Contents

Introduction 1

Product Description 1
Features of the Rack Automatic Transfer Switch 1
Initial setup 2
Access Procedures 3
Overview 3
Access priority for logging on 3
Types of user accounts 4
Recovering from a Lost Password 5
Upgrading Firmware Through a Serial Connection 6
Front Panel 8
Link-RX/TX (10/100) LED 10
Status LED 10
Load indicator LED 11
Watchdog Features 11
Overview 11
Network interface watchdog mechanism 11
Resetting the network timer 12

Control Console 13

How to Log On 13
Overview 13
Remote access to the control console 13
Local access to the control console 14
Main Screen 15
Example main screen 15
Information and status fields 16
Control Console Menus 18
How to use control console menus 18
Main Menu 18
Device Manager option 19
Network option 19
System option 20

Web Interface 21

Introduction 21
Supported Web browsers 21
How to Log On 22
Overview 22
URL address formats 23
How to Use the Tabs, Menus, and Links 24
Tabs 24
Menus 24
Quick Links 25
Home Page 26
Overview 26
Quick status icons 26
Active Alarms 27
Device Status 27
ATS Parameters 27
Recent Device Events 28
Additional information on Home page 28
Selecting a menu to perform a task 28

Unit Menus 30

Unit Tab 30
Status 30
Measurements 31
Configuration 31
Control 33
Event Counts 33
About ATS 33
Automatic Transfer Switch Settings 34
Configuring load thresholds 34
Setting the Low Load Warning Threshold 35

Administration: Security 36

Local Users 36
Setting user access (Administration>Security>
Local Users>*options*) 36
Remote Users 36

Authentication (Administration>Security>Remote Users>authentication) 36
RADIUS (Administration>Security>Remote Users>RADIUS) 37

Configuring the RADIUS Server 38

Summary of the configuration procedure 38
Configuring a RADIUS server on UNIX® with shadow passwords 39
Supported RADIUS servers 39

Inactivity Timeout (Administration>Security>Auto Log Off) 40

Administration: Network Features 41

TCP/IP and Communication Settings 41

TCP/IP settings (Administration>Network>TCP/IP) 41
DHCP response options 43
Port Speed (Administration>Network>Port Speed) 45

DNS (Administration>Network>DNS>*options*) 46

Web (Administration>Network>Web>*options*) 48

Console (Administration>Network>Console>*options*) 50

SNMP 52

SNMPv1 (Administration>Network>SNMPv1>options) 52
SNMPv3 (Administration>Network>SNMPv3>options) 54

FTP Server (Administration>Network>FTP Server) 55

Administration: Notification and Logging 57

Event Actions (Administration>Notification>Event Actions>*options*) 57

Types of notification 57
Configuring event actions 58

Active, Automatic, Direct Notification 60

E-mail notification 60
SNMP traps 63
SNMP Trap Test (Administration>Notification>SNMP Traps>test) 64
Remote Monitoring 64
Syslog (Logs>Syslog>*options*) 67

Indirect Notification Through Logs or Queries 69

Event log (Logs>Events>*options*) 69
Data log (Logs>Data>*options*) 71
Using FTP or SCP to retrieve log files 73
Queries (SNMP GETs) 75

Administration: General Options 76

Identification (Administration>General>Identification) 76

Set the Date and Time 76

Method (Administration>General>Date & Time>mode) 76
Daylight saving (Administration>General>Date & Time>daylight saving) 77
Format (Administration>General>Date & Time>date format) 77

Use an .ini File (Administration>General>User Config File) 78

System Preferences (Administration>General>Preferences) 78

Color-coding events in the event log 78
Changing the default temperature scale 79

Reset the Interface (Administration>General>Reset/Reboot) 79

Configuring Links (Administration>General>Quick Links) 79

About the Rack ATS (Administration>General>About) 80

APC Device IP Configuration Wizard 81

Capabilities, Requirements, and Installation 81

Using the Wizard to configure TCP/IP settings 81
System requirements 81
Installation 81

Use the Wizard 82

Launch the Wizard 82
Configure the basic TCP/IP settings remotely 82
Configure or reconfigure the TCP/IP settings locally 83

Exporting Configuration Settings 84

Retrieving and Exporting the .ini File 84

Summary of the procedure 84
Contents of the .ini file 85
Detailed procedures 86

The Upload Event and Error Messages 89

The event and its error messages 89
Messages in config.ini 90
Errors generated by overridden values 90
Related Topics 90

File Transfers 91

Upgrading Firmware 91

Benefits of upgrading firmware 91
Firmware files (Automatic Transfer Switch) 91
Obtain the latest firmware version 92

Firmware File Transfer Methods 92

Use FTP or SCP to upgrade one Rack ATS 93
Upgrading multiple Rack ATSs 94
Use XMODEM to upgrade one Rack ATS 94

Verifying Upgrades 96

Verify the success or failure of the transfer 96
Last Transfer Result codes 96
Verify the version numbers of installed firmware 96

Product Information 97

Warranty and Service 97

Two-Year Factory Warranty 97

Terms of warranty 97
Non-transferable warranty 97
Exclusions 98
Warranty claims 99

Life-Support Policy 100

General policy 100
Examples of life-support devices 100

Index 101

Introduction

Product Description

Features of the Rack Automatic Transfer Switch

The American Power Conversion (APC®) Rack Automatic Transfer Switch (ATS) is a high-availability switch with two input power cords, one for each AC line, which enable the Rack ATS to provide redundant power.

You can manage a Rack ATS through its Web interface, its control console interface, the InfraStruXure® Manager and Central, or Simple Network Management Protocol (SNMP).

- Access the Web interface using Hypertext Transfer Protocol (HTTP), or using secure HTTP (HTTPS) with Secure Sockets Layer (SSL).
- Access the control console through a serial connection, Telnet, or Secure SHell (SSH).
- Use InfraStruXure Manager to monitor and manage your Rack ATS.
- Use an SNMP browser and the APC PowerNet® Management Information Base (MIB) to manage your Rack ATS.

Automatic Transfer Switches have these features:

- Configurable alarm thresholds that provide network and visual alarms to help you prevent overloaded circuits.
- LED indicators on the front panel of the unit indicate operation, such as preferred source, overload current, and web connectivity. These can also be monitored via serial and the Web interface.
- The ability to monitor sources and set preferred transfer parameters via web and console interfaces.
- Three levels of user access accounts: Administrator, Device User, and Read-Only User.

- Event and data logging—the event log is accessible by Telnet, Secure CoPy (SCP), File Transfer Protocol (FTP), serial connection, or Web browser (using HTTPS access with SSL, or using HTTP access). The data log is accessible by Web browser, SCP, and FTP.
- SNMP traps, Syslog messages, and e-mail notifications based on the severity level or category of the Rack ATS and system events.
- Security protocols for authentication and encryption.

The Rack ATS does not provide power surge protection. To ensure that the device is protected from power failure or power surges, connect the Rack ATS to an APC Uninterruptible Power Supply (UPS).

Initial setup

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

- IP address of the Rack ATS
- Subnet mask
- IP address of the default gateway

Do not use the loopback address (127.0.0.1) as the default gateway address. Doing so disables the Rack ATS. You must then log on using a serial connection and reset TCP/IP settings to their defaults.

To configure the TCP/IP settings, see the *Installation and Quick Start Manual* provided as a PDF file on the APC Automatic Transfer Switch *Utility* CD, and as a printed manual.

To use a DHCP server to configure the TCP/IP settings at a Rack ATS, see TCP/IP and Communication Settings.

Access Procedures

Overview

The Rack ATS has two internal interfaces (control console and Web interface) that allow you to manage the Rack ATS.

For more information about the internal user interfaces, see Control Console and Web Interface.

The SNMP interface also allows you to use an SNMP browser with the PowerNet Management Information Base (MIB) to manage the Rack ATS.

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

Access priority for logging on

Only one user at a time can log on to the Rack ATS. The priority for access, beginning with the highest priority, is as follows:

- Local access to the control console from a computer with a direct serial connection to the Rack ATS.
- Telnet or Secure SHell (SSH) access to the control console from a remote computer.
- Web access, either directly or through the InfraStruXure Manager.

See SNMP for information about how SNMP access to the Rack ATS is controlled.

Types of user accounts

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

- An Administrator can use all of the menus in the Web interface and control console. The default user name and password are both **apc**.
- A Device User can access only the following:
  - In the Web interface, the menus on the **Unit** tab and the event and data logs, accessible under the **Events** and **Data** headings on the left navigation menu of the **Logs** tab.
  - In the control console, the equivalent features and options. A Device User can also access the event log in the control console by pressing CTRL+L.

  The default user name is **device**, and the default password is **apc**.
- A Read-Only User has the following restricted access:
  - Access through the Web interface only.
  - Access to the same menus as a Device User, but without the capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but are disabled, and the event and data logs display no button to clear the log.

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

To set **User Name** and **Password** values for the three account types, see Setting user access (Administration>Security>Local Users>options).

You must use the Web interface to configure values for the Read-Only User.

Recovering from a Lost Password

You can use a local computer (a computer that connects to the Rack ATS or other device 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 serial cable (APC part number 940-0144A) to the selected port on the computer and to the configuration port at the Rack ATS.
3. Run a terminal program (such as HyperTerminal®) and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
   - The serial port is not in use by another application.
   - The terminal settings are correct as specified in step 3.
   - The correct cable is being used as specified in step 2.
5. Press the **Reset** button. The Status LED will flash alternately orange and green. Press the **Reset** button a second time immediately while the LED is flashing to reset the user name and password to their defaults temporarily.
6. Press ENTER 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**.
9. Press CTRL+C, log off, reconnect any serial cable you disconnected, and restart any service you disabled.
10. Select **Accept changes**.

Upgrading Firmware Through a Serial Connection

For a complete description of how to download a firmware upgrade for your Rack ATS, see Upgrading Firmware. That section also explains how to use network-based file transfer tools, which complete a firmware upgrade more quickly than the XMODEM protocol, which uses a serial connection.

You can use a local computer that connects to the Rack ATS through the serial port on the front panel of the unit.

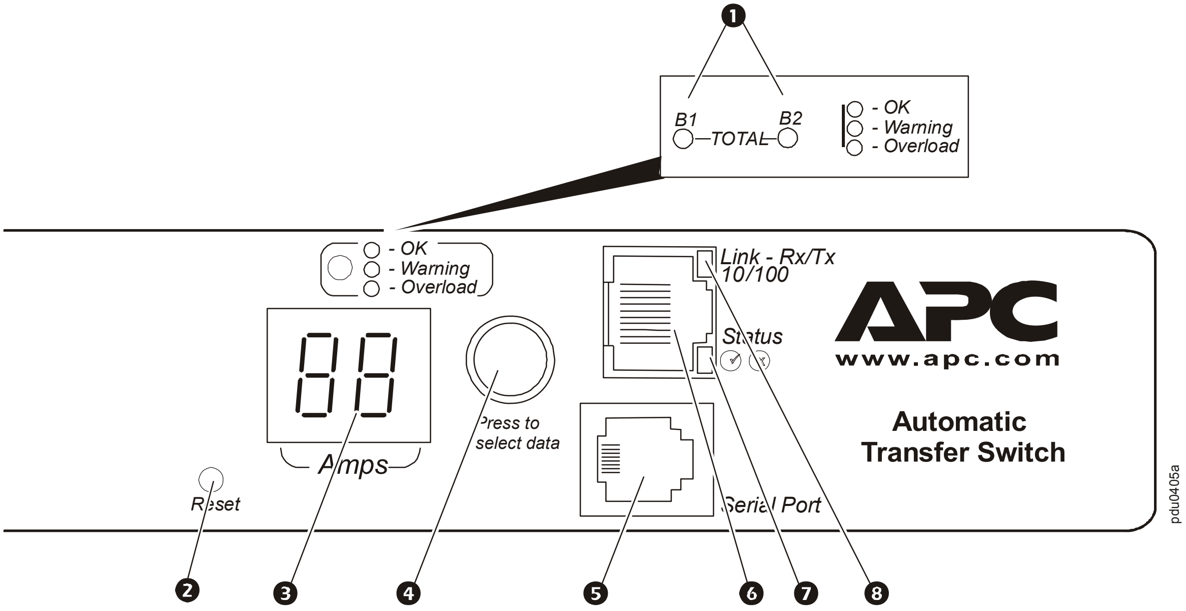
1. Obtain the individual firmware modules (the AOS module and the application module) from **www.apc.com/tools/download**.
2. Select a serial port at the local computer and disable any service that uses that port.
3. Connect the provided serial cable (APC part number 940-0144A) to the selected port and to the serial port at the Rack ATS.
4. Run a terminal program such as HyperTerminal, and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.
5. Press ENTER, repeatedly if necessary, 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**; type `Yes` at the prompt to continue.
8. Change the terminal program's baud rate to match your selection, and press ENTER. A higher baud rate causes faster upgrades.
9. From the terminal program's menu, select the binary AOS file to transfer using XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600. The Rack ATS 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.

⚠ Do not interrupt the download.

ⓘ Upgrading the firmware will not interfere with the operation of the outlets.

Front Panel



Item		Function
❶	Load Indicator LED	Identifies overload and warning conditions for the displayed bank. See Load indicator LED.
❷	Reset Button	Resets the Rack ATS Network Management Interface without affecting the outlet status.
❸	Digital Display	Displays the current (amps) for the bank indicated by the illuminated Load Indicator LED. If an internal communication failure occurs, the the text **Er** displays. Clear the alarm text by pressing the input selector. **Note:** If pressing the input selector does not clear the error message, a power supply failure may exist within the Rack ATS. Contact APC Worldwide Customer Support for technical support.

Item		Function
❹	Input Selector	Press and hold the input selector to display the IP address of the Rack ATS or to download the ATS controller firmware automatically. At five seconds, the IP address displays; at ten seconds, the ATS controller firmware will download automatically.
❺	RJ-12 Serial Port	Connects the Rack ATS to a terminal emulator program for local access to the control console. Use the supplied serial cable (APC part number 940-0144A).
❻	10/100 Base-T Connector	Connects the Rack ATS to the network.
❼	Status LED	See Status LED.
❽	Link-RX/TX LED	See Link-RX/TX (10/100) LED.

Link-RX/TX (10/100) LED

This LED indicates the network status.

Condition	Description
Off	The device that connects the Rack ATS to the network is off or not operating correctly.
Flashing Green	The Rack ATS is receiving data packets from the network at 10 Megabits per second (Mbps).
Flashing Orange	The Rack ATS is receiving data packets from the network at 100 Megabits per second (Mbps).
Solid Green or Orange	The Rack ATS is receiving no network traffic.

Status LED

This LED indicates the network status of the Rack ATS.

Condition	Description
Off	The Rack ATS is connected to an unknown network.
Solid Green	The Rack ATS has valid TCP/IP settings.
Flashing Green	The Rack ATS does not have valid TCP/IP settings.†
Solid Orange	A hardware failure has been detected in the Rack ATS. Contact APC Worldwide Customer Support.
Flashing Orange	The Rack ATS is making BOOTP requests.
Flashing Orange and Green (alternating)	The Rack ATS is making DHCP requests.

† If you do not use a BOOTP or DHCP server, see the *Installation and Quick Start Manual* provided as a PDF file on the APC Automatic Transfer Switch *Utility* CD, to configure the TCP/IP settings.

Load indicator LED

The load indicator LED identifies overload and warning conditions for the displayed bank.

Condition	Description
Solid Green	The current of the displayed bank is below the **Near Overload Warning** threshold.
Yellow	The displayed bank is in a **Near Overload Warnin**g condition. The current is above the **Near Overload Warning** threshold.
Red	The displayed bank is in an **Overload** condition. The current is above the **Overload Alarm** threshold.

Watchdog Features

Overview

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

Network interface watchdog mechanism

The Rack ATS implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the Rack ATS 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 itself.

Resetting the network timer

To ensure that the Rack ATS does not restart if the network is quiet for 9.5 minutes, the Rack ATS attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the Rack ATS, 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 restart the 9.5-minute timer frequently enough to prevent the Rack ATS 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 Manager, which is the same user account as Device User in the Web interface). A Read-Only User has no access to the control console.

If you cannot remember your user name or password, see Recovering from a Lost Password.

Remote access to the control console

You can access the control console through Telnet or Secure SHell (SSH). Telnet is enabled by default. Enabling SSH disables Telnet.

To enable or disable these access methods:

- In the Web interface, on the **Administration** tab, select **Network** on the top menu bar, and then the **access** option under **Console** on the left navigation menu.
- In the control console, use the **Telnet/SSH** option of the **Network** menu.

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

1. From a computer on the same network as the Rack ATS, at a command prompt, type **`telnet`** and the System IP address for the Rack ATS (for example `telnet 139.225.6.133`, when the Rack ATS uses the default Telnet port of 23), and press ENTER.
   If the Rack ATS uses a non-default port number (from 5000 to 32768), you must include a colon or a space, depending on your Telnet client, between the IP address (or DNS name) 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 Manager, which is the same user account as Device User in the Web interface).

SSH for high-security access. If you use the high security of SSL for the Web interface, use Secure SHell (SSH) for access to the control console. SSH encrypts user names, passwords, and transmitted data. The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.

Local access to the control console

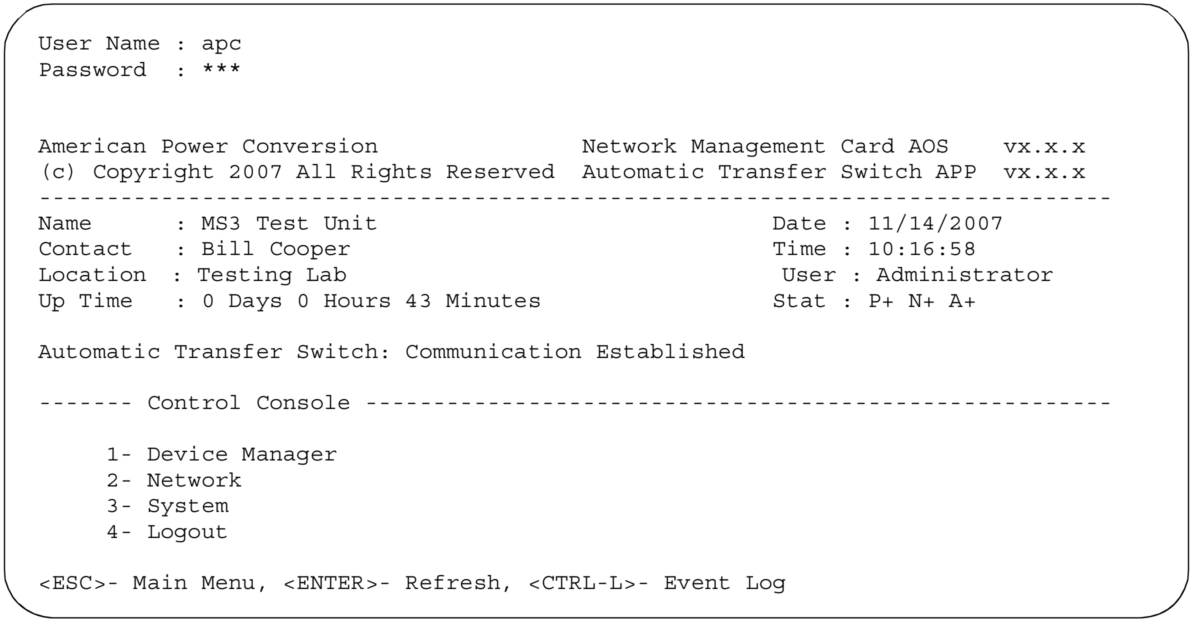
For local access, use a computer connected by serial cable to the Rack ATS through the serial port on the front panel of the unit:

1. Select a serial port at the local computer, and disable any service that uses that port.
2. Use the supplied serial cable (APC part number 940-0144A) to connect the selected port to the serial port on the front panel of the Rack ATS.
3. Run a terminal program (e.g., HyperTerminal), and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press ENTER, and at the prompts, enter your user name and password.

Main Screen

Example main screen

The following is an example of the main screen that displays when you log on to the control console of a Rack ATS:



```
User Name : apc
Password  : ***


American Power Conversion               Network Management Card AOS    vx.x.x
(c) Copyright 2007 All Rights Reserved  Automatic Transfer Switch APP  vx.x.x
-------------------------------------------------------------------------------
Name      : MS3 Test Unit                            Date : 11/14/2007
Contact   : Bill Cooper                              Time : 10:16:58
Location  : Testing Lab                               User : Administrator
Up Time   : 0 Days 0 Hours 43 Minutes                Stat : P+ N+ A+

Automatic Transfer Switch: Communication Established

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

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

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

Information and status fields

Main screen 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. In the preceding example, the application firmware for the Rack ATS is displayed.

```
Network Management Card AOS      vx.x.x
Automatic Transfer Switch APP    vx.x.x
```

- Three fields identify the system name, contact person, and location of the Rack ATS. (In the control console, use the **System** menu to set these values.)

```
Name          : MS3 Test Unit
Contact       : Bill Cooper
Location      : Testing Lab
```

- An **Up Time** field reports how long the Rack ATS has been running since it was last turned on or reset.

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

- Two fields identify when you logged in, by date and time.

```
Date : 11/14/2007
Time : 10:16:58
```

- A **User** field identifies whether you logged in through the **Administrator** or **Device Manager** user account. (The **Read-Only User** account cannot access the control console.)

```
User : Administrator
```

Main screen status fields.

- A **Stat** field reports the Rack ATS status.

```
Stat : P+ N+ A+
```

P+	The APC operating system (AOS) is functioning properly.
N+	The network is functioning properly.
N?	A BOOTP request cycle is in progress.
N–	The Rack ATS failed to connect to the network.
N!	Another device is using the Rack ATS IP address.
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.

! If P+ is not displayed, contact APC support staff. See APC Worldwide Customer Support.

- The field that indentifies the Rack ATS name also reports the operating status of the Rack ATS.

```
Automatic Transfer Switch: Communication Established
```

- An alarm counter displays the current alarm conditions and the status in the same line as the text “-----Control Console-----”.

Control Console Menus

How to use control console menus

The menus in the control console list options by number and name. To use an option, type the option's number, press ENTER, and follow any on-screen instructions. If you use an option that changes a setting or value, select **Accept Changes** to save your change before you exit the menu.

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

- Type ? and press ENTER for menu option descriptions if help exists for the menu.
- Press ENTER to refresh the menu.
- Press ESC to go back to the menu from which you accessed the current menu.
- Press CTRL+C to return to the main (**Control Console**) menu.
- Press CTRL+D to toggle through the Device Manager menus.
- Press CTRL+L to access the event log.

For information about the event log, see Indirect Notification Through Logs or Queries.

Main Menu

Use the main **Control Console** menu to access the control console's management features:

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

When you log on as Device Manager (equivalent to Device User in the Web interface), you can access only the **Device Manager** menus and the **Logout** menu.

Device Manager option

Use the options of the Device Manager menu to manage Rack ATS settings.For information about performing the following tasks, see Unit Tab:

- Configure the load thresholds for each bank.
- Configure and control the outlets.
- View the status of the power supply.

Menu option	Description
`1-Alarms List`	View the list of current alarms.
`2-ATS Status`	View current status of the Rack ATS.
`3-ATS Configuration`	Set the Rack ATS name, preferred power source, sensitivity, VRMS range, front panel operation, frequency deviation, line VRMS and narrow, medium, and wide VRMS limits.
`4-ATS Control`	Reset the Rack ATS or download ATS controller firmware using a serial connection.
`5-Load Management`	View and set the overload, near-overload, and low-load warning thresholds.
`6-Measurements`	Display all of the Rack ATS measurements.
`7-Event Counts`	Displays Redundancy Loss, Source Switch, Over Current, Source Preference Change, Spike/Dropout, Surge/Droop, and Frequency Loss event counts.
`8-About ATS`	Displays information about the ATS.

Network option

To perform the following tasks, see Administration: Network Features:

- Configure the TCP/IP settings for the Rack ATS or, when the Rack ATS will obtain its TCP/IP settings from a server, configure the settings for the type of server (DHCP or BOOTP) to be used.
- Use the Ping utility.
- Define settings that affect the FTP, Telnet, Web interface and SSL, SNMP, e-mail,

DNS, and Syslog features of the Rack ATS.

System option

To perform these tasks, see Administration: General Options:

- Control **Administrator** and **Device Manager** access. (You can control **Read-Only User** access by using the Web interface only.)
- Define the **Name**, **Contact**, and **Location** values for the system.
- Set the date and time used by the Rack ATS.
- Through the **Tools** option:
  - Restart the Rack ATS.
  - Reset parameters to their default values.
  - Delete SSH host keys and SSL certificates.
  - Upload an initialization file (.ini file) that has been downloaded from another Rack ATS. The current Rack ATS then uses the values in that .ini file to configure its own settings.
- Access and configure RADIUS information.
- Access system information about the Rack ATS.

Web Interface

Introduction

Supported Web browsers

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

Data verification, the event log, and the data log require that you enable the following for your Web browser:

- Java
- Cookies

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

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

How to Log On

Overview

You can use the DNS name or System IP address of the Rack ATS for the URL address of the Web interface. Use your case-sensitive user name and password to log on. The default user name differs by account type:

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

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

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 Rack ATS. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.

See Web (Administration>Network>Web>options) to select, enable, and disable the protocols that control access to the Web interface and to define the Web-server ports for the protocols.

For information about the Web page that appears when you log on to the Web interface, see Home Page.

URL address formats

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

Common browser error messages at log-on.

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

URL format examples.

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

– `http://139.225.6.133:5000` if HTTP is your access mode.

– `https://139.225.6.133:5000` if HTTPS is your access mode.

How to Use the Tabs, Menus, and Links

Tabs

In addition to the tab for the **Home** page, the following tabs are displayed. Click a tab to display a set of menu options:

- **Unit**: Display Rack ATS status, issue Rack ATS control commands, configure Rack ATS parameters, run diagnostic tests, configure and schedule shutdowns, and view information about the Rack ATS.
- **Logs**: View and configure event and data logs.
- **Administration**: Configure security, network connection, notification, and general settings.

Menus

Left navigation menu. Each tab (except the tab for the home page) has a left navigation menu, consisting of headings and options:

- If a heading has indented option names below it, the heading itself is not a navigational link. Click an option to display or configure parameters.
- If a heading has no indented option names, the heading itself is the navigational link. Click the heading to display or configure parameters.

Top menu bar. The **Home** and **Administration** tabs have a selection of menu options on the top menu bar. The **Security** option is selected by default when you click the **Administration** tab and the **Overview** option is selected when you click the **Home** tab.

Clicking an option on the top menu bar displays the left navigation menu for that option, with the first menu item selected by default.

Quick Links

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

- **Link 1**: The home page of the APC Web site.
- **Link 2**: Demonstrations of APC Web-enabled products.
- **Link 3:** Information on APC Remote Monitoring Services.

To reconfigure the links, see Configuring Links (Administration>General>Quick Links).

Home Page

Overview

On the **Home** page of the interface, displayed when you log on, you can view active alarm conditions and the most recent events recorded in the event log.

Quick status icons

At the upper right corner of the **Home** page, one or more icons and accompanying text indicate the current operating status of the Rack ATS:

✖	**Critical**: A critical alarm exists, which requires immediate action.
⚠	**Warning**: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
✓	**No Alarms**: No alarms are present, and the Rack ATS is operating normally.
A● ➡ ● B● ➡ A● ✗ ● B●	**Rack ATS status icon**: Displays the status of the connected Rack ATS**.** If Source A or Source B LED is green, source is active and connected to the power supply. If there are any internal power supply failures then a red “X” will be displayed. Move the mouse pointer over the icon to display the status of the active source displayed, or click on the icon to view the **ATS Status** on the **Unit** page.

At the upper right corner of every page, the Web interface displays the same icons currently displayed on the **Home** page to report Rack ATS status:

- The **No Alarms** icon if no alarms exist.
- One or both of the other icons (**Critical** and **Warning)** if any alarms exist, and after each icon, the number of active alarms of that severity.
- The Rack ATS status icon.

To return to the **Home** page to view its summary of the Rack ATS status, including the active alarms, click a quick status icon on any page of the interface.

Active Alarms

The **Active Alarms** section displays any alarms present. If no alarms are present, “No Alarms Present” will be displayed. If an alarm is present, the alarm and its description will be displayed. Click the displayed alarm to view the **Device Alarm Status** page which includes a description and severity level for each alarm present. Alternately, access the **Device Alarm Status** page by selecting the **Home** tab, then the top menu bar option **Alarm Status**.

Device Status

The **Device Status** section displays a graphic depicting the current load status of the Rack ATS. The colors green, yellow, and red signify the **Load Thresholds** set by the user. The graphic is accompanied by the measurement of the load in Amps, and a link to the **Load** page in the **Unit** tab.

ATS Parameters

The **ATS Parameters** section displays the model number, device name, contact information, device location, current rating, type of user account accessing the Rack ATS, and the amount of time the Rack ATS has been operating.

Recent Device Events

On the **Home** page, **Recent Device Events** displays, in reverse chronological order, the events that occurred most recently and the dates and times they occurred. Click **More Events** to view the entire event log.

Additional information on Home page

The IP address displays in the upper left corner.

A context-sensitive **Help** link and **Log off** link are displayed in the upper right corner of the **Home** page.

Selecting a menu to perform a task

- To do the following, see Administration: Notification and Logging:
  - Access the event log.
  - Configure the actions to be taken based on the severity level of an event.
  - Configure **SNMP Trap Receiver** settings for sending event-based traps.
  - Define who receives e-mail notification and Syslog messages for events.
  - Test e-mail settings.
- To do the following, see Data log (Logs>Data>options):
  - Access the data log.
  - Define the log interval (how often data will be sampled and recorded) for the data log.

- To do the following, see Administration: Network Features:
  - Configure new TCP/IP settings for the Rack ATS.
  - Identify the Domain Name System (DNS) Server, test its network connection, and enable or disable DNS Reverse Lookup Event Logging (which logs the domain name of the device associated with each event).
  - Define settings for FTP, Telnet, SSH, the Web interface, HTTP and HTTPS, SNMP, and e-mail.
  - Configure the Rack ATS's Syslog message feature.
- To do the following, see Administration: General Options:
  - Control **Administrator**, **Device User**, and **Read-Only User** access.
  - Define the system **Name**, **Contact**, and **Location** values.
  - Set the **Date** and **Time** used by the Rack ATS.
  - Restart the Rack ATS.
  - Reset control console settings to default settings.
  - Select **Farenheit** or **Celsius** for temperature displays.
  - Enable color-coding of alarm text in the event log.
  - Define the URL addresses of the user links and APC logo links in the Web interface.

Unit Menus

Unit Tab

Select the **Unit** tab to review status, control, and configuration settings for the Rack ATS.

Status

The left navigation menu option provides the overall status of the device.

Parameter	**Description**
Selected Source	Source currently supplying power to the load.
Preferred Source	Power source that will supply power to the Rack ATS when both input power sources are acceptable.
Switch Status	Indicates whether the alternative power source is acceptable or not (OK or FAIL).
Front Panel	Indicates if the front panel button can be used to change preferred source (Locked or Unlocked).
Source A and Source B	The overall state of each power source. **Selected**–The preferred source is supplying power to the device. **OK**–The alternate power source is acceptable and the Rack ATS will transfer to this source if the selected power source fails. **Not Ok**–The power source is not acceptable and the Rack ATS cannot transfer to this source if the preferred source fails.
Phase Sync	Inidicates whether Source A and B are in phase. The preference indicator on the front panel will flash if sources are not in phase (In sync or Out of sync).
Voltage Out	Shows whether the line voltage is present to the outlets of the ATS (ON or OFF).

Parameter	Description
Source A 24 V, Source B 24 V, +12 V,- 12 V, 5 V Power Supplies	Reports the condition of the internal power supplies (OK or FAIL).

Measurements

The left navigation menu option **Measurements** provides the various measurements of the device.

Parameter	Description
Input Frequency	Input frequency for each power supply, measured in Hertz.
Input Voltage	Input voltage for each bank of each power supply, measured in Vac. The voltage orientation is Line-to-Neutral (L/N).
Total Power	Total power drawn from the connected load to the device, measured in Watts.
Power Supplies	Values of the internal power supplies, measured in Vdc.

Configuration

source. Select **Source**, under the left navigation menu option **Configuration**, to configure source parameters.

Setting	Description
Source A Name	The user-defined name for source A. Maximum 32-characters.
Source B Name	The user-defined name for source B. Maximum 32-characters.
Preferred Source	The power source used when both input power sources are acceptable. Options are Source A, Source B, and None.
Front Panel	Lock or unlock the preferred source button on the front panel of the device.

frequency/voltage. Select **frequency/voltage**, under the left navigation menu option **Configuration**, to configure voltage and Frequency parameters.

Setting	Description
Line Frequency	Nominal source frequency for the device.
Frequency Deviation	Define the range of acceptable frequency fluctuation. If the frequency measured from the selected input source is not within this range, the Rack ATS will transfer to the alternate power source. Options are 1, 2, and 3.
Voltage Transfer Range	Define the range of acceptable voltage from a power source. If the voltage measured from the selected input source is not within this range, the Rack ATS will transfer to the alternate power source. Options are Wide, Medium, and Narrow.
Sensitivity	Define the sensitivity to changes in voltage. **High**–Cause the Rack ATS to switch to the alternate power source in response to small line voltage changes. Select this setting for the best protection for sensitive equipment. **Low**–Cause the Rack ATS to accept frequent small line voltage changes without switching to the alternate power source.
Line VRMS	Nominal source line voltage setting for the device.
Wide VRMS Limit	The voltage range to use when Voltage Transfer Range is set to Wide. This value must be greater than the Medium VRMS Limit.
Medium VRMS Limit	The voltage range to use when Voltage Transfer Range is set to Medium. This value must be greater than the Narrow VRMS Limit and less than the Wide VRMS Limit.
Narrow VRMS Limit	The voltage range to use when Voltage Transfer Range is set to Narrow. This value must be less than the Medium VRMS Limit.

Load. Select **load**, under the left navigation menu option **Configuration**, to view the Rack ATS's load status and to configure the load thresholds for the banks or phases of the Rack ATS.

The load of the Rack ATS is displayed as a graph. The graph is accompanied by the measurement of the load in Amps. Alarms associated with the load are displayed next to the graph.

Set the following alarms through the **Load** menu: **Overload Alarm**, **Near Overload Warning**, and **Low Load Warning**.

Type the threshold value in Amps and click **Apply** to save your changes or **Cancel** to exit without saving the changes.

To set the Low Load Warning Threshold, see Setting the Low Load Warning Threshold.

Control

Provides control options for the Rack ATS.

By default, the option **No action** is selected. Select **Reset ATS Controller** to restart the ATS Controller and restore the factory default settings for the controller. This command will not reset any user configurations or settings.

Note: The device will lose communication briefly when the ATS controller is reset.

Event Counts

Event Counts. View the number of occurrences of selected events.

Clearing of Event Counts. Clear all the event counts. The counting will start from 0.

About ATS

Provides the following ATS hardware information: Firmware Revision, Firmware Date, Hardware Revision, Manufacture Date, Model Number, and Serial Number.

Automatic Transfer Switch Settings

Configuring load thresholds

Web interface.

1. Select the **Unit** tab from the navigation menu. Then select **load**, under **Configuration** in the left navigation menu.
2. Set the thresholds for total current or each bank. The configurable thresholds are **Overload Alarm Threshold**, **Near Overload Warning Threshold**, and **Low Load Warning Threshold** for each bank.
3. Click **Apply** to save your changes or **Cancel** to exit without saving the changes.

Control console.

1. From the **Device Manager** menu, select **Load Management**.
2. Select a threshold to configure–**Overload Alarm Threshold (amps)**, **Near Overload Warning Threshold (amps)**, or **Low Load Warning Threshold (amps)**.
3. Select **Accept Changes**.

Setting	Description
Overload Alarm Threshold	Set the overload threshold, in amps, for the current drawn from this bank during normal operation. A load at or higher than this level generates a warning.
Near Overload Warning Threshold	Set the number of amps at which to generate an alarm that the Rack ATS is nearing overload of a bank.
Low Load Warning Threshold	Set the low threshold, in amps, for the current drawn from this bank during normal operation. A load at or below this level generates a warning.

Setting the Low Load Warning Threshold

- By default, the **Low Load Warning Threshold** is 0 Amps, which disables the warning alarm. A 2-Amp detection threshold indicates that a circuit breaker may have tripped and activates a warning alarm.
- With a setting of 0 Amps for the **Low Load Warning Threshold**, the Web interface will not indicate that a circuit breaker may have tripped.

Setting the Low Load Warning Threshold (Web interface).

1. Select the **Unit** tab from the navigation menu, then select **load**, under **Configuration** in the left navigation menu.
2. Set the **Low Load Warning Threshold** for each bank to **2 Amps.**
3. Click **Apply** to save your changes or **Cancel** to exit without saving the changes.

Administration: Security

Local Users

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

You set the case-sensitive user name and password for each account type in the same manner. Maximum length of each is 32 characters. Blank passwords (passwords with no characters) are not allowed.

For information on the permissions granted to each account type (Administrator, Device User, and Read-Only User), see Types of user accounts.

Account Type	Default User Name	Default Password	Permitted Access
Administrator	apc	apc	Web Interface and Control Console
Device User	device	apc	
Read-Only User	readonly	apc	Web Interface only

Remote Users

Authentication (Administration>Security>Remote Users>authentication)

Use this option to select how to administer remote access to the Rack ATS.

For information about local authentication (not using the centralized authentication of a RADIUS server), see the *Security Handbook,* available on the APC Automatic Transfer Switch *Utility* CD and on the APC Web site at **www.apc.com**.

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

- When a user accesses the Automatic Transfer Switch or other network-enabled device that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user's permission level.
- RADIUS user names used with the Automatic Transfer Switch 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 and local authentication are enabled. If local authentication is used, authentication is requested from the RADIUS server first.
- **RADIUS Only**: RADIUS is enabled. Local authentication is disabled.

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

RADIUS (Administration>Security>Remote Users>RADIUS)

Use this option to do the following:

- List the RADIUS servers (a maximum of two) available to the Automatic Transfer Switch, and the time-out period for each.
- Click **Add Server**, and configure the parameters for authentication by a new RADIUS server.

- Click a listed RADIUS server to display and modify its parameters.

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

Configuring the RADIUS Server

Summary of the configuration procedure

You must configure your RADIUS server to work with the Rack ATS.

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

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

Configuring a RADIUS server on UNIX® with shadow passwords

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

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

```
DEFAULT      Auth-Type = System
             APC-Service-Type = Admin
```

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

```
bconners      Auth-Type = System
              APC-Service-Type = Admin
thawk         Auth-Type = System
              APC-Service-Type = Device
```

Supported RADIUS servers

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

Inactivity Timeout (Administration>Security>Auto Log Off)

Use this option to configure the time (3 minutes by default) that the system waits before logging off an inactive user. If you change this value, you must log off for the change to take effect.

! This timer continues to run if a user closes the browser window without first logging off by clicking **Log Off** at the upper right. Because that user is still considered to be logged on, no user of that account type can log on until the time specified as **Minutes of Inactivity** expires. For example, with the default value for **Minutes of Inactivity**, if a Device User closes the browser window without logging off, no Device User can log on for 3 minutes.

TCP/IP and Communication Settings

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

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

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

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

Setting	Description
Manual	The IP address, subnet mask, and default gateway must be configured manually. Click **Next>>**, and enter the new values.
BOOTP	A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Rack ATS requests network assignment from any BOOTP server: • If it receives a valid response, it starts the network services. • If it finds a BOOTP server, but a request to that server fails or times out, the Rack ATS stops requesting network settings until it is restarted. • By default, if previously configured network settings exist, and the Rack ATS receives no valid response to five requests (the original and four retries), the Rack ATS uses the previously configured settings so that it remains accessible. Click **Next>>** to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail [1]: • **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries. • **If retries fail**: Select **Use prior settings** (the default) or **Stop BOOTP request**.
DHCP	At 32-second intervals, the Rack ATS requests network assignment from any DHCP server. By default, the number of retries is unlimited. • If the Rack ATS receives a valid response, by default it requires the APC cookie from the DHCP server in order to accept the lease and start the network services. • If the Rack ATS finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted. To change these values, click **Next>>** for the **DHCP Configuration** page[1]: • **Require vendor specific cookie to accept DHCP Address**: Disable or enable the requirement that the DHCP server provide the APC cookie. • **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.

[1] The default values for these three settings on the configuration pages generally do not need to be changed:
•**Vendor Class**: APC
•**Client ID**: The MAC address of the Automatic Transfer Switch, which uniquely identifies it on the local area network (LAN)
•**User Class**: The name of the application firmware module

Setting	Description
DHCP & BOOTP	The default setting. The Automatic Transfer Switch 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 the Rack ATS obtains its TCP/IP settings from either server, it switches this setting to **BOOTP** or **DHCP**, depending on the type of server that supplied the TCP/IP settings to the Automatic Transfer Switch. Click **Next>>** to configure the same settings that are on the **BOOTP Configuration** and **DHCP Configuration** pages[1] and to specify that the **DHCP and BOOTP** setting be retained after either type of server provides the TCP/IP values.

[1] The default values for these three settings on the configuration pages generally do not need to be changed:
- **Vendor Class**: APC
- **Client ID**: The MAC address of the Automatic Transfer Switch, which uniquely identifies it on the local area network (LAN)
- **User Class**: The name of the application firmware module

DHCP response options

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

Vendor Specific Information (option 43). The Rack ATS 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 Rack ATS that a DHCP server is configured to service APC devices. By default, this DHCP response option must contain the APC cookie for the Rack ATS to accept the lease.

To disable the requirement of an APC cookie, see DHCP.

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

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

- **Boot Mode Transition. Tag 2, Len 1, Data 1/2**
  This option 43 setting enables or disables the option **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**, which, by default, is disabled.
  – A data value of 1 enables the option **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**. Whenever the Rack ATS reboots, it will request its network assignment first from a BOOTP server, and then, if necessary, from a DHCP server.
  – A data value of 2 disables the option **Remain in DHCP & BOOTP mode after accepting TCP/IP settings**. The **TCP/IP Configuration** setting option switches to **DHCP** when the Rack ATS accepts the DHCP response. Whenever the Rack ATS 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 disabled Boot Mode Transition setting:

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

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

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

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

Port Speed (Administration>Network>Port Speed)

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

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

DNS (Administration>Network>DNS>*options*)

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

Servers. Select **servers** to specify the IP addresses of the primary and optional secondary DNS server. For the Rack ATS to send e-mail, at least the IP address of the primary DNS server must be defined.

The Automatic Transfer Switch waits up to 15 seconds for a response from the primary DNS server or the secondary DNS server (if a secondary DNS server is specified). If the Rack ATS does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the Rack ATS or on a nearby segment (but not across a wide-area network [WAN]).

To verify that DNS is working correctly after you define the IP addresses of the DNS servers, see Test.

Naming. Select **naming** to define the host name and domain name of the Rack ATS:

- **Host Name**: After you configure a host name here and a domain name in the **Domain Name** field, users can enter a host name in any field in the Rack ATS interface (except e-mail addresses) that accepts a domain name.
- **Domain Name**: You need to configure the domain name here only. In all other fields in the Automatic Transfer Switch interface (except e-mail addresses) that accept domain names, the Automatic Transfer Switch adds this domain name when only a host name is entered.
  - To override all instances of the expansion of a specified host name by the addition of the domain name, set the domain name field to its default, `somedomain.com`, or to `0.0.0.0`.
  - To override the expansion of a specific host name entry (for example, when defining a trap receiver), include a trailing period. The Rack ATS 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.

Test. Select **test** to send a DNS query that tests the setup of your DNS servers:

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

Query Type Selected	Query Question to Use
by Host	The URL
by FQDN	The fully qualified domain name, *my_server.my_domain.com*.
by IP	The IP address
by MX	The Mail Exchange address

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

Web (Administration>Network>Web>*options*)

Option	Description

access	To activate changes to any of these selections, log off from the Rack ATS:
	• **Disable**: Disables access to the Web interface. (You must use the control console to re-enable access. Select **Network** and **Web/SSL/TLS**. Then for HTTP, select **Access** and **Enabled**. For HTTPS access, also select **SSL/TLS** and **Enabled**.)
	• **Enable HTTP** (the default): Enables Hypertext Transfer Protocol (HTTP), which provides Web access by user name and password, but does not encrypt user names, passwords, and data during transmission.
	• **Enable HTTPS**: Enables Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer (SSL). SSL encrypts user names, passwords, and data during transmission, and authenticates the Rack ATS by digital certificate. When HTTPS is enabled, your browser displays a small lock icon.
	See “Creating and Installing Digital Certificates” in the *Security Handbook* on the APC Automatic Transfer Switch *Utility* CD to choose among the several methods for using digital certificates.
	HTTP Port: The TCP/IP port (80 by default) used to communicate by HTTP with the Rack ATS.
	HTTPS Port: The TCP/IP port (443 by default) used to communicate by HTTPS with the Rack ATS.
	For either of these ports, you can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) in the address field of the browser to specify the port number. For example, for a port number of 5000 and an IP address of 152.214.12.114:
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`

ssl cipher suites	Enable or disable any of the SSL encryption ciphers and hash algorithms: • **DES**: A block cipher that provides authentication by Secure Hash Algorithm. • **RC4_MD5** (enabled by default): A stream cipher that provides authentication by MD5 hash algorithm. • **RC4_SHA** (enabled by default): A stream cipher that provides authentication by Secure Hash Algorithm. • **3DES**: A block cipher that provides authentication by Secure Hash Algorithm.

Option	Description
ssl certificate	Add, replace, or remove a security certificate. **Status**: • **Not installed**: A certificate is not installed, or was installed by FTP or SCP to an incorrect location. Using **Add or Replace Certificate File** installs the certificate to the correct location, **/sec** on the Automatic Transfer Switch. • **Generating**: The Automatic Transfer Switch is generating a certificate because no valid certificate was found. • **Loading**: A certificate is being activated on the Rack ATS. • **Valid certificate**: A valid certificate was installed or was generated by the Rack ATS. Click on this link to view the certificate's contents. **If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the Rack ATS generates a default certificate, a process which delays access to the interface for up to five minutes.** You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on. **Add or Replace Certificate File**: Enter or browse to the certificate file created with the Security Wizard. See "Creating and Installing Digital Certificates" in the *Security Handbook* on the APC Automatic Transfer Switch *Utility* CD to choose a method for using digital certificates created by the Security Wizard or generated by the Rack ATS. **Remove**: Delete the current certificate.

Console (Administration>Network>Console>*options*)

Option	Description
access	Choose one of the following for access by Telnet or SSH: • **Disable**: Disables all access to the control console. • **Enable Telnet** (the default): Telnet transmits user names, passwords, and data without encryption. • **Enable SSH v1 and v2**: Do not enable both versions 1 and 2 of SSH unless you require both. They use extensive processing power. • **Enable SSH v1 only**: SSH version 1 encrypts user names, passwords, and data for transmission. There is little or no delay as you log on. • **Enable SSH v2 only**: SSH version 2 transmits user names, passwords, and data in encrypted form with more protection than version 1 from attempts to intercept, forge, or alter data during transmission. There is a noticeable delay as you log on. Configure the ports to be used by these protocols: • **Telnet Port**: The Telnet port used to communicate with the Rack ATS (23 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. Users must then use a colon (:) or a space, as required by your Telnet client program, to specify the non-default port. For example, for port 5000 and an IP address of 152.214.12.114, your Telnet client requires one of the these commands: `telnet 152.214.12.114:5000` `telnet 152.214.12.114:5000` • **SSH Port**: The SSH port used to communicate with the Rack ATS (22 by default). You can change the port setting to any unused port from 5000 to 32768 for additional security. See the documentation for your SSH client for the command line format required to specify a non-default port.
ssh encryption	Enable or disable encryption algorithms (block ciphers) compatible with SSH version 1 or version 2 clients: If your SSH v1 client cannot use **Blowfish**, you must also enable **DES**. Your SSH v2 client selects the enabled algorithm that provides the highest security. If the client cannot use the default algorithms (**3DES** or **Blowfish**), enable an AES algorithm that it can use (**AES 128** or **AES 256**).

Option	Description
ssh host key	**Status** indicates the status of the host key (private key): • **SSH Disabled: No host key in use:** When disabled, SSH cannot use a host key. • **Generating**: The Rack ATS is creating a host key because no valid host key was found. • **Loading**: A host key is being activated on the Rack ATS. • **Valid**: One of the following valid host keys is in the **/sec** directory (the required location on the Automatic Transfer Switch): •A 1024-bit host key created by the APC Security Wizard. •A 768-bit RSA host key generated by the Automatic Transfer Switch. **Add or Replace**: Browse to and upload a host key file created by the Security Wizard: If you use FTP or SCP instead to transfer the host key file, you must specify the **/sec** directory as the target location in the command. To use the APC Security Wizard, see the *Security Handbook* on the APC Automatic Transfer Switch *Utility* CD. **NOTE:** To reduce the time required to enable SSH, create and upload a host key in advance. **If you enable SSH with no host key loaded, the Rack ATS takes up to 5 minutes to create a host key, and the SSH server is not accessible during that time.** **Remove**: Remove the current host key.

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

SNMP

SNMPv1 (Administration>Network>SNMPv1>*options*)

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

When using InfraStruXure Manager to manage the Automatic Transfer Switch on the public network of an InfraStruXure system, you must have SNMP enabled in the Rack ATS interface. Read access will allow InfraStruXure Manager to receive traps from an Automatic Transfer Switch, but Write access is required while you use the interface of the Rack ATS to set 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 Automatic Transfer Switch *Utility* CD or from the APC Web site, **www.apc.com**.

Option	Description
access	**Enable SNMPv1 Access:** Enables SNMP version 1 as a method of communication with this device.

Option	Description
access control	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. • 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. • 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. **Community Name:** The name that an 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." **NMS IP/Host Name:** 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: • 149.225.12.255: Access only by an NMS on the 149.225.12 segment. • 149.225.255.255: Access only by an NMS on the 149.225 segment. • 149.255.255.255: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment. **Access Type**: The actions an NMS can perform through the community. • **Read**: GETS only, at any time • **Write**: GETS at any time, and SETS when no user is logged onto the Web interface or control console. • **Write+**: GETS and SETS at any time. • **Disabled**: No GETS or SETS at any time.

SNMPv3 (Administration>Network>SNMPv3>*options*)

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.

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

The Automatic Transfer Switch supports only MD5 authentication and DES encryption.

Option	Description
access	**SNMPv3 Access:** Enables SNMPv3 as a method of communication with this device.
user profiles	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. **User Name:** The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters. **Authentication Passphrase:** A phrase of 15 to 32 ASCII characters 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. **Privacy Passphrase:** 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. **Authentication Protocol**: The APC implementation of SNMPv3 supports MD5 authentication. Authentication will not occur unless MD5 is selected here. **Privacy Protocol:** 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. **Note:** You cannot select the privacy protocol if no authentication protocol is selected.

Option	Description
access control	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. • If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device. • 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. To edit the access control settings for a user profile, click its user name. **Access:** Mark the **Enable checkbox** to activate the access control specified by the parameters in this access control entry. **User Name:** 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 **user profiles** option on the left navigation menu. **NMS IP/Host Name:** The IP address, IP address mask, or host name that controls access by the NMS. A host name or a specific IP address (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: • 149.225.12.255: Access only by an NMS on the 149.225.12 segment. • 149.225.255.255: Access only by an NMS on the 149.225 segment. • 149.255.255.255: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.

FTP Server (Administration>Network>FTP Server)

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

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

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

At any time that you want an Automatic Transfer Switch to be accessible for management by InfraStruXure Manager and Central, FTP Server must be enabled.

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

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

Types of notification

You can configure event actions to occur in response to an event or 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
  - SNMPv1 and SNMPv3 traps
  - Syslog notification
- Indirect notification in the event log. If no direct notification is configured, users must check the log to determine which events have occurred.

For another method of indirect notification, see SNMP for SNMPv1 and SNMPv3 setup and configuration. SNMPv1 enables an NMS to perform informational queries. Configuring the most restrictive SNMP access type, READ, enables informational queries without the risk of allowing remote configuration changes. SNMPv3 uses a system of user profiles to communicate with a MIB software program to perform GETs, SETs, and receive traps.

You can also log system performance data to use for device monitoring. See Data log (Logs>Data>options) for information on how to configure and use this data logging option.

Configuring event actions

Notification Parameters. For events that have an associated clearing event, you can also set the following parameters as you configure events individually or by group, as described in the next two sections. To access the parameters, click the receiver or recipient name.

Parameter	Description
Delay x time before sending	If the event persists for the specified time, notification is sent. If the condition clears before the time expires, no notification is sent.
Repeat at an interval of *x* time	The notification is sent at the specified interval (e.g., every 2 minutes).
Up to *x* times	During an active event, the notification repeats for this number of times.
Until condition clears	The notification is sent repeatedly until the condition clears or is resolved.

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. In the list of events, review the marked columns to see whether the action you want is already configured. (By default, logging is configured for all events.)
3. To view or change the current configuration, such as recipients to be notified by e-mail or paging, or Network Management Systems (NMSs) to be notified by SNMP traps, click on the event name.

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

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

- Identifying Syslog Servers (Logs>Syslog>servers)
- E-mail recipients (Administration>Notification>E-mail>recipients)
- Indirect Notification Through Logs or Queries
- Trap Receivers (Administration>Notification>SNMP Traps>trap receivers)

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

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by group** under **Event Actions** on the left navigation menu.
2. Choose how to group events for configuration:
   - Choose **Grouped by severity**, and then select all events of one or more severity levels. You cannot change the severity of an event.
   - Choose **Grouped by category**, and then select all events in one or more pre-defined categories.
3. Click **Next>>** to move from page to page to do the following:

   a. Select event actions for the group of events.

      - To choose any action except **Logging** (the default), you must first have at least one relevant recipient or receiver configured.
      - If you choose **Logging** and have configured a Syslog server, select **Event Log** or **Syslog** (or both) on the next page.

   b. Select whether to leave the newly configured event action enabled for this group of events.

Active, Automatic, Direct Notification

E-mail notification

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

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

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

  See DNS (Administration>Network>DNS>options).

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

  See SMTP (Administration>Notification>E-mail>server).

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

  See E-mail recipients (Administration>Notification>E-mail>recipients).

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).

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

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

Setting	Description
To Address	The user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient's pager gateway account (for example, `myacct100@skytel.com`). The pager gateway will generate the page. To bypass the DNS lookup of the mail server's IP address, use the IP address in brackets instead of the e-mail domain name, e.g., use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly. **NOTE:** The recipient's pager must be able to use text-based messaging.
SMTP Server	Select one of the following methods for routing e-mail: • **Local**: Through the Rack ATS's SMTP server. This setting (recommended) ensures that the e-mail is sent before the Rack ATS's 20-second time-out, and, if necessary, is retried several times. Also do one of the following: • Enable forwarding at the Rack ATS's SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Check with the administrator of your SMTP server before changing its configuration to allow forwarding. • Set up a special e-mail account for the Rack ATS to forward e-mail to an external mail account. • **Recipient**: Directly to the recipient's SMTP server. With this setting, the Rack ATS tries to send the e-mail only once. On a busy remote SMTP server, the time-out may prevent some e-mail from being sent. When the recipient uses the Rack ATS's SMTP server, this setting has no effect.
E-mail Generation	Enables (by default) or disables sending e-mail to the recipient.

E-mail test (Administration>Notification>E-mail>test). Send a test message to a configured recipient.

SNMP traps

Trap Receivers (Administration>Notification>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.)

See SNMPv3 (Administration>Network>SNMPv3>options) for information on creating user profiles and selecting authentication and encryption methods.

SNMP Trap Test (Administration>Notification>SNMP Traps>test)

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

- The SNMP version (SNMPv1 or SNMPv3) configured for the selected trap receiver is enabled on this device.
- The trap receiver 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.)

Remote Monitoring

You can register online for the APC Remote Monitoring Service (RMS). APC RMS is a professional service that monitors your power systems and surrounding environment from a remote operation center, 24 hours a day, 7 days a week. Through the **APC RMS Web Site**, you can instantaneously modify the way APC responds to your device events. The APC RMS Web site can also be used to retrieve information concerning your equipment and system events at any time from any place where you can log on to the Internet.

registration (Administration>Notification>Remote Monitoring>Registration).

Parameter	Definition
Registration Status	The status of the most recent APC RMS registration attempt is provided. If a registration attempt is in progress, the page will automatically refresh with the latest status reported until registration is complete or a time-out occurs. The status of the primary and secondary (if necessary) registration e-mails is also displayed.
Device Model	The model name of the monitored device.
Device Serial Number	A unique alphanumeric device descriptor.
System Name	The name of the monitored device such as 'ChemLab UPS'.
System Location	A text description describing the location of the device such as 'Lab A', 'ChemLab Data Center', or '3rd floor - West wing'.
Time Zone	Company time zone.
E-mail Address	Company e-mail address used as a login to the APC RMS Web site and used by APC RMS staff to send e-mail notifications.
Password	Password used to access the APC RMS Web site.
Confirm Password	Reenter the password to confirm your first entry.
First Name	The first name of the monitored device owner or the profile owner.
Last Name	The last name of the monitored device owner or the profile owner.
Company	A text string containing the company name.
Facility Address	Further description of the company address such as a building number or campus name.
Address Line 1	Primary company street address.
Address Line 2	Secondary company street address such as a suite number.
City/Municipality	City or municipality in which the monitored device resides.
State/Province	State or province in which the monitored device resides.
Postal Code	Company zip code.

Parameter	Definition
Country Code	A two-character country descriptor.
Phone Number	Primary company phone number of device owner or profile owner.

configuration (Administration>Notification>Remote Monitoring>configuration).

Parameter	Definition
APC RMS E-mail Status	Indicates if APC RMS E-mail is enabled. This can only be enabled after a successful registration has been completed.
Reset Fields To Default Values	Reset all APC RMS E-mail Configuration fields to factory defaults.
Primary Registration E-mail Recipient	Primary destination address of APC RMS registration e-mail.
Secondary Registration E-mail Recipient	Failover destination address of APC RMS registration e-mail. This is used if primary address is not available.
Primary Data E-mail Recipient	Primary destination address of APC RMS device specific data such as device identification, status, and events.
Secondary Data E-mail Recipient	Failover destination address of APC RMS device specific data. This is used if primary address is not available.
Send Via	Select the SMTP server to be used for sending e-mails; Recipient (APC) or Local (SMTP server on this form).
Primary DNS Server	Primary Domain Name Server used to find the mail server. The default is the APC primary server.
Secondary DNS Server	Failover Domain Name Server used if the primary server is unavailable. The default is the APC secondary server.
SMTP Server	SMTP mail server to use when sending e-mails. The default is the APC mail server.

Syslog (Logs>Syslog>*options*)

The Rack ATS can send messages to up to four Syslog servers when an event occurs. The Syslog servers record events that occur at network devices in a log that provides a centralized record of events.

This user's guide does not describe Syslog or its configuration values in detail. For more information about Syslog, see **RFC3164**.

Identifying Syslog Servers (Logs>Syslog>servers).

Setting	Definition
Syslog Server	Uses IP addresses or host names to identify from one to four servers to receive Syslog messages sent by the Rack ATS.
Port	The user datagram protocol (UDP) port that the Rack ATS will use to send Syslog messages. The default is **514**, the UDP port assigned to Syslog.

Syslog Settings (Logs>Syslog>settings).

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

Setting	**Definition**
Severity Mapping	Maps each severity level of Rack ATS events to available Syslog priorities. You should not need to change the mappings. The following definitions are from RFC3164: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages Following are the default settings for the **Local Priority** settings: • **Severe** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info** **NOTE:** To disable Syslog messages, see Configuring event actions.

Syslog Test and Format Example (Logs>Syslog>test). 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, according to the required message fields.
   – The priority (PRI): The Syslog priority assigned to the message's event, and the facility code of messages sent by the Rack ATS.
   – The Header: A time stamp and the IP address of the Rack ATS.
   – The message (MSG) part:
     - The TAG field, followed by a colon and space, identifies the event type.
     - The CONTENT field is the event text, followed (optionally) by a space and the event code.

For example, `APC: Test Syslog` is valid.

Indirect Notification Through Logs or Queries

Event log (Logs>Events>*options*)

Displaying and using the event log (Logs>Events>log). View or delete the event log. By default, the log displays all events recorded during the last two days, in reverse chronological order.

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

  In your browser's options, JavaScript® must be enabled for you to use the **Launch Log in New Window** button.

  You can also use FTP or SCP to view the event log. See Using FTP or SCP to retrieve log files.

- **Filtering the log by date or time:** To display the entire event log, or to change the number of days or weeks for which the log displays the most recent events, select **Last**. Select a time range from the drop-down menu, then click **Apply**. The filter configuration is saved until the device restarts.
  To display events logged during a specific time range, select **From**. Specify the beginning and ending times (using the 24-hour clock format) and dates for which to display events, then click **Apply**. The filter configuration is saved until the device restarts.
- **Filtering the log by event**: To specify the events that display in the log, click **Filter Log**. Unmark the checkbox of an event category or alarm severity level to remove it from view. Text at the upper right corner of the event log page indicates that a filter is active. The filter is active until you clear it or the device restarts. To remove an active filter, click **Filter Log**, then **Clear Filter (Show All)**.

Events are processed through the filter using **OR** logic.

- Events that you do not select from the Filter By Severity list never display in the filtered event log, even if the event occurs in a category you selected from the Filter by Category list.
- Events that you do not select from the Filter by Category list never display in the filtered event log, even if devices in the category enter an alarm state you selected from the Filter by Severity list.

- **Deleting the event log**: 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, see Configuring by group.

For lists of all configurable events and their current configuration, select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu.

See Configuring by event.

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

With reverse lookup enabled, when a network-related event occurs, both the IP address and the domain name for the networked device associated with the event are logged in the event log. If no domain name entry exists for the device, only its IP address is logged with the event. Since domain names generally change less frequently than IP addresses, enabling reverse lookup can improve the ability to identify addresses of networked devices that are causing events.

Data log (Logs>Data>*options*)

Displaying and using the data log (Logs>Data>log). View a log of measurements of the present load, including the minimum and maximum load current for each bank. Each entry is listed by the date and time the data was recorded.

- **Displaying the data log**: You can view the data log as a page of the Web interface (the default view) or, to see more of the data without scrolling, click **Launch Log in New Window** from that page to display a full-screen view of the log.
- The values displayed are source A frequency, source A voltage, source B frequency, source B voltage, and the selected source along with the present min and max load.

In your browser's options, JavaScript must be enabled for you to use the **Launch Log in New Window** button.

Alternatively, you can use FTP or SCP to view the data log. See Using FTP or SCP to retrieve log files.

- **Filtering the log by date or time**: To display the entire data log, or to change the number of days or weeks for which the log displays the most recent events, select **Last**. Select a time range from the drop-down menu, then click **Apply**. The filter configuration is saved until the device restarts.
  To display data logged during a specific time range, select **From**. Specify the beginning and ending dates and times for which to display data, then click **Apply**. The filter configuration is saved until the device restarts.

  Enter the time using the 24-hour clock format.

- **Deleting the data log**: To delete all data recorded in the log, click **Clear Data Log** on the Web page that displays the log. Deleted data cannot be retrieved.

Setting the data collection interval (Logs>Data>interval). Define, in the **Log Interval** setting, how frequently data is sampled and stored in the data log, and view the calculation of how many days of data the log can store, based on the interval you selected. When the log is full, the older entries are deleted. To avoid automatic deletion of older data, enable and configure data log rotation, described in the next section.

Configuring data log rotation (Logs>Data>rotation). Set up a password-protected data log repository on a specified FTP server. Enabling rotation causes the contents of the data log to be appended to the file you specify by name and location. Updates to this file occur at the upload interval you specify.

Parameter	Description
Data Log Rotation	Enable or disable (the default) data log rotation.
FTP Server Address	The location of the FTP server where the data repository file is stored.
User Name	The user name required to retrieve data from the repository file.
Password	The password required to retrieve data from the repository file.
File Path	The path to the repository file.
Filename	The name of the repository file (an ASCII text file).
Delay *X* hours between uploads	The number of hours between uploads of data to the file.
Maximum Retries	The maximum number of times the upload will be attempted after initial failure.
Failure Wait Time	How long in minutes before an attempt to upload data times out.

Using FTP or SCP to retrieve log files

An Administrator or Device User can use FTP or SCP to retrieve a tab-delineated event log file (*event.txt*) or data log file (*data.txt*) and import it into a spreadsheet.

- The file reports all events or data recorded since the log was last deleted or truncated because it reached maximum size.
- The file includes information that the event log or data log does not display.
  - The version of the file format (first field).
  - The date and time the file was retrieved.
  - The **Name**, **Contact**, and **Location** values and IP address of the Rack ATS.
  - The unique **Event Code** for each recorded event (*event.txt* file only).

The Rack ATS uses a four-digit year for log entries. You may need to select a four-digit date format in your spreadsheet application to display all four digits.

If you are using the encryption-based security protocols for your system, use SCP to retrieve the log file.

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 Automatic Transfer Switch *Utility* CD and on the APC Web site (**www.apc.com**) for information on available protocols and methods for setting up the type of security you need.

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

1. At a command prompt, type **ftp** and the Rack ATS's IP address, and press ENTER. If the **Port** setting for the **FTP Server** option (set through the **Network** menu of the **Administration** tab) has been changed from its default (**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 File Transfers. You can specify any port from 5001 to 32768.

2. Use the case-sensitive **User Name** and **Password** for Administrator or Device User to log on. For Administrator, **apc** is the default for **User Name** and **Password**. For the Device User, the defaults are **device** for **User Name** and **apc** for **Password**.
3. Use the **get** command to transmit the text of a log to your local drive.

   ```
   ftp>get event.txt
   ```

   or

   ```
    ftp>get data.txt
   ```

4. You can use the **del** command to clear the contents of either log.

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

   or

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

   You will not be asked to confirm the deletion.
   – If you clear the data log, the event log records a deleted-log event.
   –If you clear the event log, a new *event.txt* file records the event.

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

Queries (SNMP GETs)

See SNMP for a description of SNMP access types that enable an NMS to perform informational queries. Configuring the most restrictive SNMP access type, READ, enables informational queries without allowing remote configuration changes.

Administration: General Options

Identification (Administration>General>Identification)

Define values for **Name** (the device name), **Location** (the physical location), and **Contact** (the person responsible for the device) used by the Rack ATS's SNMP agent. These settings are the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifiers (OIDs).

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

Set the Date and Time

Method (Administration>General>Date & Time>mode)

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

- **Manual Mode**: Do one of the following:
  - Enter the date and time for the Rack ATS.
  - Mark the checkbox **Apply Local Computer Time** to match the date and time settings of the computer you are using.
- **Synchronize with NTP Server**: Have an NTP Server define the date and time for the Rack ATS.

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.

Setting	Definition
Time Zone	Select a time zone. The number of hours preceding each time zone in the list is the offset from Coordinated Universal Time (UTC), formerly Greenwich Mean Time).
Update Interval	Define how often, in hours, the Rack ATS accesses the NTP Server for an update. *Minimum*: 1; *Maximum*: 8760 (1 year).
Update Using NTP Now	Initiate an immediate update of date and time by the NTP Server.

Daylight saving (Administration>General>Date & Time>daylight saving)

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

When customizing DST:

- If the local DST always starts or ends on the fourth occurrence of a specific weekday of a month (e.g, the fourth Sunday), choose Fourth/Last. If a fifth Sunday occurs in that month in a subsequent year, the time setting still changes on the fourth Sunday.
- If the local DST always starts or ends on the last occurrence of a specific weekday of a month, whether it is the fourth or the fifth occurrence, choose Fifth/Last.

Format (Administration>General>Date & Time>date format)

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

Use an .ini File (Administration>General>User Config File)

Use the settings from one Rack ATS to configure another. Retrieve the config.ini file from the configured Rack ATS, customize that file (e.g., to change the IP address), and upload the customized file to the new Rack ATS. The file name can be up to 64 characters, and must have the.ini suffix.

Status	Reports the progress of the upload. The upload succeeds even if the file contains errors, but a system event reports the errors in the event log.
Upload	Browse to the customized file and upload it so that the current Rack ATS can use it to set its own configuration.

To retrieve and customize the file of a configured Rack ATS, see Exporting Configuration Settings.

Instead of uploading the file to one Rack ATS, you can export the file to multiple Rack ATSs by using an FTP or SCP script or a batch file and the APC .ini file utility, available on the APC Automatic Transfer Switch *Utility* CD and the APC Web site **www.apc.com/tools/download**.

System Preferences (Administration>General>Preferences)

Color-coding events in the event log

This option is disabled by default. Mark the Event Log Color Coding check box to enable color-coding of alarm text recorded in the event log. System-event entries and configuration-change entries do not change color.

Text color	Definition
Red	**Critical:** A critical alarm exists, which requires immediate action.
Orange	**Warning:** An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
Black	Informational event
Green	**Normal:** No alarms are present.

Changing the default temperature scale

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

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

Action	Definition
Reboot Management Interface	Restarts the interface of the Rack ATS.
Reset All[1]	Check-mark **Exclude TCP/IP** to reset all configuration values; unmark **Exclude TCP/IP** to reset all values except TCP/IP.
Reset Only[1]	**TCP/IP settings**: Set TCP/IP Configuration to **DHCP & BOOTP**, its default setting, requiring that the Rack ATS receive its TCP/IP settings from a DHCP or BOOTP server. See TCP/IP settings (Administration>Network>TCP/IP).
	Event configuration: Reset all changes to event configuration, by event and by group, to their default settings.

[1] Resetting may take up to a minute. The Automatic Transfer Switch name and output voltage settings will not be reset.

Configuring Links (Administration>General>Quick Links)

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

By default, these links access the following Web pages:

- **Link 1**: The home page of the APC Web site.
- **Link 2**: A page where you can use samples of APC Web-enabled products.
- **Link 3**: The home page of the APC Remote Monitoring Service.

To reconfigure any of the following, click the link name in the **Display** column:

- **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 or server.

About the Rack ATS (Administration>General>About)

The hardware information is especially useful to APC Customer Support to troubleshoot problems with the Rack ATS.

Firmware information for the Application Module and APC OS (AOS) indicates the name, the firmware version, and the date and time each firmware module was created. This information is also useful in troubleshooting and enables you to determine if updated firmware is available at the APC Web site.

APC Device IP Configuration Wizard

Capabilities, Requirements, and Installation

Using the Wizard to configure TCP/IP settings

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

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

System requirements

The Wizard runs on Microsoft Windows 2000, Windows Server 2003, and Windows XP operating systems.

Installation

To install the Wizard from the APC Automatic Transfer Switch *Utility* CD:

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

To install the Wizard from a downloaded executable file:

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

Use the Wizard

❗ Most software firewalls must be temporarily disabled for the Wizard to discover unconfigured Automatic Transfer Switches.

Launch the Wizard

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

Configure the basic TCP/IP settings remotely

Prepare to configure the settings. Before you run the Wizard:

1. Contact your network administrator to obtain valid TCP/IP settings.
2. If you are configuring multiple unconfigured Rack ATSs or network-enabled devices, obtain the MAC address of each one to identify it when the Wizard discovers it. (The Wizard displays the MAC address on the screen on which you then enter the TCP/IP settings.)
   – For a Rack ATS that you install, the MAC address is on a label on the bottom of the card.
   – For a network-enabled device (with an embedded Rack ATS), the MAC address is on a label on the device.

     You can also obtain the MAC address from the Quality Assurance slip that came with the Rack ATS or device.

Run the Wizard to perform the configuration. To discover and configure unconfigured Rack ATSs or network-enabled devices over the network:

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

On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the Rack ATS or device after the Wizard transmits the settings.

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

Configure or reconfigure the TCP/IP settings locally

1. Contact your network administrator to obtain valid TCP/IP settings.
2. Connect the serial cable (which came with the Rack ATS or device) from an available communications port on your computer to the serial port of the card or device. Make sure no other application is using the computer port.
3. From the **Start** menu, launch the Wizard application.
4. If the Network Management Card or network-enabled device is not configured, wait for the Wizard to detect it. Otherwise, click **Next>**.
5. Select **Locally (through the serial port)**, and click **Next >**.
6. Enter the system IP, subnet mask, and default gateway for the Rack ATS or device, and click **Next >**.
7. On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the Rack ATS or device after the Wizard transmits the settings.
8. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**. If you selected **Start a Web browser when finished** in step 7, you can now configure other parameters through the Web interface of the card or device.

Exporting Configuration Settings

Retrieving and Exporting the .ini File

Summary of the procedure

An Administrator can retrieve the .ini file of one Rack ATS and export it to another Rack ATS or to multiple Rack ATSs.

1. Configure the Rack ATS to have the settings you want to export.
2. Retrieve the .ini file from that Rack ATS.
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 Rack ATS to transfer the copied file to one or more additional Rack ATSs. (To transfer the file to multiple Rack ATSs simultaneously, write an FTP or SCP script that repeats the steps for transferring the file to a single Rack ATS.)

Each receiving Rack ATS uses the file to reconfigure its own settings and then deletes it.

Contents of the .ini file

The config.ini file that you retrieve from the Rack ATS contains the following:

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

  Only section headings and keywords supported for the specific Rack ATS from which you retrieve the file are included.

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

  See Customizing for configuration guidelines for date and time settings.

Detailed procedures

Use the following procedures to retrieve the settings of one Rack ATS and export them to one or more other Rack ATSs.

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

1. Configure a Rack ATS with the settings you want to export.

   To avoid errors, configure the Rack ATS by using its Web interface or control console whenever possible. Directly editing the .ini file risks introducing errors.

2. Use FTP to retrieve the config.ini file from the Rack ATS you configured:

   a. Open a connection to the Rack ATS, using its IP Address. For example:

   ```
   ftp> open 158.165.2.132
   ```

   b. Log on using the Administrator user name and password.

   c. Retrieve the config.ini file containing the Rack ATS's 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 Rack ATSs and export them to other Rack ATSs, see *Release Notes: ini File Utility, version 1.0* on the APC Automatic Transfer Switch *Utility* CD and from **www.apc.com**.

Customizing. You must customize the file to change at least the TCP/IP settings before you export it.

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

enclosed in quotation marks. (Leading or trailing spaces not within the opening and closing quotation marks are ignored.)

– To export a system time with the greatest accuracy, if the receiving Rack ATSs can access a Network Time Protocol server, configure `enabled` for `NTPEnable`: `NTPEnable=enabled`

– Alternatively, reduce transmission time by exporting the `[SystemDate/Time]` section as a separate .ini file.

– Add comments about changes that you made. The first printable character of a comment line must be a semicolon (`;`).

2. Copy the customized file to another file name in the same folder:

– The copy, which you will export to other Rack ATSs, 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.

Exporting the file to a single Rack ATS. To export the .ini file to another Automatic Transfer Switch, do either of the following:

- From the Web interface of the receiving Rack ATS, select the **Administration** tab, **General** on the top menu bar, and **User Config File** on the left navigation menu. Enter the full path of the file, or use **Browse**.
- Use any file transfer protocol supported by Automatic Transfer Switches, i.e., FTP, FTP Client, SCP, or TFTP). The following example uses FTP:

a. From the folder containing the copy of the customized .ini file, use FTP to log in to the Rack ATS to which you are exporting the .ini file:

```
ftp> open ip_address
```

b. Export the copy of the customized .ini file to the root directory of the receiving Rack ATS:

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

Exporting the file to multiple Rack ATSs. To export the .ini file to multiple Automatic Transfer Switches:

- Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single Management Card.
- 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 Automatic Transfer Switch *Utility* CD and from **www.apc.com**.

The Upload Event and Error Messages

The event and its error messages

The following system event occurs when the receiving Automatic Transfer Switch completes using the .ini file to update its settings.

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

This event has no default severity level.

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

Event text	Description
Configuration file warning: Invalid keyword on line *number*. Configuration file warning: Invalid value on line *number*.	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line *number.*	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line *number*.	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, the Rack ATS 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.

Messages in config.ini

A device associated with the Rack ATS from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the device (such as a UPS or Integrated Environmental Monitor) is not present or, for another reason, is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values. For example:

```
UPS not discovered
IEM not discovered
```

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

Errors generated by overridden values

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

See Contents of the .ini file for information about which values are overridden.

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

Related Topics

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

See APC Device IP Configuration Wizard.

File Transfers

Upgrading Firmware

Benefits of upgrading firmware

When you upgrade the firmware on the Automatic Transfer Switch:

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

Keeping the firmware versions consistent across your network ensures that all Automatic Transfer Switches support the same features in the same manner.

Firmware files (Automatic Transfer Switch)

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

The APC Operating System (AOS) and application module files used with the Automatic Transfer Switch share the same basic format:

`apc_`***`hardware-version`***`_`***`type`***`_`***`firmware-version`***`.bin`

- **`apc`**: Indicates that this is an APC file.
- ***`hardware-version`***: **`hw0`***x* identifies the version of the hardware on which you can use this binary file.
- ***`type`***: Identifies whether the file is for the APC Operating System (AOS) or the application module for the Automatic Transfer Switch.
- ***`version`***: The version number of the file.
- **`bin`**: Indicates that this is a binary file.

Obtain the latest firmware version

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

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

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

Firmware File Transfer Methods

To upgrade the firmware of a Rack ATS, use one of these methods:

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

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

Use FTP or SCP to upgrade one Rack ATS

FTP. For you to use FTP to upgrade one Rack ATS over the network:

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

To transfer the files:

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

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

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

   – **apc_hw02_aos_*xxx*.bin**

   – **apc_hw02_*application*_*xxx*.bin**

2. Open an FTP client session:

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

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

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

   ```
   ftp> open 150.250.6.10 21000
   ```

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

4. Log on as Administrator; **apc** is the default user name and password.

5. Upgrade the AOS. (In the example, *xxx* is the firmware version number:

   ```
   ftp> bin
   ftp> put apc_hw02_aos_xxx.bin
   ```

6. When FTP confirms the transfer, type **quit** to close the session.

7. After 20 seconds, repeat step 2 through step 5. In step 5, use the application module file name.

SCP. To use Secure CoPy (SCP) to upgrade firmware for a Rack ATS:

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 Rack ATS. The following example uses *xxx* to represent the version number of the AOS module:
   ```
   scp apc_hw02_aos_xxx.bin apc@158.205.6.185:apc_hw02_aos_xxx.bin
   ```
3. Use a similar SCP command line, with the name of the application module, to transfer the second firmware module to the Rack ATS.

Upgrading multiple Rack ATSs

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

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

Use FTP or SCP to upgrade multiple Rack ATSs. To upgrade multiple Automatic Transfer Switchs using an FTP client or using SCP, write a script which automatically performs the procedure.

Use XMODEM to upgrade one Rack ATS

To upgrade the firmware for a Rack ATS that is not on the network:

1. Obtain the individual firmware modules (the AOS module and the application module) from **www.apc.com/tools/download**.
2. Select a serial port at the local computer and disable any service that uses the port.
3. Connect the provided serial cable (APC part number 940-0144A) to the selected port and to the serial port at the Rack ATS.

4. Run a terminal program such as HyperTerminal, and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Save the changes.
5. Press ENTER, repeatedly if necessary, 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. Select a baud rate, change the terminal program's baud rate to match your selection, and press ENTER. A higher baud rate causes faster upgrades.
9. From the terminal program's menu, select the binary AOS file to transfer using XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600. The Rack ATS 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.

⚠ Do not interrupt the download.

Upgrading the firmware will not interfere with the operation of the outlets.

For information about the format used for firmware modules, see Firmware files (Automatic Transfer Switch).

Verifying Upgrades

Verify the success or failure of the transfer

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

Last Transfer Result codes

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

Verify the version numbers of installed firmware

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

Product Information

Warranty and Service

Two-Year Factory Warranty

This warranty applies only to the products you purchase for your use in accordance with this manual.

Terms of warranty

APC warrants its products to be free from defects in materials and workmanship for a period of two years from the date of purchase. APC will repair or replace defective products covered by this warranty. This warranty does not apply to equipment that has been damaged by accident, negligence or misapplication or has been altered or modified in any way. Repair or replacement of a defective product or part thereof does not extend the original warranty period. Any parts furnished under this warranty may be new or factory-remanufactured.

Non-transferable warranty

This warranty extends only to the original purchaser who must have properly registered the product. The product may be registered at the APC Web site, **www.apc.com**.

Exclusions

APC shall not be liable under the warranty if its testing and examination disclose that the alleged defect in the product does not exist or was caused by end user's or any third person's misuse, negligence, improper installation or testing. Further, APC shall not be liable under the warranty for unauthorized attempts to repair or modify wrong or inadequate electrical voltage or connection, inappropriate on-site operation conditions, corrosive atmosphere, repair, installation, exposure to the elements, Acts of God, fire, theft, or installation contrary to APC recommendations or specifications or in any event if the APC serial number has been altered, defaced, or removed, or any other cause beyond the range of the intended use.

THERE ARE NO WARRANTIES, EXPRESS OR IMPLIED, BY OPERATION OF LAW OR OTHERWISE, OF PRODUCTS SOLD, SERVICED OR FURNISHED UNDER THIS AGREEMENT OR IN CONNECTION HEREWITH. APC DISCLAIMS ALL IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTION AND FITNESS FOR A PARTICULAR PURPOSE. APC EXPRESS WARRANTIES WILL NOT BE ENLARGED, DIMINISHED, OR AFFECTED BY AND NO OBLIGATION OR LIABILITY WILL ARISE OUT OF, APC RENDERING OF TECHNICAL OR OTHER ADVICE OR SERVICE IN CONNECTION WITH THE PRODUCTS. THE FOREGOING WARRANTIES AND REMEDIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES AND REMEDIES. THE WARRANTIES SET FORTH ABOVE CONSTITUTE APC'S SOLE LIABILITY AND PURCHASER'S EXCLUSIVE REMEDY FOR ANY BREACH OF SUCH WARRANTIES. APC WARRANTIES EXTEND ONLY TO PURCHASER AND ARE NOT EXTENDED TO ANY THIRD PARTIES.

IN NO EVENT SHALL APC, ITS OFFICERS, DIRECTORS, AFFILIATES OR EMPLOYEES BE LIABLE FOR ANY FORM OF INDIRECT, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, ARISING OUT OF THE USE, SERVICE OR INSTALLATION, OF THE PRODUCTS, WHETHER SUCH DAMAGES ARISE IN CONTRACT OR TORT, IRRESPECTIVE OF FAULT, NEGLIGENCE OR STRICT LIABILITY OR WHETHER APC HAS BEEN ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES. SPECIFICALLY, APC IS NOT LIABLE FOR ANY COSTS, SUCH AS LOST PROFITS OR REVENUE, LOSS OF EQUIPMENT, LOSS OF USE OF EQUIPMENT, LOSS OF SOFTWARE, LOSS OF DATA, COSTS OF SUBSTITUENTS, CLAIMS BY THIRD PARTIES, OR OTHERWISE.

NO SALESMAN, EMPLOYEE OR AGENT OF APC IS AUTHORIZED TO ADD TO OR VARY THE TERMS OF THIS WARRANTY. WARRANTY TERMS MAY BE MODIFIED, IF AT ALL, ONLY IN WRITING SIGNED BY AN APC OFFICER AND LEGAL DEPARTMENT.

Warranty claims

Customers with warranty claims issues may access the APC customer support network through the Support page of the APC Web site, **www.apc.com/support**. Select your country from the country selection pull-down menu at the top of the Web page. Select the Support tab to obtain contact information for customer support in your region.

Life-Support Policy

General policy

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

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

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

Examples of life-support devices

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

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

Index

A

About options
  for information about the Rack ATS 80
Access
  enabling or disabling methods of access
    to the control console 50
    to the Web interface 48
Administration
  General menu 76
  Network menu 41
  Notification menu 57
  Security 36
  Security Menu 36
  Security menu 36
Apply Local Computer Time 76
Authenticate 63
Authenticating users through RADIUS 36
Authentication Traps setting 63
Automatic log-off for inactivity 40

B

BOOTP
  BOOTP server providing TCP/IP settings 41
  Status LED indicating BOOTP requests 10
Browsers
  error messages 23
  Types and versions supported 21
  types and versions supported 21

C

Certificates, how to create, view, or remove 49
Community Name
  for trap receivers 63
config.ini file, contents 85
Configuring
  RADIUS authentication 37
Contact identification (whom to contact) 76
Control console
  configuring access 50
  Device Manager menu 19
  navigating menus 18
  refreshing menus 18

D

Data log
  displaying and using 71
  filtering by date or time 71
  importing into spreadsheet 73
  Log Interval setting 72
  rotation (archiving) 72
  using FTP or SCP to retrieve 73
Date & Time settings 76
Date format, configuring 77
Daylight saving time 77
Device IP Configuration Wizard
  installation and system requirements 81
  using the wizard
    for local configuration. 83
    for remote configuration 82
Device Manager menu, control console 19
DHCP
  APC cookie 43
  DHCP server providing TCP/IP settings 41
  response options 43
Disable
  e-mail to a recipient 62
  encryption algorithms for SSH 50
  reverse lookup 70
  SSL cipher suites 48

- Telnet 50

DNS
- defining host and domain names 46
- query types 47
- specifying DNS servers by IP address 46

E

E-mail
- configuring notification parameters 60
- configuring recipients 62
- test message 62
- using for paging 62

Enable
- e-mail forwarding to external SMTP servers 62
- e-mail to a recipient 62
- encryption algorithms for SSH 50
- reverse lookup 70
- SSL cipher suites 48
- Telnet 50
- versions of SSH 50

Error messages
- browser 23
- for firmware file transfer 96
- from overridden values during .ini file transfer 90

Ethernet port speed 45

Event actions 57
- configuring by event 58
- configuring by group 59

Event log
- accessing 18, 69
- errors from overridden values during .ini file transfer 90
- using FTP del command 74
- using FTP or SCP to retrieve 73

event.txt file
- contents 73
- importing into spreadsheet 73

F

Facility Code (Syslog setting) 67

File transfers
- to upgrade firmware 91
- verification 96

Firmware
- benefits of upgrading 91
- file transfer methods
  - automated upgrade tool 92
  - FTP or SCP 93
  - XMODEM 94
- files for the Rack ATS 91
- obtaining the latest version 92
- verifying upgrades and updates 96

Firmware versions displayed on main screen 16

From Address (SMTP setting) 61

FTP
- server settings 55
- transferring firmware files 93
- using to retrieve event or data log 73

G

General menu, Administration tab 76

H

Help
- in Web interface 28

Host keys
- adding or replacing 51
- status 51

Host name of trap receivers 63, 65

I

Identification (Name, Location, and Contact)
- in control console 16

in Web interface 76
Inactivity timeout 40
ini files, *See* User configuration files

J

JavaScript, required to launch log in new window 69

K

keywords
user configuration file 85

L

Last Transfer Result codes 96
Launch Log in New Window, JavaScript requirement. 69
Life support policy 100
Links, configuration 79
Local SMTP Server
defining by IP address or DNS name 61
recommended option for routing e-mail 62
Local Users, setting user access 36
Location (system value) 76
Logging on
locally (through a serial port) to the control console 14
remotely to the control console 13
Web interface 22
Login date and time
control console 16
Web interface 76

M

Main screen
displaying identification 16
firmware values displayed 16
login date and time 16
status 17
Up Time 16
User access identification 16
Menus
Device Manager 19
General 76
Logs 57
Network 29, 41
Notification 57
Security 36
top menu bar 24
Message Generation (Syslog setting) 67

N

Network menu 41
Network Time Protocol (NTP) 76
NMS IP/Host Name for trap receivers 63, 65
Notification menu 57

O

Override keyword, in user configuration file 85

P

Paging
by using e-mail 62
Passwords
default for all account types 22
defining for each account type 36
recovering from a lost password 5
recovering from lost password 5
Port speed, configuring for Ethernet 45
Ports
FTP server 56
HTTP and HTTPS 48
RADIUS server 38

Telnet and SSH 50
Primary NTP Server 76

Q

Quick Links, configuration 79

R

RADIUS
configuration 37
server configuration 38
Reboot Management Interface 79
Recent Events
Device Events on home page 28
Recipient SMTP server 62
Remote Monitoring Service 79
Remote Users
authentication 37
setting user access 36
Reset
preventing automated reset
for inactivity 12
Reset All 79
Reset Only 79
Reverse lookup 70

S

SCP
for high-security file transfer 56
transferring firmware files 93
using to retrieve event or data log 73
Secondary NTP Server 76
Section headings, user configuration
file 85
Security menu
Administration
Security Menu 36
Severity Mapping (Syslog setting) 68
SMTP server
selecting for e-mail recipients 62
settings 61
SNMP
authentication traps 63
disabling SNMPv1 52
SSH
encryption algorithms 50
host keys 51
SSL
cipher suites 48
configuring cipher suites 48
how to create, view, or remove certificates 49
Status
control console main screen 17
Web interface 26, 27
Synchronize with NTP Server,
(Date & Time) 76
Syslog 67
identifying the Syslog server 67
mapping event severity to Syslog priorities 68
settings 67
test 68
System Name 76

T

TCP/IP configuration 41
Temperature units (Fahrenheit or Celsius) 79
Test
DNS query 47
e-mail recipient settings 62
RADIUS server path 38
Syslog 68
trap receiver 64
Time setting 76
Time Zone, for synchronizing with NTP
server 77
Timeout setting for RADIUS 38
To Address, e-mail recipients 62

Traps
trap receivers 63

U

Up Time
control console main screen 16
in Web interface 80
Update Interval, Date & Time setting 77
Update Using NTP Now, Date & Time setting 77
Upgrading firmware 91
URL address formats 23
User access identification, control console interface 16
User configuration files
contents 85
overriding device-specific values 85
retrieving and exporting 84
system event and error messages 89
using FTP to retrieve and transfer the files 83
using the APC utility to retrieve and transfer the files 86, 88, 94
User names
default by account type 22
defining for each account type. 36
maximum number of characters for RADIUS 36

V

Verifying firmware upgrades and updates 96

W

Web interface
configuring access 48
logging on 22
URL address formats 23

X

XMODEM to transfer firmware files 94

APC Worldwide Customer Support

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

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

Regional centers

Direct InfraStruXure Customer Support Line	(1)(877)537-0607 (toll free)
APC headquarters U.S., Canada	(1)(800)800-4272 (toll free)
Latin America	(1)(401)789-5735 (USA)
Europe, Middle East, Africa	(353)(91)702000 (Ireland)
Western Europe (inc. Scandinavia)	+800 0272 0272
Japan	(0) 36402-2001
Australia, New Zealand, South Pacific area	(61) (2) 9955 9366 (Australia)

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

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

Copyright

990-3076-001 **12/2007**

CERTIFIED
InfraStruXure
by APC