displays the screen with data entry boxes for the TCP/IP settings of that card or device.
  - To skip configuring the Network Management Card or device whose MAC address is currently displayed, click **Cancel**.
  - To configure the TCP/IP settings of the next card, repeat this procedure beginning at step 3.

## Configure or reconfigure the TCP/IP settings locally

To configure a single Network Management Card or network-enabled device through a serial connection:

1. Contact your network administrator to obtain valid TCP/IP settings.
2. Connect the RS-232 configuration cable that came with the Network Management Card or device.
  - a. Connect one end to an available communications port on your computer. Make sure no other application is using the port.
  - b. Connect the other end to the serial port of the card or device.
3. From the **Start** menu, launch the Wizard application.
  - If the Network Management Card or network-enabled device is not configured, wait for the Wizard to detect it.
  - If you are assigning basic TCP/IP settings serially to a Network Management Card or device, click **Next>**.
4. Select **Locally (through the serial port)**, and click **Next >**.
5. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the Network Management Card or device. Then click **Next >**.
6. On the **Transmit Current Settings Locally** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the Network Management Card or device after you transmit the settings.
7. Switch the main breaker on the front of the electrical panel to OFF. Wait one second. Switch the main breaker to ON.



**Note:** If you wait too long to return power to the Cooling Unit, you must repeat step 7.

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**.

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



# How to Export Configuration Settings

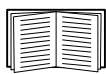
---

## 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 RC and export that file to another InRow RC or to multiple InRow RCs.

1. Configure the InRow RC to have the settings you want to export.
2. Retrieve the .ini file from that InRow RC.
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 RC to transfer the copied file to one or more additional InRow RCs. (To transfer the file to multiple InRow RCs simultaneously, write an FTP or SCP script that repeats the steps for transferring the file to a single InRow RC.)
5. Each receiving InRow RC 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 RCs and export them to other InRow RCs, see *Release Notes: ini File Utility, version 1.0* on the APC Network Management Card *utility* CD.

### Contents of the .ini file

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

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



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

- Each keyword is followed by an equals sign and the current *value* for that parameter 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 RC) 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 RC or cause that InRow RC to use an NTP Server to set its date and time.



See “[Customizing](#)” on page 58 for configuration guidelines for date and time settings.

## Detailed procedures

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

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

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



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

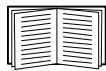
2. Use FTP to retrieve the file config.ini from the InRow RC you configured:
3. Open a connection to the InRow RC, using its IP address. For example:

```
ftp> open 158.165.2.132
```

4. Log on, using the Administrator user name and password configured for the InRow RC.
5. Retrieve the config.ini file containing the InRow RC current settings:

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

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



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

**Customizing.** You must customize the file to change at least the TCP/IP settings before you export it. 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 RCs 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 (;).
- Copy the customized file to another file name in the same folder:
- The copy, which you will export to other InRow RCs, 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 RC.** To transfer the .ini file to one other InRow RC, do either of the following:

- From the Web interface of the receiving InRow RC, 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 RCs (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 RC to which you are exporting the .ini file. For example:

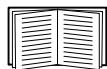
```
ftp> open 158.165.4.135
```

- b. Export the copy of the customized .ini file. The receiving InRow RC 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 RCs.** To export the .ini file to multiple InRow RCs:

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



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

# The Upload Event and Error Messages

## The event and its error messages

The following event occurs when the receiving InRow RC 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.

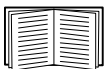


**Note:** The export to and the subsequent upload by the receiving InRow RC succeeds even if there are errors.

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, the InRow RC stores and processes what it can, but ignores what it cannot. Reduce the size of the file, or divide it into two files, and try uploading again.

## Errors generated by overridden values

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

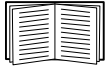


See “[Contents of the .ini file](#)” on page 57 for information about which values are overridden.

The overridden values are device-specific and not appropriate to export to other InRow RCs. 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 RCs by using the APC Device IP Configuration Wizard.



See [“APC Device IP Configuration Wizard”](#) on page 54 for a detailed description of how to discover and configure the basic TCP/IP settings of unconfigured InRow RCs remotely over your TCP/IP network. This section will also tell you how to configure or reconfigure one InRow RC through a direct connection from the serial port of your computer to the InRow RC.

# File Transfers

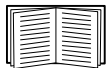
---

## Overview

The InRow RC automatically recognizes binary firmware files. Each of these files contains a header and one or more Cyclical Redundancy Checks (CRCs) to ensure that the data contained in the file is not corrupted before or during the transfer operation.

When new firmware is transmitted to the InRow RC, the program code is updated and new features become available.

This chapter describes how to transfer firmware files to the InRow RC.



To verify a file transfer, see [“Verifying Upgrades and Updates” on page 66](#).

## Upgrading Firmware

### Benefits of upgrading firmware

Upgrading the firmware on the InRow RC has the following benefits:

- New firmware has 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 RCs support the same features in the same manner.

### Firmware files (InRow RC)

A firmware version consists of two modules: An APC Operating System (AOS) module and an application module.

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

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

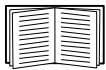
- **apc**: Indicates that this is an APC file.
- *hardware-version*: *hw0x* identifies the version of the hardware on which you can use this binary file.
- *type*: *aos* if the file is the APC Operating System (AOS) module, or *acrp* if the file is the application module for the InRow RC.
- *version*: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

## Obtain the latest firmware version

**Automated upgrade tool for Microsoft Windows systems.** An automated self-extracting executable tool combines the firmware modules that you need to automate your upgrades on any supported Windows operating system. You can obtain the latest firmware version of the tool at no cost. At the support section of the APC web site [www.apc.com/tools/download](http://www.apc.com/tools/download), find the latest firmware release for your APC product (in this case, your InRow RC) and download the automated tool.

Each upgrade tool is specific to an APC product type. If you use a version of the tool from the APC Web site, make sure that you use the upgrade tool that corresponds with your APC product type.

**Manual upgrades, primarily for Linux systems.** If all computers on your network are running Linux, you must upgrade the firmware of the InRow RCs manually, i.e., by using the separate APC firmware modules (AOS module and application module).



If you have a networked computer running a supported Microsoft Windows operating system on your network, you can use the tool described in “[Automated upgrade tool for Microsoft Windows systems](#)” on page 63 to upgrade the firmware of the InRow RC automatically over the network. This tool automates the entire upgrade process.

You can obtain the individual firmware modules you need for a manual firmware upgrade by extracting them from the automated tool.

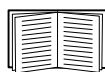
## Firmware file transfer methods

To upgrade the firmware of the InRow RC:

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



**Note:** When you transfer individual firmware modules and do not use the automated firmware upgrade tool to upgrade the firmware for the InRow RC, you must transfer the AOS module to the InRow RC before you transfer the application module.



For more information about the firmware modules, see “[Firmware files \(InRow RC\)](#)” on page 62.

## Use FTP or SCP to upgrade one InRow RC

**Instructions for using FTP.** For you to be able to use FTP to upgrade a single InRow RC over the network:

- The InRow RC must be connected to the network.
- The FTP server must be enabled at the InRow RC.
- The InRow RC must have its TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway** addresses) configured.

To use FTP to upgrade the InRow RC:

1. Open an MS-DOS command prompt window on a computer that is connected to the network. Go to the directory that contains the firmware upgrade files, and list the files. For the directory C:\apc, the commands would be those shown in **bold**:

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

Files listed for the InRow RC, for example, might be the following (with xxx representing the version number of each file):

- apc\_hw03\_aos\_**xxx**.bin
- apc\_hw03\_acrc\_**xxx**.bin

2. Open an FTP client session:

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

3. Type **open** and the InRow RC IP address, and press ENTER. If the **port** setting for the FTP Server (accessible through the **Administration** tab, **Network** on the top menu bar, and **FTP Server** on the left navigation menu) has changed from its default of **21**, you must use the non-default value in the FTP command.
  - a. For some FTP clients, use a colon to add the port number to the end of the IP address.
  - b. For Windows FTP clients, separate the port number from the IP address by a space. For example, if the InRow RC **FTP Server Port** setting has been changed from its default of **21**, such as to **21000**, you would use the following command for a Windows FTP client transferring a file to the InRow RC with an IP address of 150.250.6.10.  
ftp> **open 150.250.6.10 21000**
4. Log on using the Administrator user name and password. (**apc** is the default for both.)
5. Upgrade the AOS. (In the **put** command in the following example, xxx is the firmware version number, with no periods separating the digits:)

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

6. When FTP confirms the transfer, type **quit** to close the session.
7. Wait 20 seconds, and then repeat step 2 through step 5, but in step 5, use the application module file name instead of the AOS module.



**Instructions for using SCP.** To use Secure CoPy (SCP) to upgrade the firmware for one InRow RC:

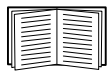
1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the InRow RC. The following example assumes an InRow RC IP address of 158.205.6.185, and an AOS module of **apc\_hw03\_aos\_xxx.bin**. (with *xxx* representing the version number of the AOS module, with no periods separating the digits).

```
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 instead of the AOS module, to transfer the application module to the InRow RC.

## Upgrade multiple InRow RCs

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



See *Release Notes: ini File Utility, version 1.0* on the APC Network Management Card *utility* CD.

**Use FTP or SCP to upgrade multiple InRow RCs.** To upgrade multiple InRow RCs using an FTP client or using SCP, write a script which automatically performs the procedure. For FTP, use the steps in “[Use FTP or SCP to upgrade one InRow RC](#)” on page 64 in the script.

## Use XMODEM to upgrade one InRow RC

To use XMODEM to upgrade the firmware for a single InRow RC that is not on the network:

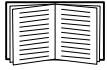
1. Obtain the individual firmware modules (the AOS module and the application module) from [www.apc.com/tools/download](http://www.apc.com/tools/download).
2. Select a serial port at the local computer and disable any service which uses that port.
3. Connect the RS-232 configuration cable (APC part number 940-0103A) that came with the InRow RC to the selected port and to the serial port at the InRow RC.
4. Run a terminal program (such as HyperTerminal), and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, no flow control, and save the changes.
5. Press ENTER twice to display the **User Name** prompt.
6. Enter the Administrator user name and password (**apc** by default for both).
7. From the **Control Console** menu, select **System**, then **Tools**, then **File Transfer**, then **XMODEM**; and type **Yes** at the prompt to continue.
8. At the prompt for the baud rate, enter an appropriate baud rate for the terminal program to use for the transfer. A higher baud rate causes faster firmware upgrades.



**Note:** Allowed values are 2400, 9600, 19200, and 38400. To choose a baud rate different from your current connection, disconnect from the terminal session. Configure the selected port for the desired baud rate and reconnect the terminal session.

Press ENTER. The screen displays uppercase C, indicating transfer mode.

9. From the terminal program menu, select the binary AOS file to transfer via XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600 (if you selected a different rate in step 8). The InRow RC automatically restarts.
10. Repeat step 4 through step 9 to install the application module. In step 9, use the application module file name, not the AOS module file name.



For information about the file name format used for application modules, see [“Firmware files \(InRow RC\)” on page 62](#).

## Verifying Upgrades and Updates

### Overview

To verify that the firmware upgrade was successful, see the **Last Transfer Result** message, available through the **FTP Server** option of the **Network** menu (in the control console only), or use an SNMP GET to the **mfiletransferStatusLastTransferResult** object identifier (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.

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



# 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 the APC Customer Support Center by telephone or e-mail.
  - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.

For information on how to obtain local customer support, contact the APC representative or other distributors from whom you purchased your APC product.

© 2012 APC by Schneider Electric. APC, the APC logo, and InRow are owned by Schneider Electric Industries S.A.S., American Power Conversion Corporation, or their affiliated companies. All other trademarks are property of their respective owners.