

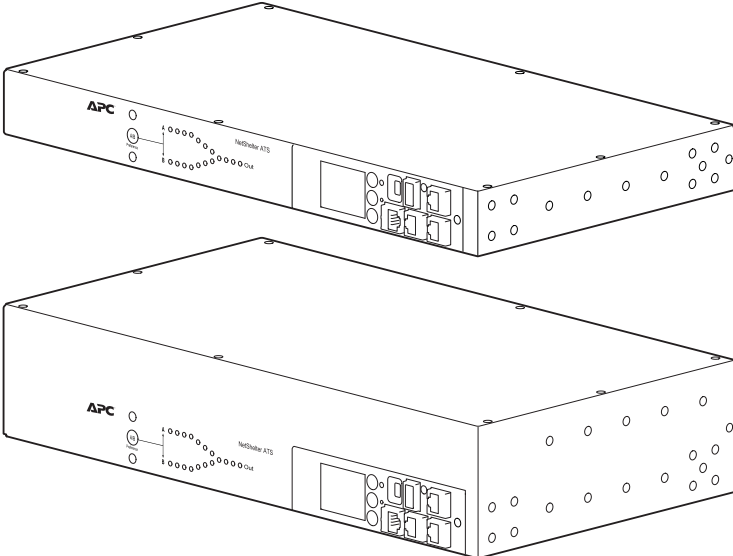
Rack ATS with Network Management Card 3

User Guide



AP44XXA

990-91718A-001
Release date: December 2022



Legal Information

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this guide are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owners.

This guide and its content are protected under applicable copyright laws and furnished for informational use only. No part of this guide may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the guide or its content, except for a non-exclusive and personal license to consult it on an "as is" basis. Schneider Electric products and equipment should be installed, operated, serviced, and maintained only by qualified personnel.

As standards, specifications, and designs change from time to time, information contained in this guide may be subject to change without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this material or consequences arising out of or resulting from the use of the information contained herein.

APC, the APC logo, Data Center Expert, EcoStruxure IT, NetShelter, and Powernet are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owners.

Table of Contents

Important Safety Instructions — SAVE THESE INSTRUCTIONS	9
Rack ATS Safety	10
Overview	11
Additional Documentation	11
User Comments	11
Product Features	12
Internal Protection Measures	13
How Switching Works	14
Types of User Accounts	15
Watchdog Features	16
Network Interface Watchdog Mechanism	16
Resetting the Network Timer	16
Network Port Sharing (NPS)	17
Display ID	17
Install an NPS Group	18
Firmware Upgrade with NPS	18
Getting Started	19
Establish Network Settings	19
About IPv4 Setup	19
About IPv6 Setup	20
TCP/IP Configuration Methods	20
.ini File Utility	25
Updating Firmware	26
Firmware File Transfer Methods	26
Use the Firmware Update Utility	27
Manually Update One Rack ATS with FTP or SCP	28
Use a USB Drive To Transfer and Update Files	29
How To Update Multiple Rack ATS Units	29
Firmware Upgrade with NPS	29
Verifying Upgrades and Updates	30
Verify the Success Or Failure of the Transfer	30
Last Transfer Result Codes	30
Verify the Version of Installed Firmware	30
Network Management with Other Applications	31
Recover from a Lost Password	32
Front Panel Overview	33
Device Status LED	34
Network Status LED	34
10/100/1000 Status LED	34
LCD Display Screens	35
Default Screens	36
Menu screens	37
Alarm Status Indicators	39

Command Line Interface	40
Log On to the CLI	40
Local Access to the CLI.....	40
Remote Access to the CLI	41
About the Main Screen	42
Using the CLI	44
Command Syntax.....	45
Command Response Codes	46
Prompting for User Input during Command Execution	46
Command Editing.....	46
History	46
Auto Completion.....	47
Delimiter	47
Options and Arguments Inputs	47
Response Format and Message Codes.....	48
Network Management Card Command Descriptions	49
? or help	49
about.....	51
alarmcount.....	51
boot.....	52
bye, exit, or quit.....	53
cd.....	53
clrrst	53
console.....	54
date.....	55
delete	55
dir	56
dns.....	57
eapol	58
email	59
eventlog.....	60
exit.....	61
firewall.....	61
format.....	61
ftp	62
help.....	62
lang.....	62
lastrst	63
ledblink.....	63
logzip	63
netstat	64
ntp.....	64
ping.....	65
portSpeed.....	65
prompt.....	66
pwd	66
quit.....	66
radius	67

reboot.....	68
resetToDef	68
session.....	69
smtp.....	70
snmp.....	71
snmpv3.....	72
ssh.....	73
ssl.....	74
snmptrap.....	77
system.....	78
tcpip.....	79
tcpip6.....	80
user.....	81
userdfit.....	82
web.....	83
whoami.....	84
wifi.....	84
xferINI.....	85
xferStatus.....	85
Device Command Descriptions.....	86
Network Port Sharing Commands.....	86
aboutATS.....	86
atsMeasure.....	87
atsStatus.....	87
bkLowLoad.....	88
bkNearOver.....	89
bkOverLoad.....	90
bkPeakLoad.....	91
bkReading.....	92
eventCounts.....	93
freqDeviat.....	93
frontPanel.....	94
Humidity Sensor Note:.....	95
humAlGen.....	95
humHyst.....	96
humLow.....	97
humMin.....	98
humReading.....	99
humStatus.....	99
lcd.....	100
lcdBlink.....	100
lineVRMS.....	101
logToFlash.....	102
phLowLoad.....	103
phNearOver.....	103
phOverLoad.....	104
phPeakLoad.....	104
phReading.....	105

prodInfo	105
sensorName	106
sourceAName	106
sourceBName	107
sourcePref	107
Temperature Sensor Note:	108
tempAlGen.....	108
tempHigh	109
tempHyst	110
tempMax	111
tempPeak	112
tempReading	112
vMediumLimit.....	113
vNarrowLmt	114
vSensitvty	115
vWideLmt	116
vXferRange.....	117
Web User Interface	118
Log on to the Web UI.....	118
URL address formats	119
First Log On	119
Web UI Features	120
Tabs	120
Limited Status Access.....	120
Device Status Icons	121
Quick Links	121
Network Port Sharing (NPS) on the Web UI	122
Home Tab	123
Status Tab.....	124
View NPS Groups	124
View Device Alarms	125
View Device Status	125
View The Unit Status	126
View Load Status	126
View Power Measurements.....	127
View Environment Status	127
View Network Status	128
Control Tab	130
Manage User Sessions.....	130
Reset the Network Interface.....	131
Configuration Tab	132
Configure the Rack ATS	133
Configure NPS Groups	133
Configure Rack ATS Name and Location.....	134
Set Preferred Power Source.....	134
Configure Switching Behavior.....	135
Configure Load Thresholds	138

Turn the LCD Display On or Off	139
Configure Temperature and Humidity Sensors	139
Manage Security Settings	141
Manage Settings for User Sessions	141
Enable Ping Response	142
Manage Local User Settings	142
Configure Default User Settings	144
Manage Remote User Settings	145
Configure a RADIUS Server	146
Firewall Menus	147
802.1X Security Configuration	149
Configure Network Settings	150
Protocol Configuration Summary	150
Configure TCP/IP and Communication Settings for IPv4 and IPv6	151
Configure Network Port Speed	152
Configure DNS	153
Test DNS Configuration	153
Configure Web Access	154
Configure SSL Certificate for Web Access	155
Configure CLI Access	155
Configure SSH Host Key	156
SNMP Options	157
SNMPv1	158
SNMPv3	159
Configure FTP Server	160
Wi-Fi Configuration with AP9834	161
Configure Notifications	161
Configure Notifications By Event	161
Configure Notifications By Group	162
Set Up E-mail Notifications	163
SNMP Traps	165
General Configuration	166
Configure identification	166
Configure Date, Time, and Daylight Savings	167
Create and Import Settings with the Config File	168
Configure Quick Links	168
Configure Logs	169
Identify Syslog Servers	169
Configure Syslog Settings	169
Test Syslog Servers	170
Tests Tab	171
Set the LCD Light to Blink	171
Set the LED Light to Blink	171
Logs Tab	172
View and Configure the Event Log	172
Viewing the Event Log	172
Reverse Lookup	173

Change the Log Size	174
Network Port Sharing Event Logs and Traps.....	174
View and Configure the Data Log	174
Log.....	174
Graphing	175
Set Logging Intervals	175
Configure Rotation Settings.....	176
Specify Data Log Size.....	176
Firewall Log	177
Use FTP or SCP to Retrieve Log Files.....	177
Download Log Files to a USB Flash Drive	178
About Tab.....	179
About the Rack ATS	179
About the Network.....	179
Support Resources	180
How to Export Configuration Settings	181
Summary of the Procedure	181
Contents of the .ini File	181
.ini and Network Port Sharing.....	181
Detailed Procedures.....	182
Retrieve .ini File	182
Edit .ini File	183
Transfer the File To a Single Rack ATS.....	183
Transfer the File To Multiple Rack ATS Units.....	183
The Upload Event and Error Messages.....	184
The Event and Its Error Messages	184
Messages in Config.ini.....	184
Errors Generated By Overridden Values.....	184
Related Topics	184
Troubleshooting	185
Rack ATS Access Problems.....	185
SNMP Problems	186
Worldwide Customer Support.....	187
Source Code Copyright Notice.....	188

Important Safety Instructions — SAVE THESE INSTRUCTIONS

Read these instructions carefully and look at the equipment to become familiar with it before trying to install, operate, service or maintain it. The following safety messages may appear throughout this manual or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.



The addition of this symbol to a “Danger” or “Warning” safety message indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.



This is the safety alert symbol. It is used to alert the user to potential personal injury hazards. Obey all safety messages with this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in death or serious injury.**

Failure to follow these instructions will result in death or serious injury.

⚠ WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in death or serious injury.**

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠ CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result in minor or moderate injury.**

Failure to follow these instructions can result in injury or equipment damage.

NOTICE

NOTICE is used to address practices not related to physical injury. The safety alert symbol shall not be used with this type of safety message.

Failure to follow these instructions can result in equipment damage.

Please Note

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

A qualified person is one who has skills and knowledge related to the construction, installation, and operation of electrical equipment and has received safety training to recognize and avoid the hazards involved.

Always abide strictly by local laws and regulations in force in the place of installation.

Rack ATS Safety

DANGER

HAZARDOUS VOLTAGE

Do not operate the Rack ATS outside Rated Voltage (+/- 10%). Voltage limits and transfer ranges represent software control of switching behavior, not input voltages for use.

Failure to follow these instructions will result in death or serious injury.

Overview

The APC™ Rack Automatic Transfer Switch (Rack ATS) with Network Management Card 3 (NMC3) provides redundant power to single-corded equipment loads, such as servers. The Rack ATS has two input power cords that supply power to the connected loads from both a primary and secondary power source. If the primary source becomes unavailable or goes out of the configured power range, the Rack ATS will switch to draw power from the secondary source without interrupting critical loads. The Rack ATS has built-in network connectivity, which allows remote management via the Web User Interface (Web UI), its Command Line Interface (CLI), Data Center Expert™, EcoStruxure™ IT, or Simple Network Management Protocol (SNMP).

NOTE: A Network Management Card (NMC) is a Web-based device that manages communication with third-party systems (such as your network). The NMC supports a single management interface across a variety of APC products for a more uniform customer experience.

NOTE: Update your firmware to the latest version after startup. Check www.apc.com for the latest version of the Rack ATS firmware. Enter the model number for your equipment in the Search bar of the website's home page (www.apc.com). Select the desired product from the search results to open that product page. Select the Software & Firmware tab on the product page to view and download any available firmware for that product.

Additional Documentation

You can find the latest version of this manual and additional documentation on www.apc.com:

- *Safety Sheet:* Includes critical safety information for the Rack ATS.
- *Installation Manual:* Describes the procedure for physical installation and initial setup of your Rack ATS
- *Release Notes:* Describes new features, fixed issues, and known issues for the latest firmware version.
- *Security Handbook:* Describes security features for the Network Management Card and for devices with embedded components of the Network Management Card.

To find product documentation, enter the model number for your equipment in the Search bar of the website's home page (www.apc.com). Select the desired product from the search results to open that product page. Select the Documentation tab on the product page to view the list of available literature for that product. Literature can be opened within the website or downloaded as a pdf.

User Comments

We welcome your comments about this document. Contact us at www.apc.com.

Product Features

The Rack ATS has these additional features:

- LED indicators on the front panel of the unit indicate operation conditions such as preferred source, overload current, and Web connectivity. These conditions can also be monitored via the CLI and Web UI.
 - Gigabit Ethernet connectivity.
 - Various levels of access: Super User, Administrator, Device User, Read-Only, and Network-Only User. (These have user name and password requirements.)
 - A multiple-user login feature, which allows up to four users to be logged in simultaneously.
 - 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/TLS, or using HTTP access). The Data Log is accessible by Web browser, SCP, or FTP.
 - SNMP traps, Syslog messages, and e-mail notifications based on the severity level or category of Rack ATS and NMC system events.
 - Security protocols for authentication and encryption.
 - The ability to monitor sources and set source-transfer parameters via Web and CLI interfaces.
 - Set alarm thresholds that provide network and visual alarms to help you prevent overloaded circuits.
 - Temperature and Humidity monitoring (with APC Temperature/Humidity sensors AP9335T and AP9335TH, not included).
 - Internal protection measures against short circuits. (See [Internal Protection Measures](#), page 13 for details.)
- NOTE:** It is recommended that you always connect each Rack ATS source to a Double Conversion On-Line Uninterruptible Power Supply (UPS).
- Network Port Sharing (NPS): Up to 32 AP44XXA Series Rack ATS Units can be connected using the Link A and B ports so that only one network connection is necessary.
 - An NPS guest firmware auto-update feature allows the NPS host to automatically pass a firmware update to its connected guests.

NOTICE

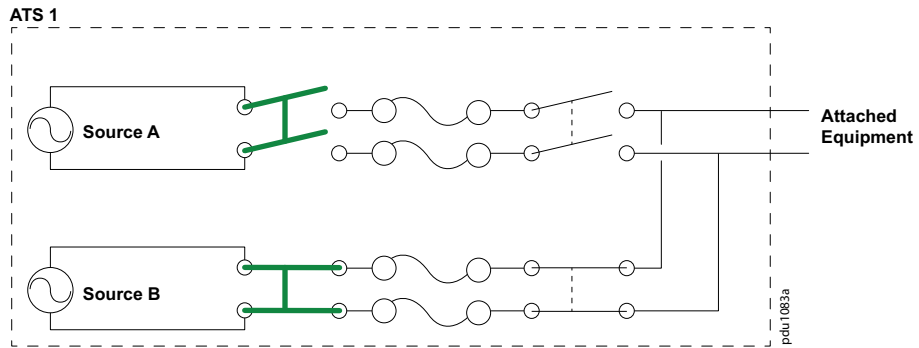
Update the firmware to enable NPS features.

See [Firmware File Transfer Methods](#), page 26 for instructions to update the firmware.

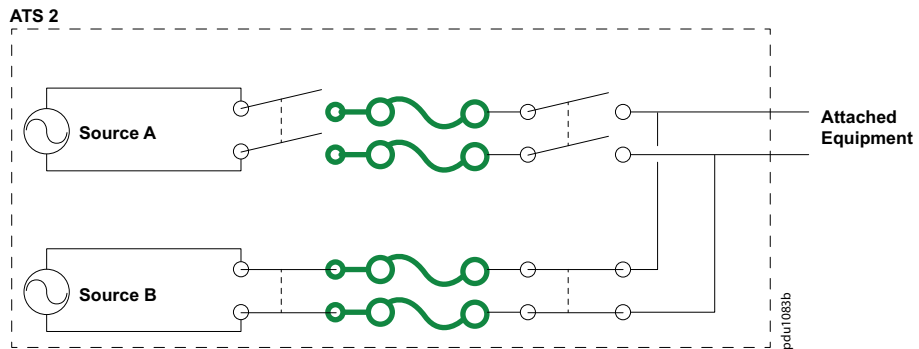
Internal Protection Measures

Rack ATS units may include the following internal protection measures:

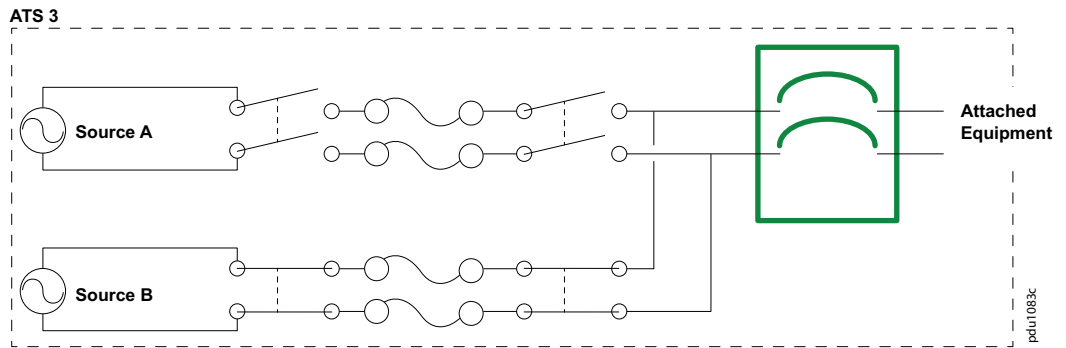
Input relays in every model open when their source is disconnected to help prevent electric backfeed from one input cord into another (ATS 1).



Two or four non-replaceable fuses (depending on the model) help to protect the Rack ATS from short circuits (ATS 2).



Some 2U models have two single- or double-pole circuit breakers to help protect against bank overloads (ATS 3).



The Rack ATS does not include power surge protection. To help protect your Rack ATS from external power surges, it is recommended that you always connect each Rack ATS source to a Double Conversion On-Line Uninterruptible Power Supply (UPS).

How Switching Works

Switching behavior is determined by several performance parameters: Line VRMS, Transfer Limits, Transfer Ranges, and Sensitivity. You can adjust these parameters so that the Rack ATS accepts power that meets the needs of your equipment (see Configuration Tab, page 132 for more details).

- **Line VRMS:** The ideal voltage range for your equipment. Acceptable line voltages vary per Rack ATS model (see the *Specification Sheet* for your Rack ATS model on www.apc.com).
- **Transfer limits:** The maximum and minimum voltages the Rack ATS will accept before switching sources. Transfer limits are meant to allow for small, acceptable surges and drops in power. Do not allow the Rack ATS to operate near the high transfer limit for long periods of time, as this can reduce the life expectancy of the Rack ATS and your equipment.
- **Transfer ranges:** Pre-defined sets of transfer limits. You can configure up to three transfer ranges, but you can enable only one transfer range at a time.
- **Sensitivity:** How long the Rack ATS waits to determine whether or not it will switch sources. High sensitivity provides extra responsiveness for delicate equipment. Low sensitivity helps to prevent excessive switching in cases of fluctuating power inputs.

NOTE: The entire switching process takes a maximum of 10 milliseconds (ms) at high sensitivity, and 12 ms at low sensitivity. (This applies to both 50 Hz and 60 Hz sources.)

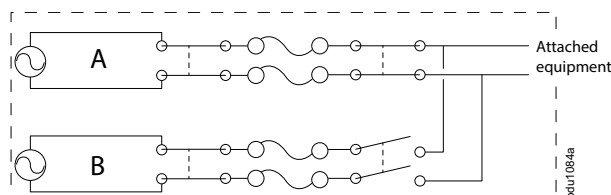
The Rack ATS constantly monitors the voltage and frequency of power coming from sources A and B. If one source begins to supply power that does not fall within the performance parameters, the Rack ATS will disqualify that source. One of two things happens next:

1. If the disqualified source *is not* in use, the Rack ATS will generate an alarm to indicate that redundancy has been lost.
2. If the disqualified source *is* in use, the Rack ATS will switch to draw power from the other available source.

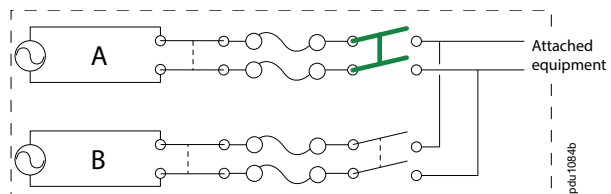
If a preferred source is set, the Rack ATS will wait 30 seconds to monitor that source. After 30 seconds, if the preferred source becomes usable again, the Rack ATS will switch back to the preferred source.

Example:

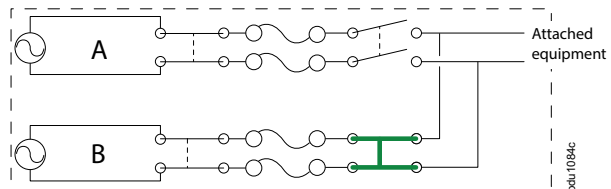
Source A is providing power to the attached equipment, while Source B is isolated from the attached equipment.



Firmware detects that Source A is out of the user-specified transfer range. The input power from Source A is removed by disengaging the relay. This allows for out-of-phase switching and significantly reduces the opportunity for relay welding. (The first relay will only open if the input voltage is too low.)



Source B relays are engaged. Source B provides power to the attached equipment.



Types of User Accounts

The Rack ATS has various levels of access (Super User, Administrator, Device User, Read-only User, and Network-only User), which are protected by user name and password requirements. Up to four users are allowed to log on to the same Rack ATS simultaneously.

NOTE: You will be prompted to enter a new password the first time you connect to the Rack ATS with the Super User account. The Administrator, Device User, Read-only User, and Network-only User accounts are disabled by default, and cannot be enabled until the Super User default password (**apc**) is changed.

- An Administrator or the Super User can use all of the menus in the Web UI and all of the commands in the CLI. Administrator user types can be deleted, but the Super User cannot be deleted. The default user name and password for the Super User or an Administrator are both **apc**.

NOTE: It is recommended that you only use the Super User account to gain initial access to the device. Use the Administrator account for other operations that require this level of access.

NOTE: The Super User or an Administrator can manage another Administrator's account (enable, disable, change password, etc).

- A Device User has read and write access to device-related screens. Administrative functions like **Session Management** under the **Security** menu and **Firewall** under **Logs** are unavailable.
- A Read-Only User has access to the same menus as a Device User, but without the ability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but disabled. The event and data logs display no button to clear the log. The default user name for this account is **readonly**, and the default password is **apc**.
- A Network-Only User (remote user) can only log on using the Web UI and CLI (Telnet or SSH). A network-only user has read/write access to network related menus only.

Watchdog Features

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 “Network Interface Restarted” event is recorded in the Event Log.

Network Interface Watchdog Mechanism

The Rack ATS implements internal watchdog mechanisms to help 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. The network interface watchdog mechanism is only enabled on a Rack ATS that discovers an active network interface connection at start-up.

Resetting the Network Timer

To help 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 the response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network and is on the same subnet. The network traffic of that computer should restart the 9.5-minute timer frequently enough to prevent the Rack ATS from restarting.

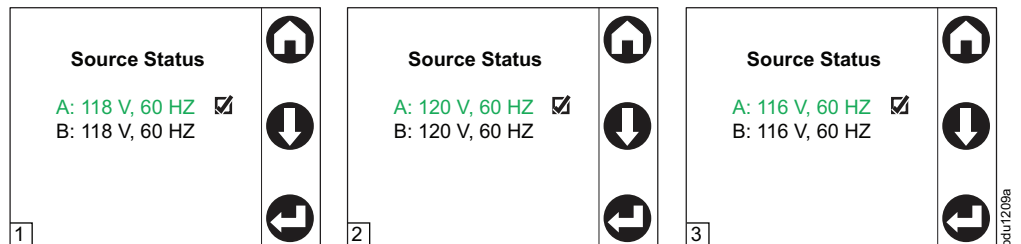
Network Port Sharing (NPS)

You can use the Network Port Sharing feature to view the status of and configure and manage up to 32 Rack ATS units using only one network connection. This is made possible by connecting the Rack ATS units using the Link A and B ports on the front panel of each unit.

NOTE: All Rack ATS units in the group must be in the AP44XXA series. The NPS host ATS compares its own firmware version with the versions found on each guest. In the event of a version difference, the host copies its firmware to the non-complying guests by means of the NPS chain.

Display ID

The display ID is a number, 1 to 32, used to uniquely identify the Rack ATS units in a group. After two or more Rack ATS units are connected to one another in an NPS group, they can be identified on the various interfaces by the use of this "Display ID". You can view this Display ID in the bottom left corner of the LCD display.



Install an NPS Group

NOTE: To reduce the possibility of communication issues, the maximum total length of cabling (Cat5e+) connecting ATS units in a group should not exceed 10 meters.

NOTE: Only one Rack ATS in an NPS group is allowed to be the host. If two host units are connected, one is automatically chosen to be the host for the NPS group. If a guest unit has an active network link, you can select that guest to become the host.

See [Configure NPS Groups](#), page 133 for more details about NPS groups.

Connect up to 32 Rack ATS units using the Link A and B ports on the front panel of each unit. You can assign specific Display IDs by powering up the units manually for the first time in the desired order (1 to 32).

1. Before powering up any of the Rack PDUs connected in a group, determine the Display ID order that you would like.
2. First power up the unit that you would like to have Display ID 1.
3. After that unit has initialized and the LCD has started displaying its screens, power on the unit that you would like to have Display ID 2.
4. Continue in the same way for the remaining units, as applicable for your setup.
5. Connect the Network port of one of the grouped Rack ATS units to a network hub or switch. This unit becomes the host for the Rack ATS group. Guest ATS data can be viewed on the host ATS. Set up network functionality for this Host Rack ATS as specified in the [Establish Network Settings](#), page 19. The host ATS will automatically discover any guest ATS Units connected through the Link A and B ports.

The Rack ATS group is now available from the host unit's IP address. If needed, you can use SNMP OID `ats5gIdentConfigModuleID` to change the NPS IDs. You can change the host unit from the **Configuration > ATS > Groups** page.

The host Rack ATS supports many features that are not supported by NPS guests. These include, but are not limited to:

- SNMP `ats5g` Group OIDs
- Initiating AOS/APP firmware updates for guest ATS units
- Time synchronization for guest ATS units
- Data logging for the guest ATS units

Firmware Upgrade with NPS

At start-up and routinely during operation, the NPS host compares its own firmware version with the versions found on each guest. In the event of a version difference, the host copies its firmware to the non-complying guests by means of the NPS chain.

NOTE: Automatic firmware upgrade is only available for AP44XXA Series Rack ATS units as this functionality requires resident firmware support in both the NPS host and guests. This functionality requires that any replacement Rack ATS units also be AP44XXA Series models to maintain correct operation of the NPS chain.

Getting Started

To start using the Rack ATS:

1. Install the Rack ATS using the *Installation and Quick Start Manual* on www.apc.com.
2. Apply power and connect to your network. Follow the directions in the *Installation Manual*.
3. Establish the network settings. See *Establish Network Settings*, page 19
4. Update the ATS firmware. See *Updating Firmware*, page 26.
5. Begin using the Rack ATS with one of the following interfaces:
 - The Display Panel. See *Front Panel Overview*, page 33.
NOTE: The front panel allows you to view Rack ATS settings, but not configure them.
 - The CLI. See *Command Line Interface*, page 40.
 - The Web UI. See *Web User Interface*, page 118.

Establish Network Settings

EcoStruxure Data Center Expert™ (DCE) provides DHCP configuration for SNMPv1 devices discovered on the DCE private network. If your Rack ATS is connected to a DCE private network, you can disregard this section and use DCE to provide an IP address through the **Private (LAN2) DHCP Discovery** tab in DCE. See your DCE documentation for details.

NOTE: You must enable SNMPv1 on the Rack ATS. Establish a local connection to the CLI (*Local Access to the CLI*, page 24) and use the `snmp` command to enable SNMPv1 (*snmp*, page 71).

About IPv4 Setup

You must define three TCP/IP settings for the Rack ATS before it can operate on the network:

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

If a default gateway is unavailable, use the IP address of a computer that is located on the same subnet as the Rack ATS and is usually running. The Rack ATS used the default gateway to test the network when traffic is very light.

NOTE: Do NOT use the loopback address (127.0.0.1) as the default gateway. Doing so disables the network connection of the Rack ATS. To enable the network connection again, you must log on using a serial connection and reset the TCP/IP settings to their defaults.

For detailed information on how to use a DHCP server to configure the TCP/IP settings on a Rack ATS, see **DHCP Response Options** under *Configure TCP/IP and Communication Settings for IPv4 and IPv6*, page 151.

About IPv6 Setup

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

TCP/IP Configuration Methods

Use one of the following methods to define the TCP/IP settings needed by the Rack ATS:

- BOOTP or DHCP server (see [DHCP and BOOTP Configuration](#), page 22).
 - NOTE:** DHCP is the default method of network configuration for the Rack ATS. Most networks are configured with a DHCP server.
- CLI (see [Local Access to the CLI](#), page 24 or [Remote Access to the CLI](#), page 24).
- Device IP Configuration Wizard (see [Device IP Configuration Utility](#), page 20).
 - NOTE:** SNMP is disabled by default, and must be enabled for the Device IP configuration Wizard to function. You can enable SNMP from the CLI. (See [Local Access to the CLI](#), page 24 for instructions to access the CLI. See [snmp](#), page 71 to enable snmp).
- You can use the .ini file to export .ini file settings from a configured Rack ATS to one or more unconfigured Rack ATS units. To do this from the Web UI, go to **Configuration > General > User Config File**. See [How to Export Configuration Settings](#), page 181 for further options and detailed instructions on how to edit the .ini file.

Device IP Configuration Utility

SNMP is disabled by default, and must be enabled for the Device IP configuration Wizard to function. You can enable SNMP from the CLI. (See [Local Access to the CLI](#), page 24 for instructions to access the CLI. See [snmp](#), page 71 to enable snmp).

The Device IP Configuration Wizard can discover Rack ATS units that do not have an IP address assigned. Once discovered, you can configure the IP address settings for the Network Management Cards (NMCs). You can also search for devices already on the network by entering an IP range to define the search. The Wizard scans the IP addresses in the defined range and discovers Rack ATS units that already have a DHCP-assigned IP address.

NOTE:

- For detailed information on the Wizard, see the FAQ article *How do I configure APC Network Management Card network settings?* (FA156064).
- To use the DHCP Option 12 (AOS 5.1.5 or higher), see the FAQ article *Which DHCP options are used when an APC Network Management Device makes a DHCPv4 request?* (FA156110).
- To find an FAQ article, go to www.apc.com/support, select **FAQS** under Resources and Tools, then enter the article number or title in the Search bar.

System Requirements

The Device IP Configuration Wizard runs on Microsoft® Windows® 2000, Windows Server® 2003, Windows Server 2012, and on 32- and 64-bit versions of Windows XP®, Windows Vista®, Windows 2008, Windows 7, Windows 8, and Windows 10 operating systems. The Device IP Configuration Wizard supports Network Management Cards that have firmware version 3.0.x or higher and is for IPv4 only.

Install the Device IP Configuration Utility

1. On www.apc.com, enter "Network Management Device IP Configuration Wizard" in the Search bar. Select the latest version of the Device IP Configuration Wizard to open its product page.
2. Download the latest version of the Device IP Configuration Wizard.
3. Extract the .zip file to your desktop, and run the executable file (*DevIPSetup.exe*).

NOTE: If you leave the **Start a Web browser when finished** option enabled, you can use **apc** for both the user name and password to access the Rack ATS through your browser.

When Installed, the Device IP configuration Wizard is available through the Windows **Start** menu options.

DHCP and BOOTP Configuration

The default TCP/IP configuration setting, **DHCP**, assumes that a properly configured DHCP server is available to provide TCP/IP settings to the Rack ATS. You can also configure the setting for BOOTP.

A user configuration (INI) file can function as a BOOTP or DHCP boot file.

After configuring the BOOTP or DHCP server, you can log into the CLI (see [Local Access to the CLI](#), page 24 for instructions) and view the IP address assigned to your Rack Monitor 250 (see [View or Configure TCP/IP settings in the CLI](#), page 25 for instructions.)

DHCP server configuration

You can use an RFC2131/RFC2132-compliant DHCP server to configure the TCP/IP settings for the Rack ATS.

1. The Rack ATS sends out a DHCP request that uses the following to identify itself:
 - A Vendor Class Identifier (APC by default)
 - A Client Identifier (by default, the MAC address of the Rack ATS)
 - A User Class Identifier (by default, the identification of the application firmware installed on the Rack ATS)
 - A Host Name (by default, apcXXYYZZ with XXYYZZ being the last six digits of the Rack ATS serial number). This is known as DHCP Option 12.
2. A properly configured DHCP server responds with a DHCP offer that includes all the settings that the Rack ATS needs for network communication. The DHCP offer also includes the Vendor Specific Information option (DHCP option 43). The Rack ATS can be configured to ignore DHCP offers that do not encapsulate the APC cookie in DHCP option 43 using the following hexadecimal format. (The Rack ATS does not require this cookie by default.)

Option 43 = 01 04 31 41 50 43

- The first byte (01) is the code.
- The second byte (04) is the length.
- The remaining bytes (31 41 50 43) are the APC cookie. See your DHCP server documentation to add code to the Vendor Specific Information option.

NOTE: By selecting the **Require vendor specific cookie to accept DHCP Address** check box in the Web UI, you can require the DHCP server to provide an "APC" cookie, which supplies information to the Rack ATS.

For additional information on supported DHCP options, see [Configure TCP/IP and Communication Settings for IPv4 and IPv6](#), page 151.

BOOTP server configuration

For the Rack ATS to use a BOOTP server to configure its TCP/IP settings, it must find a properly configured RFC951-compliant BOOTP server.

1. In the BOOTPTAB file of the BOOTP server, enter the Rack ATS MAC address, IP address, subnet mask, and default gateway, and, optionally, a bootup file name. Look for the MAC address on the bottom of the Rack ATS.
2. Use a serial connection to access the CLI, then enter `-b <bootp>` to enable BOOTP. The default username and password are both **apc**.

See [Local Access to the CLI](#), page 24 for detailed instructions to access the CLI.

3. Enter `-Y` to reboot the Rack ATS.

When the Rack ATS reboots, the BOOTP server provides it with the TCP/IP settings.

- If you specified a bootup file name, the Rack ATS attempts to transfer that file from the BOOTP server using TFTP or FTP. The Rack ATS assumes all settings specified in the bootup file.
- If you did not specify a bootup file name, you can configure the other settings of the Rack ATS remotely through its Web UI or CLI. The default user name and password are **apc** for both interfaces. To create a bootup file, see your BOOTP server documentation.

Local Access to the CLI

For local access, use a computer that connects to the Rack ATS through the Console port to access the CLI.

NOTE: This procedure assumes that a Virtual COM Port (VCP) driver is installed on the computer. If needed, download and install the VCP driver for your operating system from ftdichip.com.

1. Open an application to view the COM ports for the computer, according to the instructions for your operating system. (In Windows operating systems, you can view ports in the Device Manager.)
2. Use a Micro USB cable to connect the Console port of the Rack ATS to a USB port on the computer.

A newly occupied serial COM port should appear in the port-viewing application. Take note of the port number or re-assign the port as needed.

3. Run a terminal program (e.g., TeraTerm or PuTTY) and configure the selected serial COM port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Use the port to make a serial connection to the Rack ATS.
4. Press ENTER up to three times to display the User Name prompt. Then enter the user name and password.

By default, the user name and password for the Super User are both **apc**. If this is your first log on, you will be prompted to change the default password. It is recommended that you use a strong password which conforms with your company's password requirements.

If you are configuring your network settings for the first time, see [View or Configure TCP/IP settings in the CLI](#), page 25 to complete the configuration.

Remote Access to the CLI

From any computer on the same network as the Rack ATS, you can use ARP and Ping to assign an IP address to the Rack ATS, and then use SSH or Telnet to access the CLI of that Rack ATS and configure the other TCP/IP settings. By default, SSH is enabled by and Telnet is disabled.

NOTE: After the IP address of the Rack ATS is configured, you can access the Rack ATS using SSH or Telnet, without first using ARP and Ping, but SSH is required for initial CLI configuration. You can use the **console** command to enable or disable SSH or Telnet. If needed, you can also use the Web UI to enable or disable SSH or Telnet.

1. Use ARP to define an IP address for the Rack ATS and use the MAC address of the Rack ATS in the ARP command. For example, to define an IP address of 156.205.14.141 for a Rack ATS that has a MAC address of 00 c0 b7 63 9f 67, use one of the following commands:
 - Windows command format:
`arp -s 156.205.14.141 00-c0-b7-63-9f-67`
 - LINUX command format: `arp -s 156.205.14.141 00:c0:b7:63:9f:67`

NOTE: The MAC address can be found on the bottom of the Rack ATS.
2. Use Ping with a size of 113 bytes to assign the IP address defined by the ARP command. For example:
 - Windows command format: `ping 156.205.14.141 -l 113`
 - LINUX command format: `ping 156.205.14.141 -s 113`
3. Use SSH or Telnet to access the Rack ATS at its newly assigned IP address. (For example: `telnet 156.205.14.141`) Use **apc** for both the user name and password.

See [View or Configure TCP/IP settings in the CLI](#), page 25 to finish the configuration.

View or Configure TCP/IP settings in the CLI

To view an IP address assigned via DHCP or BOOTP:

1. Log on to the CLI.
2. Enter `tcpip` to view the IPv4 address.
Enter `tcpip6` to view the IPv6 address.

To assign TCP/IPv4 settings manually:

1. Log on to the CLI.
2. Contact your network administrator to obtain the IP address, subnet mask, and default gateway for the Rack ATS.
3. Use these three commands to configure network settings. (Text in italics indicates a variable.)

```
tcpip -i yourIPAddress
tcpip -s yourSubnetMask
tcpip -g yourDefaultGateway
```

For each variable, type a numeric value that has the format `xxx.xxx.xxx.xxx`. For example, to set a system IP address of 156.205.14.141, type the following command and press ENTER:

```
tcpip -i 156.205.14.141
```

NOTE: You can also enter all three command options on the same line:

```
tcpip -i yourIPAddress -s yourSubnetMask tcpip -g
yourDefaultGateway
```

4. Type `exit`, and then press ENTER. The Rack ATS restarts to apply the changes.

To assign TCP/IPv6 settings manually:

1. Log on to the CLI.
2. Contact your network administrator to obtain the IP address, subnet mask, and default gateway for the Rack ATS.
3. Use these three commands to configure network settings. (Text in italics indicates a variable.)

```
tcpip6 -man enable
tcpip6 -i yourIPAddress
tcpip -g yourDefaultGateway
```

NOTE: For the IP address and Default Gateway, type a numeric value that has the format `xxxx:xxxx:xxxx:xxxx/xx`.

```
tcpip -d6 DHCPv6 mode
```

Where the DHCPv6 mode can be `router`, `statefull`, `stateless`, or `never`.

4. Type `exit`, and then press ENTER. The Rack ATS restarts to apply the changes.

For more detailed information on `tcpip` commands, see `tcpip`, page 79 or `tcpip6`, page 80.

.ini File Utility

You can use the .ini file export utility to export .ini file settings from a configured Rack ATS to an unconfigured Rack ATS. For more information, see **Create and Import Settings with the Config File**.

Updating Firmware

When you update the firmware on the Rack ATS:

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

Keeping the firmware versions consistent across your network helps ensure that all Rack ATS units support the same features in the same manner. Here, upgrading simply means placing the firmware file on the Rack ATS; there is no installation required. Check regularly on www.apc.com for any new updates.

Firmware File Transfer Methods

Obtain the free, latest firmware version from the APC website. Enter the model number for your equipment in the Search bar of the website's home page (www.apc.com). Select the desired product from the search results to open that product page. Select the Software & Firmware tab on the product page to view and download any available firmware for that product.

To update the firmware of one or more Rack ATS units, use one of these five methods:

- On a Windows operating system, use the **Firmware Update Utility** downloaded from www.apc.com.
- On any supported operating system, use **FTP** or **SCP** to transfer the individual AOS and application firmware modules.
- Use a **USB drive** to transfer the individual firmware modules from your computer.
- For updates to multiple Rack ATS units, see [How To Update Multiple Rack ATS Units](#), page 29.

Use the Firmware Update Utility

This Firmware Update Utility is part of the firmware update package available on www.apc.com. (Never use an Update Utility designated for one product to update the firmware of another product).

Use the Utility for updates on Windows-based systems

On any supported Windows operating system, the Firmware Update Utility automates the firmware transfer.

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

Use the Utility for manual updates, primarily on Linux

On non-Windows operating systems, the Firmware Update Utility extracts the firmware file, but does not upgrade the Rack ATS.

To extract the firmware files:

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

See *Firmware File Transfer Methods*, page 26 for the different upgrade methods after extraction.

Manually Update One Rack ATS with FTP or SCP

FTP

To use FTP to update a Rack ATS over the network:

- The Rack ATS must be on the network with its system IP, subnet mask, and default gateway configured.
- The FTP server must be enabled at the Rack ATS. You can enable the FTP server under **Configuration > Network > FTP Server**.

To transfer the files:

1. Extract the firmware file.
2. At a computer on the network, open a command prompt window. Go to the directory that contains the firmware files, and list the files:

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

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

3. Open an FTP client session: `C:\apc>ftp`
4. Type `open` with the IP address of the Rack ATS, and press ENTER. If the **port** setting for the FTP Server has changed from its default of **21**, you must use the non-default value in the FTP command.

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

```
ftp> open 150.250.6.10 21000
```

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

5. Log on as the Super User (**apc** is the default user name and password) or Administrator.
6. Send the .nmc3 file:

```
put apc_hw21_ats5g_0-0-0.nmc3
```

(where 0-0-0 is the firmware version number).

7. When FTP confirms the transfer, type `quit` to close the session.

SCP

To use Secure CoPy (SCP) to update firmware for the Rack ATS, follow these steps (this procedure assumes bootmon does not need upgrading, it is always necessary to update the other two though):

NOTE: As SCP is part of SSH, enabling SSH also enables SCP. SSH is enabled by default.

1. Locate the firmware file.
2. Use an SCP command line to transfer the firmware to the Rack ATS. The following example uses 0-0-0 to represent the version number of the firmware:

```
scp -c <cipher> apc_hw21_ats5g_0-0-0.nmc3
```

```
apc@158.205.6.185:apc_hw21_ats5g_0-0-0.nmc3
```

NOTE: This SCP command is for OpenSSH. The command may differ depending on the SSH tool used. `<cipher>` can be either `aes256-cbc` or `3des-cbc`.

Use a USB Drive To Transfer and Update Files

Use a USB drive to transfer and update files. Before starting the transfer, make sure the USB drive is formatted in FAT32.

1. Create a folder named **apcfirm** on the USB flash drive.
2. Use a text editor to create a file named **nmc3.rcf**. (The file extension must be .rcf, not .txt for example.)
Add only the following text to the file: `NMC3=app.nmc3`
Save the file to the **apcfirm** folder.
3. Download the firmware update files and unzip them. Copy the **app.nmc3** firmware file into the **apcfirm** folder.
4. Insert the flash drive into a USB port on your Rack ATS.
5. Use the Web UI, the CLI, or the **Reset** button on the front of the Rack ATS to reboot the management interface. Wait for the reboot to finish.
6. Check that the update was completed successfully using the procedures in *Verifying Upgrades and Updates*, page 30.

How To Update Multiple Rack ATS Units

Use one of these methods:

- **Firmware Update Utility:** Use this for multiple firmware updates in IPv4 if you have Windows. The Utility records all update steps in a log as a good reference to validate the update. The Utility is included with your firmware download. For more information, see
 - Use the Firmware Update Utility, page 27, or
 - FAQ article FA156099: *How do I perform a mass firmware upgrade on APC network enabled products?* on www.apc.com.
- **Export configuration settings:** You can create batch files and use the .ini file utility to retrieve configuration settings from multiple Rack ATS and export them to other Rack ATS Units. For more information on how to download the .ini file utility,
 - See FAQ article FA156117: *How can I mass configure a Network Management Card (NMC) or NMC embedded product?* on www.apc.com, and
 - Read the release notes (release notes are included with the utility file).
- **Use FTP or SCP to update multiple Rack ATS units:** To update multiple Rack ATS Units using an FTP client or using SCP, write a script which automatically performs the procedure.

NOTE: To find an FAQ article, go to www.apc.com/support, select **FAQS** under Resources and Tools, then enter the article number or title in the Search bar.

Firmware Upgrade with NPS

At start-up and routinely during operation, the NPS host compares its own firmware version with the versions found on each guest. In the event of a version difference, the host copies its firmware to the non-complying guests by means of the NPS chain.

NOTE: Automatic firmware upgrade is only available for AP44XXA Series Rack ATS units as this functionality requires resident firmware support in both the NPS host and guests. This functionality requires that any replacement Rack ATS units also be AP44XXA Series models to maintain correct operation of the NPS chain.

Verifying Upgrades and Updates

Verify the Success Or Failure of the Transfer

To verify whether a firmware update succeeded, use the `xferStatus` command in the CLI to view the last transfer result, or use an SNMP GET to the `mfiletransferStatusLastTransferResult` OID.

Last Transfer Result Codes

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

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

Verify the Version of Installed Firmware

Path: About > Network

Use this Web UI page to verify the version of the updated firmware. You can also use an SNMP GET to the MIB II `sysDescr` OID, or use the `aboutATS` command in the CLI.

Network Management with Other Applications

These applications and utilities work with a Rack ATS that is connected to the network.

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

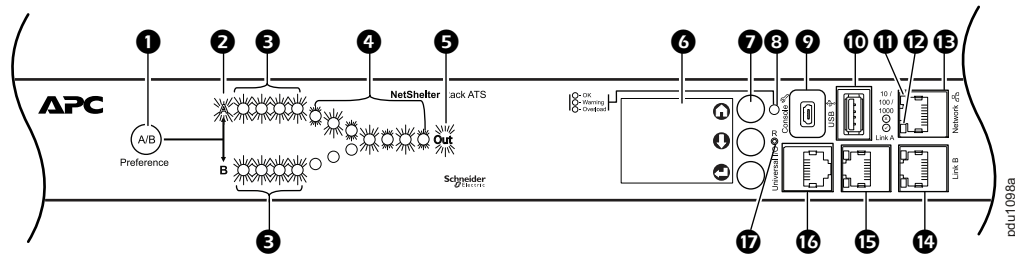
Recover from a Lost Password

Resetting the Rack ATS will reset the unit to its default configuration. Export the .ini file after configuring your Rack ATS and keep it in a safe place. If you have this file saved, you will be able to retrieve your configuration after a lost password event.

You can use any secure interface to complete the recovery process. This includes the local CLI by serial connection, remote CLI by SSH, or Web by HTTPS, all of which are covered in this manual.

1. Hold down the **Reset** button for 20–25 seconds, ensuring the Status LED is flashing green during this time. When the Status LED changes to orange, release the **Reset** button to allow the Rack ATS to complete its reboot process.
2. Access the Rack ATS through one of the secure interfaces to set your custom password and configure the device. After resetting the device to defaults, the first log in can be completed with the default user name **apc** and password **apc**.

Front Panel Overview



Your Rack ATS is configured so the display backlight turns off after 10 minutes of inactivity. Press any display navigation button to illuminate the backlight.

Item	Function
1 Preference A/B Button	Press to set a preferred power source: the first press sets Source A, the second press sets Source B, and the third press sets no preference.
2 Source A and B LEDs	Indicates preferred power source. If no source is preferred, both LEDs are illuminated. You can also see the Preferred Source on the LCD Display.
3 Input Connector LEDs	Provides information about input voltage from each source. If the RMS input voltage and measured frequency are within the selected tolerance range, the corresponding LED will be illuminated. In a normal operating condition (full source redundancy) both sets of LEDs are illuminated.
4 Output Connector LEDs	Indicates which source is being used for the output (only one path will be illuminated at any time). Together, the Source Preference LEDs, the Connector LEDs, and the Output LED show the power flow through the Rack ATS.
5 Output LED	Shows that voltage is available at the output for the Rack ATS.
6 LCD Display	View Rack ATS status, settings, and product information.
7 Display navigation buttons	On the LCD Display, icons indicate the purpose of adjacent buttons. 🏠 Home: Press to move through monitor screens or return to monitor screens from sub-menus. ⬇️ Down: Press to move through monitor screens or menu items. ⏏️ Select: Press to select menu items or navigate to the main menu from monitor screens.
8 Device Status LED	See Device Status LED, page 34.
9 Console port	Connect your computer to the Rack ATS for local access to the CLI. Use a Micro USB cable (not provided).
10 USB port	Use USB drives for firmware upgrades.
11 10/100/1000 Status LED	See 10/100/1000 Status LED, page 34.
12 Network status LED	See Network Status LED, page 34.
13 Network Port	Connects the Rack ATS to the network using a network cable (not provided).
14 Link A and Link B ports	For use with the Network Port Sharing feature to connect multiple Rack ATS units to one another. Both ports can be used as the In or Out port. A terminator is not required.
15 Universal I/O	Port for connecting an optional APC Temperature Sensor (AP9335T) or an optional APC Temperature/ Humidity Sensor (AP9335TH).
17 Reset switch	Restarts the network and serial communication.

Device Status LED

This LED identifies the alarm status for the Rack ATS.

Alarms may be related to the ATS hardware (for example, load threshold violations and redundancy loss) or environmental monitoring (for example, temperature threshold violations and sensor communication alarms).

Condition	Description
Solid Green	No Critical or Warning alarms are present.
Solid Yellow	At least one Warning alarm is present, but no Critical alarms are present.
Flashing Red	At least one Critical alarm is present.

Network Status LED

This LED indicates the network status.





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. ¹
Solid orange	A hardware failure has been detected in the Rack ATS.
Flashing orange	The Rack ATS is making BOOTP requests.
Flashing orange and green (alternating)	The Rack ATS is making DHCP requests.
¹ If you do not use a BOOTP or a DHCP server, see Local Access to the CLI , page 40 or Remote Access to the CLI , page 24 to configure the TCP/IP settings.	


10/100/1000 Status LED

This LED indicates the network status of the Rack ATS.

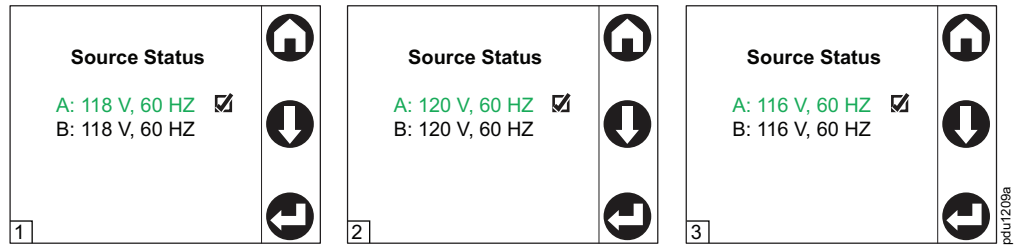
Condition	Description
Off	One or more of the following situations exists: <ul style="list-style-type: none"> The Rack ATS is not receiving input power. The cable that connects the Rack ATS to the network is disconnected or defective. The device that connects the Rack ATS to the network is turned off. The Rack ATS itself is not operating properly. It may need to be repaired or replaced. Contact Customer Support.
Solid Yellow	The Rack ATS is connected to a network operating at 10–100 Megabits per second (Mbps).
Solid Green	The Rack ATS is connected to a network operating at 1000 Mbps.
Flashing Yellow	The Rack ATS is receiving or transmitting data packets at 10–100 Mbps.
Flashing Green	The Rack ATS is receiving or transmitting data packets at 1000 Mbps.

LCD Display Screens

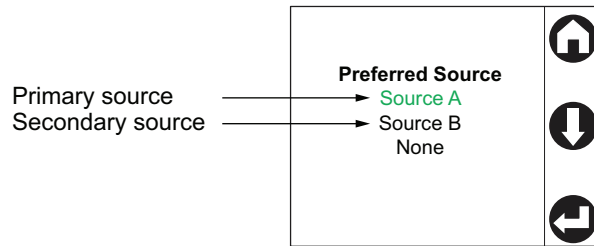
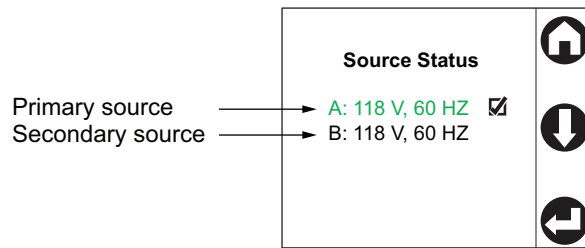
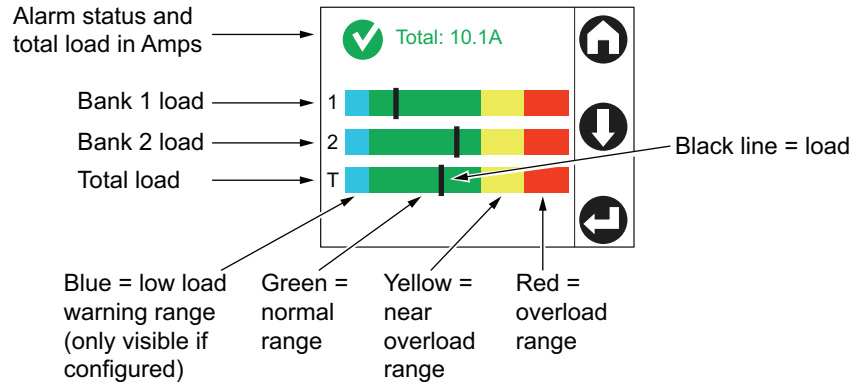
The front panel LCD Display automatically rotates between four default screens. You can press Home  or Down  to move through these screens manually. You can press Select  to go to the main menu or select menu items. Down  allows you to move through menu items and menu screens.

After 30 seconds without activity, the LCD display will revert to the default screens. You can also press Home  to return to the default screens.

If the unit is part of an NPS group, the NPS ID appears in the bottom-left corner of the LCD Display.

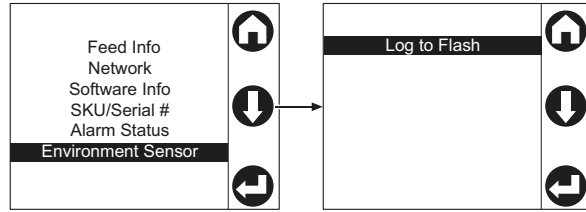


Default Screens

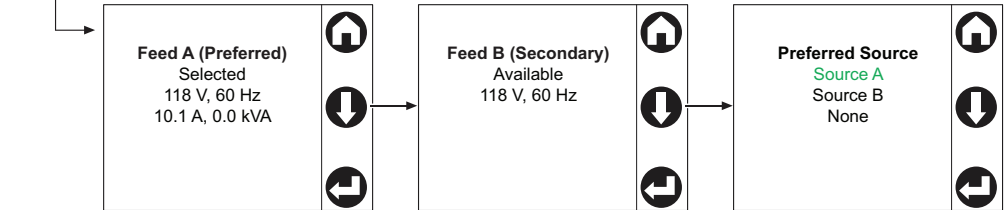


NOTE: The number of banks varies by model.

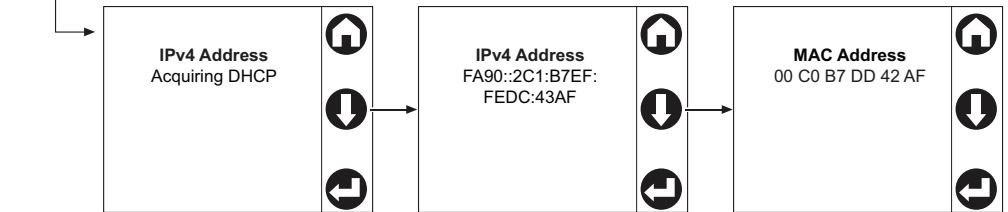
Menu screens



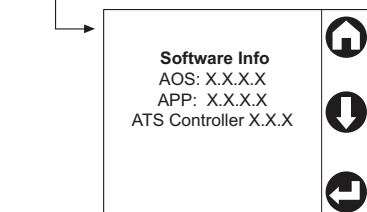
Feed Info View information for each power source (Feed A and Feed B), or view the Preferred Source (in green text).



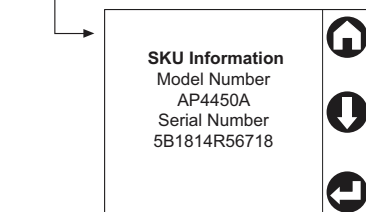
Network View the IPv4 Address, the IPv6 Address, or the MAC Address.



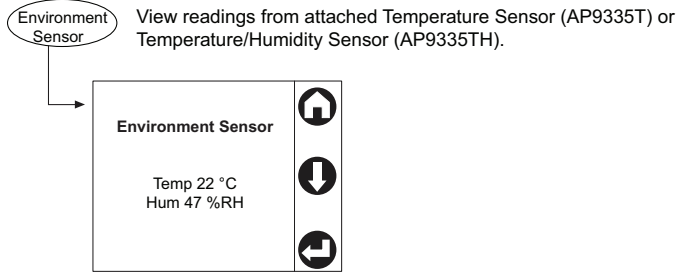
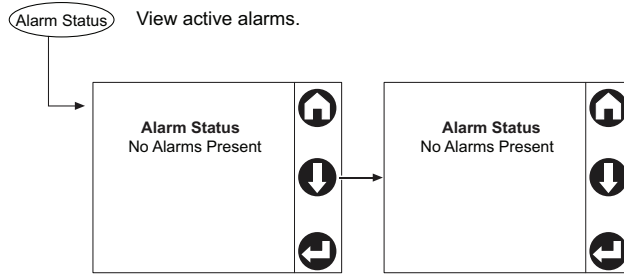
Software info View the current software version for each firmware module.



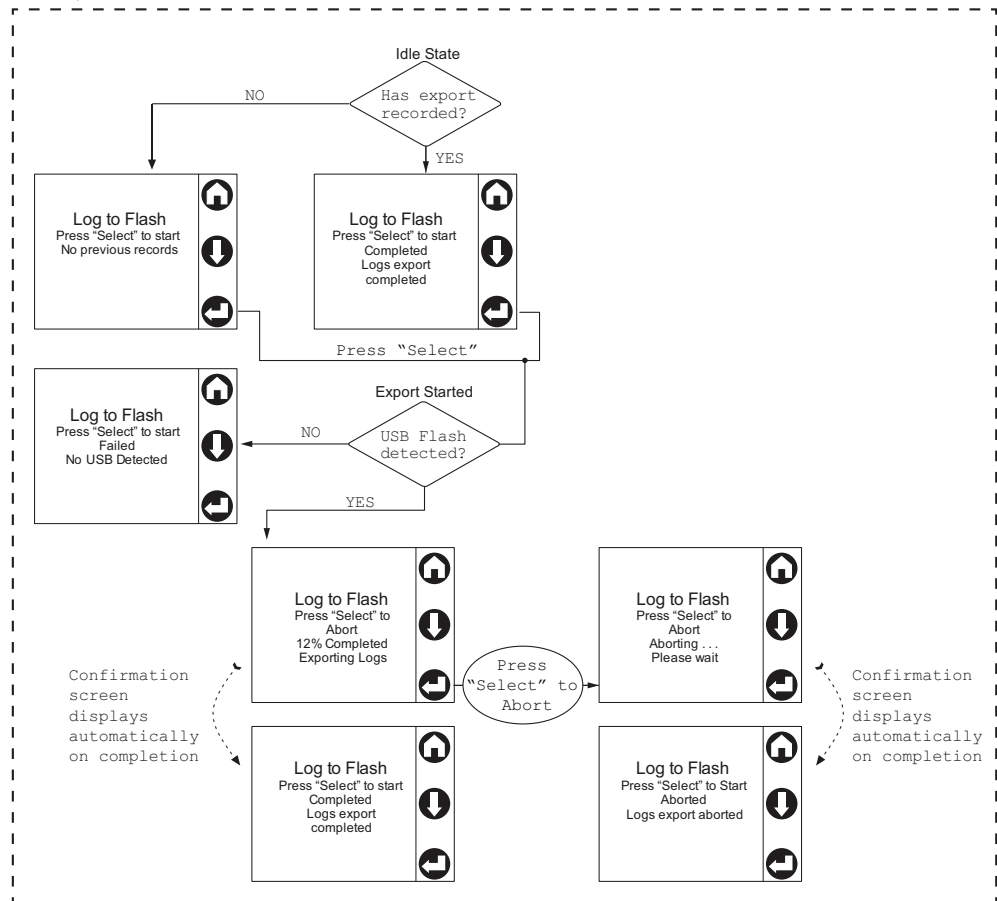
SKU/Serial# View the model and serial number for your Rack ATS.



peku1210a



Log to Flash Insert a USB drive to the USB port to download compressed log files. Extract the files to your computer to view the logs.



Alarm Status Indicators

When an alarm is generated, alarm status indicators show the level of the alarm (Warning or Critical).

No Alarm screens	Warning Alarm (Low Load and Near Overload) screens	Critical Alarm (Overload) screens
<p>Feed A (Preferred) Selected 118 V, 60 Hz 10.1 A, 0.0 kVA</p>	<p>Active Alarms: 1</p> <p>Feed A (Preferred) Selected 118 V, 60 Hz 10.1 A, 0.0 kVA</p>	<p>Active Alarms: 1</p> <p>Feed A (Preferred) Selected 118 V, 60 Hz 10.1 A, 0.0 kVA</p>
<p>Alarm Status No Alarms Present</p>	<p>Alarm Status 1 Warning Alarm</p>	<p>Alarm Status 1 Critical Alarm</p>

pd1408594

Command Line Interface

You can use the Command Line Interface (CLI) to configure, manage, and monitor the status of the Rack ATS (and any connected Rack ATS units if using the Network Port Sharing feature). Additionally, the CLI enables you to create scripts for automated operation. You can configure all parameters of a Rack ATS (including those for which there are not specific CLI commands) by using the CLI to transfer an INI file to the Rack ATS. The CLI uses XMODEM to perform the transfer. However, you cannot read the current INI file through XMODEM.

Log On to the CLI

To access the CLI, you can use either a local (serial) connection or a remote (Telnet or SSH) connection with a computer on the same network as the Rack ATS.

Local Access to the CLI

For local access, use a computer that connects to the Rack ATS through the Console port to access the CLI.

NOTE: This procedure assumes that a Virtual COM Port (VCP) driver is installed on the computer. If needed, download and install the VCP driver for your operating system from ftdichip.com.

1. Open an application to view the COM ports for the computer, according to the instructions for your operating system. (In Windows operating systems, you can view ports in the Device Manager.)
2. Use a Micro USB cable to connect the Console port of the Rack ATS to a USB port on the computer.
A newly occupied serial COM port should appear in the port-viewing application. Take note of the port number or re-assign the port as needed.
3. Run a terminal program (e.g., TeraTerm or PuTTY) and configure the selected serial COM port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control. Use the port to make a serial connection to the Rack ATS.
4. Press ENTER up to three times to display the User Name prompt. Then enter the user name and password.

By default, the user name and password for the Super User are both **apc**. If this is your first log on, you will be prompted to change the default password. It is recommended that you use a strong password which conforms with your company's password requirements.

If you are configuring your network settings for the first time, see [View or Configure TCP/IP settings in the CLI](#), page 25 to complete the configuration.

Remote Access to the CLI

You can choose to access the CLI through Telnet and/or SSH. SSH is enabled by default. You can use the `console` command to enable or disable either Telnet or SSH. If needed, you can also use the Web UI (under **Configuration > Network > Console > Access**) to enable or disable Telnet or SSH.

Telnet for Basic Access

Telnet provides the basic security measure of authentication by user name and password, but not the high-security benefits of encryption. Telnet is disabled by default.

To access the CLI via Telnet:

1. At a command prompt, type `telnet` and the 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. (These are commands for general use; some clients do not allow you to specify the port as an argument and some types of Linux might require extra commands).
2. Enter the user name and password. If you cannot remember your user name or password, see the procedure to *Recover from a Lost Password*, page 32.

SSH for High-security Access

If you use the higher security of SSL/TLS for the Web UI, use SSH for access to the CLI. SSH encrypts user names, passwords, and transmitted data. The interface, user accounts, and user access rights are the same whether you access the CLI through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer. See the *Security Handbook* on www.apc.com for more information on configuring and using SSH. SSH is enabled by default.

About the Main Screen

The following screen is displayed when you log on to the CLI of a Rack ATS.

```

Schneider Electric                               Network Management Card AOS           vx.x.x
(c) Copyright 2022 All Rights Reserved           ATS5G APP                               vx.x.x
-----
Name      : Test Lab                            Date       : 3/12/22
Contact   : Don Adams                           Time       : 5:58:30
Location  : Building 3                          User       : Administrator
Up Time   : 0 Days 21 Hours 21 Minutes          Stat      : P+ N4+ N6+ A+
-----
IPv4      : Enabled                             IPv6      : Enabled
Ping response : Enabled
-----
HTTP      : Disabled                           HTTPS     : Enabled
FTP       : Disabled                           Telnet    : Disabled
SSH/SCP   : Enabled                             SNMPv1    : Disabled
SNMPv3    : Disabled
-----
Super User : Enabled                           RADIUS    : Disabled
Administrator : Disabled                       Device User : Disabled
Read-only User : Disabled                       Network-Only User : Disabled

Type ? For command listing
Use tcpip for IP address (-i), subnet (-s), and gateway (-g)

apc >

```

- Two fields identify the operating system (AOS) and application (APP) firmware versions. The application firmware name identifies the type of device that connects to the network (for example, a Rack ATS).

```

Network Management Card AOS           vx.x.x
ATS4g APP                             vx.x.x

```

- Three fields identify the system name, contact person, and location of the Rack ATS.

```

Name      Test Lab
Contact   Don Adams
Location  : Building 3

```

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

```

Up Time: 0 Days, 21 Hours, 21 Minutes

```

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

```
Date: 11/2/2021
Time: 09:06:45
```

- The `User` field identifies whether you logged in through the **Super User**, **Administrator**, **Device User**, **Read-Only**, or **Network-Only** account.

```
User: Administrator
```

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

```
Stat: P+ N4+ N6+ A+
```

P+	The APC Operating System (AOS) is functioning properly.
----	---

IPv4 only	IPv6 only	IPv4 and IPv6*	Description
N+	N+	N4+ N6+	The network is functioning properly.
N?	N6?	N4? N6?	A BOOTP request cycle is in progress.
N-	N6-	N4- N6-	The Rack ATS failed to connect to the network.
N!	N6!	N4! N6!	Another device is using the Rack ATS IP address.

* The N4 and N6 values can be different from one another: you could, for example, have N4- N6+.

A+	The application is functioning properly.
A-	The application has a bad checksum.
A?	The application is initializing.
A!	The application is not compatible with the AOS.

NOTE: If P+ is not displayed, contact the APC Customer Care Center at www.apc.com/support.

- The remaining fields show which protocols and user accounts are enabled.

Using the CLI

At the CLI, you can use commands to configure the Rack ATS. To use a command, type the command and press ENTER. Commands and arguments are valid in lowercase, uppercase, or mixed case. Options are case-sensitive.

While using the CLI, you can also do the following:

- Type `help` or `?` and press ENTER to view a list of available commands, based on your account type.
- To obtain information about the purpose and syntax of a specified command, type the command, a space, and `help` or `?`. For example, to view RADIUS configuration options, type:
`radius ?` or `radius help`
- Press the UP arrow key to view the command that was entered most recently in the session. Use the UP and DOWN arrow keys to scroll through a list of up to ten previous commands.
- Type at least one letter of a command and press the TAB key to scroll through a list of valid commands that match the text you have typed in the command line.
- Type `bye`, `exit` or `quit` to close the connection to the CLI.

Command Syntax

Item	Description
-	Options are preceded by a hyphen.
< >	Definitions of options are enclosed in angle brackets. For example: <code>-dp <device password></code>
[]	If a command accepts multiple options or an option accepts mutually exclusive arguments, the values may be enclosed in brackets.
	A vertical line between items enclosed in brackets or angle brackets indicates that the items are mutually exclusive. You must use one of the items.

Example of a command that supports multiple options:

```
ftp [-p <port number>] [-S <enable | disable>]
```

In this example, the `ftp` command accepts the option `-p`, which defines the port number, and the option `-S`, which enables or disables the FTP feature.

To change the FTP port number to 5010, and enable FTP:

1. Enter the `ftp` command, the port option, and the argument 5010:
`ftp -p 5010`
2. After the first command succeeds, enter the `ftp` command, the enable/disable option, and the `enable` selection:
`ftp -S enable`

Example of a command that accepts mutually exclusive arguments for an option:

```
alarmcount -p [all | warning | critical]
```

In this example, the option `-p` accepts only three arguments: `all`, `warning`, or `critical`. For example, to view the number of active critical alarms, enter `alarmcount -p critical`

The command will not succeed if you enter an argument that is not specified.

Command Response Codes

The command response codes enable scripted operations to detect error conditions reliably without having to match error message text.

The CLI reports all command operations with the following format:

```
E [0-9] [0-9] [0-9] : Error message
```

Code	Message
E000	Success
E001	Successfully Issued
E002	Reboot required for change to take effect
E100	Command failed
E101	Command not found
E102	Parameter error (reported when there is any problem with the arguments supplied to the command: too few, too many, wrong type, etc.)
E103	Command Line Error
E104	User Level Denial
E105	Command Prefill
E106	Data Not Available
E107	Serial Communications Lost
E108	EAPoL disabled due to invalid/encrypted certificate
E200	Input error (only reported when an error occurs during the execution of a command)
E201	No Response (reported when a sensor fails to respond)
E206	Invalid value
E213	Device busy or lost communication. Please try again.

Prompting for User Input during Command Execution

Certain commands require additional user input (for example, transfer .ini prompting for baud rate). There is a fixed timeout period of one minute for such prompts. If you do not enter any text within the timeout period, then the command will print `E100: Command Failed` and the command prompt will display again.

Command Editing

The Backspace key is the only editing function available during command entry. The Backspace key will delete the last character of the command string you are currently entering.

History

The CLI implements a command history buffer recalling the 10 previous commands. You can navigate backwards and forwards through entered commands using the Up and Down arrow keys respectively.

Auto Completion

The CLI supports command auto-completion. If you enter a partial command, you can press the Tab key to complete the command with the first available matched command. If no match exists, the system does not complete the command.

Additional presses of the Tab key will select the next available command match. Once all available commands have been scrolled through, the original, partially entered command displays.

Delimiter

The CLI uses (ASCII 0x20) as the delimiter between commands and arguments. Extra white space between commands and arguments is ignored.

All fields in command responses are delimited with commas for efficient parsing.

Options and Arguments Inputs

If you enter a command with *no options* and *no arguments*, the current value of all options available is returned.

If you enter a command with an option and *no arguments*, only the current value of that option is returned.

If you enter a command followed by a question mark (?) or `help`, help text that explains the command is returned.

```
<space> ::= (" " | multiple" ")
<valid letter_number> ::= (a-z | A-Z | 0-9)
<string> ::= (1 - 64 consecutive printable valid ASCII characters
[ranging from hex 0x20 to 0x7E inclusive] )
```

NOTE: If the string includes a blank, the entire string **MUST** be surrounded by quotes(" ").

```
<option> ::= "-" (<valid letter_number> | <valid letter_number> <valid
letter_number>)
```

```
<argument> ::= <helpArg> | <alarmcountArg> | <bootArg> | <cdArg> |
<consoleArg> | <dateArg> | <deleteArg> | <ftpArg> | <pingArg> |
<portspeedArg> | <promptArg> | <radiusArg> | <resettodefArg> |
<systemArg> | <tcpipArg> | <userArg> | <webArg> | <string>
```

```
<optionArg> ::= <option> <argument>
```

Response Format and Message Codes

All CLI commands will issue the following:

```
<three digit response code>: <response message>
```

If applicable, the command will also issue `<cr><lf>` and the output of the command.

Successful command operations have a response code of less than 100. Any response code of 100 or greater indicates a failure of some type.

```
E[0-9][0-9][0-9]: Error message
```

Example:

```
E000: Success
```

(If applicable, the output of the command is also included.)

Network Management Card Command Descriptions

? or help

Access: Super User, Administrator, Device User, Read Only

Description: View a list of all the CLI commands available to your account type. To view help text for a specific command, type the command followed by a question mark.

Parameters: [<command>]

Example 1:

```
apc> ?
System Commands:
-----
?          about    alarmcount  boot        bye         cd
clrrst    console  date        delete     dir         dns
eapol     email    eventlog    exit       firewall    format
ftp       help     lang        lastrst    ledblink    logzip
netstat   ntp      ping        portspeed  prompt     pwd
quit      radius   reboot     resetToDef session     smtp
snmp      snmptrap snmpv3      ssh        ssl         system
tcpip     tcpip6   user        userdflt   web         whoami
wifi      xferINI  xferstatus

Device Commands:
-----
aboutATS  atsMeasure  atsStatus  freqDeviat  even-
tCounts   frontPanel
humAlGen  humLow      humMin     humHyst     humReading  humStatus
lcd       lcdBlink   lineVRMS   phLowLoad   phNearOver  phOverLoad
phPeakLoad  phReading  prodInfo   sensorName  sourceA-
Name      sourceBName
sourcePref  tempAlGen  tempHigh   tempMax     tempHyst    tempPeak
tempReading  tempAtatus vMediumLmt vNarrowLmt vSensitvty vWideLmt
vXferRange  logToFlash
```

NOTE: Available device commands depend on your Rack ATS model and connected sensors.

Example 2:

```
apc> help boot
```

```
Usage: boot -- Configuration Options
```

```
boot  [-b <dhcpBootp | dhcp | bootp | manual>] (Boot Mode)
      [-a <remainDhcpBootp | gotoDhcpOrBootp>] (After IP Assignment)
      [-o <stop | prevSettings>] (On Retry Fail)
      [-c <enable | disable>] (Require DHCP Cookie)
      [-s <retry then stop #>] (Note: 0 = never)
      [-f <retry then fail #>] (Note: 0 = never)
      [-v <vendor class>]
      [-i <client id>]
      [-u <user class>]
```

Error Message: E000, E102

about

Access: Super User, Administrator, Device User, Read Only

Description: Displays system information (Model Number, Serial Number, Manufacture Dates, etc.)

Parameters: None

Example:

```

apc> about

E000: Success

Hardware Factory
-----
Model Number:      XXXXXXXXXXXX
Serial Number:     XXXXXXXXXXXXXX
Hardware Revision:  XXXX
Manufacture Date:  2/9/2022
MAC Address:       00 05 A2 18 00 01
Management Uptime: 0 Days 1 Hour 42 Minutes
    
```

Error Message: E000

alarmcount

Access: Super User, Administrator, Device User, Read Only

Description: Displays alarms present in the system.

Parameters:

Option	Argument	Description
-p	all	View the number of active alarms reported by the Rack ATS. Information about the alarms is provided in the Event Log.
	warning	View the number of active warning alarms.
	critical	View the number of active critical alarms.

Example: To view all active warning alarms, type:

```

apc> alarmcount
E000: Success
AlarmCount: 0
    
```

Error Message: E000, E102

boot

Access: Super User, Administrator

Description: Allows the user to get or set the network startup configuration of the device, such as setting boot mode (DHCP vs BOOTP vs MANUAL).

Parameters:

Option	Argument	Description
-b <boot mode>	dhcp bootp manual	Define how the TCP/IP settings will be configured when the Rack ATS turns on, resets, or restarts. See <i>Configure TCP/IP and Communication Settings for IPv4 and IPv6</i> , page 151 for information about each boot mode setting.
-c	[<enable disable>] (Require DHCP Cookie)	dhcp and dhcpBootp boot modes only. Enable or disable the requirement that the DHCP server provide the APC cookie.
-v	[<vendor class>]	Vendor Class is APC.
-i	[<client id>]	The MAC address of the Rack ATS, which uniquely identifies it on the network.
-u	[<user class>]	The name of the application firmware module.

Example: Using a DHCP server to obtain network settings:

```

apc> boot
E000: Success
Boot Mode:                manual
Non-Manual Mode Shared Settings
-----
Vendor class:             <device class>
Client id:                XX XX XX XX XX XX
User class:               <user class>
After IP assignment:     gotoDhcpOrBootp

DHCP Settings
-----
Retry then stop:         4
DHCP cookie is:         enable

BOOTP Settings
-----
Retry then fail:         never
On retry failure:       prevSettings

```

Error Message: E000, E102

bye, exit, or quit

Access: Super User, Administrator, Device User, Read Only User

Description: Exit the CLI.

Parameters: None.

Example 1:

```
apc> bye
Bye
```

Example 2:

```
apc> exit
Bye
```

Example 3:

```
apc> quit
Bye
```

Error Message: None.

cd

Access: Super User, Administrator, Device User, Read Only

Description: Allows the user to set the working directory of the file system. The working directory is set back to the root directory '/' when the user logs out of the CLI.

Parameters: <directory name>

Example:

```
apc> cd logs
E000: Success
```

```
apc> cd /
E000: Success
```

Error Message: E000, E102

clrrst

Access: Super User, Administrator

Description: Clear reset reason.

Example: None

Error Message: None

console

Access: Super User, Administrator

Description: Define whether users can access the Command Line Interface using Telnet, which is disabled by default, or Secure SHell (SSH), which is enabled by default and provides protection by transmitting user names, passwords, and data in encrypted form. You can change the Telnet or SSH port setting for additional security. Alternately, disable network access to the Command Line Interface.

Parameters:

Option	Argument	Description
-S	<enable disable>	Enable or Disable SSH access to the device. Enabling SSH enables SCP.
-t	<enable disable>	Enable or Disable Telnet access to the device.
-pt	<telnet port n>	Define the Telnet port used to communicate with the Rack ATS (23 by default).
-ps	<SSH port n>	Define the SSH port used to communicate with the Rack ATS (22 by default).
-b	2400 9600 19200 38400	Configure the speed of the console port connection (9600 bps by default).

Example 1: To enable SSH access to the Command Line Interface, type:

```
console -S ssh
```

Example 2:

```
apc> console
E000: Success

Telnet:          enabled
SSH:             disabled
Telnet Port:     23
SSH Port:        22
Baud Rate:       9600
```

Error Message: E000, E102

date

Access: Super User, Administrator

Definition: Get and set the date and time of the system. To configure an NTP server to define the date and time for the Rack ATS.

Parameters:

Option	Argument	Description
-d	<"datestring">	Set the current date. The format must match the current -f setting.
-t	<00:00:00>	Configure the current time, in hours, minutes, and seconds. Use the 24-hour clock format.
-f	mm/dd/yy dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd	Select the numerical format in which to display all dates in this user interface. 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.
-z	<time zone offset>	Set the difference with GMT in order to specify your time zone. This enables you to synchronize with other people in different time zones.

Example 1: To display the date using the format yyyy-mm-dd, type:

```
date -f yyyy-mm-dd
```

Example 2: To define the date as February 9, 2022, using the format configured in the preceding example, type:

```
date -d "2022-02-09"
```

Example 3: To define the time as 5:21:03 p.m., type:

```
date -t 17:21:03
```

Error Message: E000, E100, E102

delete

Access: Super User, Administrator

Description: Delete a file in the file system.

Parameters:

Argument	Description
<file name>	Type the name of the file to delete.

Example:

```
apc> delete /db/prefs.dat
E000: Success
```

Error Messages: E000, E102

dir

Access: Super User, Administrator, Device User, Read Only

Description: Displays the content of the working directory.

Parameters: None

Example:

```
apc> dir
E000: Success
--wx-wx-wx      1 apc      apc      3145728 May 3  2022  aos.bin
--wx-wx-wx      1 apc      apc      3145728 May 4  2022  app.bin
-rw-rw-rw-      1 apc      apc      45000 May 6  2022  config.ini
drwxrwxrwx      1 apc      apc           0 May 3  2022  db/
drwxrwxrwx      1 apc      apc           0 May 3  2022  ssl/
drwxrwxrwx      1 apc      apc           0 May 3  2022  ssh/
drwxrwxrwx      1 apc      apc           0 May 3  2022  logs/
drwxrwxrwx      1 apc      apc           0 May 3  2022  sec/
drwxrwxrwx      1 apc      apc           0 May 3  2022  dbg/
```

Error Messages: E000

dns

Access: Super User, Administrator

Definition: Configure the manual Domain Name System (DNS) settings.

Parameters:

Option	Argument	Description
-OM	enable disable	Override the manual DNS.
-p	<primary DNS server>	Set the primary DNS server.
-s	<secondary DNS server>	Set the secondary DNS server.
-d	<domain name>	Set the domain name.
-n	<domain name IPv6>	Set the domain name IPv6.
-h	<host name>	Set the host name.
-y	<enable disable>	System-hostname sync

Example:

```

apc> dns

E000: Success

Active Primary DNS Server:      x.x.x.x
Active Secondary DNS Server:    x.x.x.x

Override Manual DNS Settings:   enabled
Primary DNS Server:            x.x.x.x
Secondary DNS Server:          x.x.x.x
Domain Name:                   example.com
Domain Name IPv6:              example.com
System Name Sync:              Enabled
Host Name:                     ExampleHostName

```

Error Message: E000, E102

eapol

Access: Super User, Administrator, User

Description: Configure EAPoL (802.1X Security) settings.

Parameters:

Option	Argument	Description
-S	enable disable	Enable or disable EAPoL.
-n	<supplicant name>	Set the supplicant name.
-p	<private key passphrase>	Set the private key passphrase.

Example 1: To display the result of an `eapol` command:

```
apc>eapol
E000: Success
Active EAPoL Settings
-----
      Status:enabled
      Supplicant Name:NMC-Supplicant
      Passphrase:<hidden>
      CA file Status:Valid Certificate
      Private Key Status:Valid Certificate
      Public Key Status:Valid Certificate
      Result:Success
```

Example 2: To enable EAPoL:

```
apc>eapol -S enable
E002: Success
Reboot required for change to take effect.
```

Example 3: To change the supplicant name:

```
apc>eapol -n "NMC-Supplicant"
E000: Success
```

Example 4: To set the passphrase:

```
apc>eapol -p "client_password"
E000: Success
```

email

Access: Super User, Administrator

Description: View email

Parameters:

Parameters	Argument
-g[n]	<enable disable> (Generation)
-t[n]	<To Address>
-o[n]	<long short> (Format)
-l[n]	<Language Code>
-r [n]	<Local recipient custom> (Route)
Custom Route Option	
-f[n]	<From Address>
-s{n}	<SMTP Server>
-p[n]	<Port>
-a[n]	<enable disable> (Authentication)
-u[n]	<User Name>
-w[n]	-w[n]
-e[n]	<none ifsupported always implicit> (Encryption)
-c[n]	<enable disable > (Required Certificate)
-i[n]	<Certificate File Name>
n=	Email Recipient Number 1, 2, 3 or 4)

Example:

```
apc> email
E000: Success

Recipient: 1
Generation: enabled
Address: example@example.com
Format: long
Language: enUs - English
Route: local
```

Error Message: E000, E102

eventlog

Access: Super User, Administrator, Device User, Read Only

Description: View the date and time you retrieved the Event Log, the status of the Rack ATS, and the status of sensors connected to the Rack ATS. View the most recent device events and the date and time they occurred. Use the following keys to navigate the Event Log:

Parameters:

Key	Description
ESC	Close the Event Log and return to the Command Line Interface.
ENTER	Update the log display. Use this command to view events that were recorded after you last retrieved and displayed the log.
SPACEBAR	View the next page of the Event Log.
B	View the preceding page of the Event Log. This command is not available at the main page of the Event Log.
D	Delete the Event Log. Follow the prompts to confirm or deny the deletion. Deleted events cannot be retrieved.

Example:

```
apc> eventlog
---- Event Log -----
Date: 2/9/2022 Time: 13:22:26
-----
Metered Rack ATS: Communication Established
Date           Time           Event
-----
2/9/2022      13:17:22      System: Set Time.
2/9/2022      13:16:57      System: Configuration change. Date format
                preference.
2/9/2022      13:16:49      System: Set Date.
2/9/2022      13:16:35      System: Configuration change. Date format
                preference.
2/9/2022      13:16:08      System: Set Date.
2/9/2022      13:15:30      System: Set Time.
2/9/2022      13:15:00      System: Set Time.
2/9/2022      13:13:58      System: Set Date.
2/9/2022      13:12:22      System: Set Date.
2/9/2022      13:12:08      System: Set Date.
2/9/2022      13:11:41      System: Set Date.
<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

Error Message: E000, E100

exit

See `bye`, `exit`, or `quit`, page 53.

firewall

Access: Super User, Administrator

Description: Establishes a barrier between a trusted, secure internal network and another network.

Parameters:

Parameters	Argument	Description
-s	<enable disable>	Enable or disable the firewall.
-f	<file name to activate>	Name of the firewall to activate.
-t	<file name to test> <duration time in minutes>	Name of firewall to test and duration time in minutes.
-fe	No argument. List only	Shows active file errors.
-te	No argument. List only	Shows test file errors.
-c	No argument.	Cancel a firewall test.
-r	No argument. List only	Shows active firewall rules.
-l	No argument. List only	Shows firewall activity log.
-y	No argument.	Skip firewall test prompt.

Error Message: E000, E102

format

Access: Super User, Administrator

Description: Allows the user to format the FLASH file system. This will delete all configuration data, Event and Data Logs, certificates and keys, and reset the card to the factory defaults.

NOTE: The user must confirm by entering "YES" when prompted.

Parameters: None

Example:

```
apc> format

Format FLASH file system

Warning: This will delete all configuration data,
        event and data logs, certs and keys.

Enter 'YES' to continue or <ENTER> to cancel:
apc>
```

Error Message: None

ftp

Access: Super User, Administrator

Description: Get/set the ftp configuration data

NOTE: The system will reboot if any configuration is changed.

Parameters:

Option	Argument	Definition
-p	<port number> (valid ranges are: 21 and 5000-32768)	Define the TCP/IP port that the FTP server uses to communicate with the Rack ATS (21 by default). The FTP server uses both the specified port and the port one number lower than the specified port.
-s	<enable disable>	Configure access to the FTP server.

Example: To change the TCP/IP port to 5001, type:

```
apc> ftp -p 5001
E000: Success
```

```
apc> ftp
E000: Success
Service: Enabled
Ftp Port: 5001
```

```
apc> ftp -p 21
E000: Success
```

Error Message: E000, E102

help

See ? or help, page 49.

lang

Access: Super User, Administrator, Device User

Description: Displays the language in use

Parameters: None

Example:

```
apc>lang
E000: Success
```

```
Languages
enUs - English
```

Error Message: None

lastrst

Access: Super User, Administrator

Description: View the reason for the last reset.

Parameters: None

Example:

```
apc> lastrst
00 Reset Cleared
E000: Success
```

Error Message: E000, E102

ledblink

Access: Super User, Administrator

Description: Sets the blink rate to the LED on the Rack Power Distribution Unit.

Parameters: <time> = Number of minutes to blink the LED

Example:

```
apc> ledblink 1
E000: Success
```

Error Message: E000, E102

logzip

Access: Super User, Administrator

Description: Places large logs into a zip file before sending.

Parameters: [-m <email recipient>] (email recipient number (1-4))

Example:

```
apc> logzip
Generating files
/dbg/debug_ZA1023006009.tar
E000: Success
```

Error Message: E000, E102

netstat

Access: Super User, Administrator

Description: Displays incoming and outgoing network connections.

Parameters: None

Example:

```
apc> netstat

Current IP Information:
Family              mHome      Type      IPAddress
IPv6                 4          auto      FE80::2CO:B7FF:FE51:F304/64
IPv6                 0          manual    :::1/128
IPv4                 0          manual    127.0.0.1/32
```

Error Message: E000, E102

ntp

Access: Super User, Administrator

Description: Synchronizes the time of a computer client or server.

Parameters:

Option	Argument	Definition
-OM	enable disable	Override the manual settings
-p	<primary NTP server>	Specify the primary server
-s	<secondary NTP server>	Specify the secondary server

Example 1: To enable the override of manual setting, type:

```
ntp -OM enable
```

Example 2: To specify the primary NTP server, type:

```
ntp -p 150.250.6.10
```

Error Message: E000, E102

ping

Access: Super User, Administrator, Device User

Description: Perform a network 'ping' to any external network device.

Parameters:

Argument	Description
<IP address or DNS name>	Type an IP address with the format xxx.xxx.xxx.xxx, or the DNS name configured by the DNS server.

Example:

```
apc> ping 192.168.1.50
E000: Success
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
Reply from 192.168.1.50: time(ms)= <10
```

Error Message: E000, E100, E102

portSpeed

Access: Super User, Administrator

Description: Allows the user to get/set the network port speed.

NOTE: The system will reboot if any configuration is changed.

Parameters:

Option	Arguments	Description
-s	auto 10H 10F 100H 100F	Define the communication speed of the Ethernet port. The <code>auto</code> command enables the Ethernet devices to negotiate to transmit at the highest possible speed.
H = Half Duplex 10 = 10 Meg Bits		
F = Full Duplex 100 = 100 Meg Bits		

Example:

```
apc> portspeed
E000: Success

Port Speed: 10 Half_Duplex

apc> portspeed -s 10h
E000: Success

apc> portspeed
E000: Success
Port Speed: 10 Half_Duplex

apc> portspeed -s auto
E000: Success
```

Error Message: E000, E102

prompt

Access: Super User, Administrator, Device User

Description: Allows the user to change the format of the prompt, either short or long.

Parameters:

Option	Argument	Description
-s	long	The prompt includes the account type of the currently logged-in user.
	short	The default setting. The prompt is four characters long: <code>apc></code>

Example:

```
apc> prompt -s long
E000: Success

Administrator@apc>prompt -s short
E000: Success
```

Error Message: E000, E102

pwd

Access: Super User, Administrator, Device User, Read Only

Description: Output the path of the current working directory.

Parameters: None

Example:

```
apc> pwd
/

apc> cd logs
E000: Success

apc> pwd
/logs
```

Error Message: E000, E102

quit

See `bye`, `exit`, or `quit`, page 53.

radius

Access: Super User, Administrator

Description: View the existing RADIUS settings, enable or disable RADIUS authentication, and configure basic authentication parameters for up to two RADIUS servers.

For detailed information about configuring your RADIUS server, see the *Security Handbook*, available at www.apc.com.

Parameters:

Option	Argument	Description
-a	local radiusLocal radius	Configure RADIUS authentication: local — RADIUS is disabled. Local authentication is enabled. radiusLocal — RADIUS, then Local Authentication. RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used. radius — RADIUS is enabled. Local authentication is disabled.
-p1 -p2	<server IP>	The server name or IP address of the primary or secondary RADIUS server. 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. The Rack ATS supports ports 1812, 5000 to 32768.
-s1 -s2	<server secret>	The shared secret between the primary or secondary RADIUS server and the Rack ATS.
-t1 -t2	<server timeout>	The time in seconds that the Rack ATS waits for a response from the primary or secondary RADIUS server.

Example 1: To view the existing RADIUS settings for the Rack ATS, type `radius` and press ENTER.

Example 2: To enable RADIUS and local authentication, type:

```
apc> radius -a radiusLocal
E000: Success
```

Example 3: To configure a 10-second timeout for a secondary RADIUS server, type:

```
apc> radius -t2 10
E000: Success
```

Error Message: E000, E102

reboot

Access: Super User, Administrator

Description: Restart the interface of the NMC only. Forces the network device to reboot.

Parameters:

Option	Description
-Y	Skip confirmation prompt (Uppercase Y only)

Example 1:

```
apc> reboot
E000: Success
Reboot Management Interface
Enter 'YES' to continue or <ENTER> to cancel: <user enters 'YES'>
Rebooting...
```

Example 2:

```
apc> reboot -Y
E000: Success
Reboot Management Interface
Rebooting...
```

Error Message: E000, E100

resetToDef

Access: Super User, Administrator

Description: Resets all parameters to their defaults. Deletes all accounts and clears Event and Data Logs. Resets all configuration changes, including event actions, device settings, and, optionally, TCP/IP configuration settings.

Parameters:

Option	Arguments	Description
-p	all keepip	all = all configuration data, including the IP address. keepip = all configuration data, except the IP address. Reset all configuration changes, including event actions, device settings, and, optional, TCP/IP configuration settings.

Example: To reset all of the configuration changes *except* the TCP/IP settings for the Rack ATS, type:

```
apc> resettodef -p keepip
Reset to Defaults Except TCP/IP
Enter 'YES' to continue or <ENTER> to cancel: <user enters 'YES'>
```

Error Message: E000, E100

session

Access: Super User, Administrator

Description: Records who is logged in, the serial, time and ID.

Parameters:

Option	Arguments
-d	[-d <session nID>] (Delete)
-M	<enable disable> (MultiUser Enable)
-a	<enable disable> (Remote Authentication Override)

Example:

```
apc>session
User          Interface      Address        Logged In Time    ID
-----
apc           Web            x.x.x.x       00:00:08         156
apc           Telnet        x.x.x.x       00:00:02         157
E000: Success
```

Error Message: E000, E102

smtp

Access: Super User, Administrator

Description: Internet standard for electronic mail

Parameters:

Option	Argument
-f	<From Address>
-s	<SMTP Server>
-p	<Port> 1
-a	<enable disable> (Authentication)
-u	<User Name>
-w	<Password>
-e	<none ifavail always implicit> (Encryption)
-c	<enable disable> (Require Certificate)
-i	<Certificate File Name>
1 — Port options are 25, 465, 587, 2525, 5000 to 32768	

Example:

```
apc> smtp
E000: Success
```

```
From:          address@example.com
Server:        mail.example.com
Port:          25
Auth:          disabled
User:          User
Password:      <not set>
Encryption:    none
Req. Cert:     disabled
Cert File:     <n/a>
```

Error Message: E000, E102

snmp

Access: Super User, Administrator

Description: View and configure SNMPv1 settings. SNMPv1 is disabled by default.

Parameters:

Option	Arguments	Description
-c	<Community>	Identify the group of Rack ATS units
-a	<read write writeplus disable>	Set the access level
-n	<IP or Domain Name>	The host's name or address
-S	<enable disable>	Enable or disable SNMPv1

Example: To enable SNMP version1, type:

```
apc> snmp
E000: Success
  SNMPv1:      enabled

Access Control summary:
Access Control #:      1
Community:           public
Access Type:         read
Address:             0.0.0.0

Access Control #:      2
Community:           private
Access Type:         write +
Address:             0.0.0.0

Access Control #:      3
Community:           public2
Access Type:         disabled
Address:             0.0.0.0

Access Control #:      4
Community:           private2
Access Type:         disabled
Address:             0.0.0.0
```

Error Message: E000, E102

snmpv3

Access: Super User, Administrator

Description: View the existing SNMPv3 settings, enable or disable SNMP, and configure basic SNMP parameters.

NOTE: SNMPv3 is disabled by default. A valid user profile must be enabled with passphrases (-a[n], -c[n]) set before SNMPv3 communications can be established.

Parameters:

Option	Arguments	Description
-S	<enable disable>	Enable or disable SNMPv3
-u[n]	<User Name>	User Name
-a[n]	<Auth phrase>	Authentication phrase of User profile
-c[n]	<Crypt phrase>	Crypt phrase of User profile
-ap[n]	<sha md5 none>	(Authentication Protocol)
-pp[n]	<aes des \ none>	(Privacy Protocol)
-ac[n]	<enable disable>	(Access)
-au[n]	<User profile name>	Access User Profile
-n[n]	<IP or Domain Name>	The host's name or address

[n] = Access Control # = 1, 2, 3, through 8

Example:

```
apc> snmpv3
E000: Success
SNMPv3 Configuration
  SNMPV3:          disabled

SNMPV3 User Profiles

  Index:          1
  User Name:      apc snmp profile1
  Authentication: None
  Encryption:     None

  Index:          2
  User Name:      apc snmp profile2
  Authentication: None
  Encryption:     None

  Index:          3
  User Name:      apc snmp profile3
  Authentication: None
  Encryption:     None

  Index:          4
  User Name:      apc snmp profile4
  Authentication: None
  Encryption:     None
```


SNMPv3 Access Control

```

Index:          1
User Name:      apc snmp profile1
Access:         disabled
NMS IP/Host Name: 0.0.0.0

Index:          2
User Name:      apc snmp profile2
Access:         disabled
NMS IP/Host Name: 0.0.0.0

Index:          3
User Name:      apc snmp profile3
Access:         disabled
NMS IP/Host Name: 0.0.0.0

Index:          4
User Name:      apc snmp profile4
Access:         disabled
NMS IP/Host Name: 0.0.0.0
    
```

Error Message: E000, E102

ssh

Access: Super User, Administrator, Network-Only User

Description: Configure SSH keys. You must enter the sub-command `key` after `ssh`.

Parameters:

Sub-command	Option	Argument	Description
key Show, generate, or delete a key.	-s	none	Show the current key.
	-f	none	Show the current fingerprint.
	-d	none	Delete the current key.
	-i	<filename>. p15	Import a key from a PKCS#15 file.
	-ecdsa	<256> (bit size)	Generate an ECDSA key.
	-rsa	<1024 2048 4096>(bit size)	Generate an RSA key.

Example 1: To delete the SSH server key, enter:

```

apc> ssh key -d
E000: Success
    
```

Example 2: To generate a 2048-bit RSA SSH Server key, enter:

```

apc> ssh key -rsa 2048
E000: Success
    
```

Error Messages: E000, E102

ssl

There are three SSL sub-commands: `key`, `csr`, and `cert`.

key

Access: Super User, Administrator, Network-Only User

Description: Show, generate, or delete a key.

Parameters:

Option	Argument	Description
-s	none	Show the current key.
-d	none	Delete the current key.
-i	<filename>.p15ssl	Import a key from a PKCS#15 file* that has been uploaded to your Rack ATS.
-ecdsa	<256 384 521> (bit size)	Generate an ECDSA key.
-rsa	<1024 2048 4096>(bit size)	Generate an RSA key.

*You can generate a PKCS#15 file with the NMC Security Wizard (available on www.apc.com).

Example 1: To generate a new Web UI key, enter:

```
apc> ssl key -ecdsa 256
E000: Success
```

Example 2: To delete a key, enter:

```
apc> ssl key -d
E000: Success
```

Error Messages: E000, E102

CSR**Access:** Super User, Administrator**Description:** Show or create a Certificate Signing Request (CSR).**Parameters:**

Option	Argument	Description
-s	<file>	Show the current CSR. If no file path is specified, the command checks the default location: <code>ssl/nmc.csr</code> .
-q	<file>	Create a CSR from an active configuration. If no file path is specified, the CSR is stored at the default location: <code>ssl/nmc.csr</code> .
-CN	<name> <file>	Create a custom CSR. <code>name</code> = the hostname of your device. <code>file</code> = an optional custom file path. The default is <code>ssl/nmc.csr</code> .
-O	<organization>	Optional: Your organization.
-OU	<organization unit>	Optional: Your organizational unit.
-C	<country>	Optional: The country where you, your organizational unit, or the device is located.
-san	<name IP>	Optional: Subject Alternative Name. <code>name</code> = the DNS name of this device. <code>IP</code> = the IPv4 or IPv6 address of your device.

Example 1: To create a quick CSR from the current configuration, enter:

```
apc> ssl csr -q
E000: Success
```

Example 2: To create a minimal CSR, enter:

```
apc> ssl csr -CN 192.168.1.100 -C US
E000: Success
```

Example 3: To show a CSR in the default location, enter:

```
apc> ssl csr -s
E000: Success

Certificate Signing Request (ssl/nmc.csr)
-----
Subject: CN=192.168.1.100, C=US
Subject Public Key Info:
  Public Key Algorithm: ECDSA (256 bit)
  X:
    xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
    xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
  Y:
    xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
    xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
  Curve: P-256

Subject Alternative Name:
  DNS: abcdefg.123.456.my-website.com
  IP Address:192.168.1.100
  IP Address:AB90::3A36:78EE:CD3C:ABC2
```

Error Messages: E000, E102

cert**Access:** Super User, Administrator**Description:** Show or import a certificate.**Parameters:**

Option	Argument	Description
-s	<file>	Show the current certificate or the certificate file.
-f	<file>	Show certificate fingerprint.
-i	<file>	Import a new certificate.

NOTE: The argument is optional for all three options. If no file path is specified, the command checks the default location: `ssl/nmc.crt`.

Example 1: To show the active certificate, enter:

```

apc> ssl cert -s
E000: Success

Certificate
-----
Serial Number: XXXXXXXXXXXXXXXXXXX
Issuer: CN=., C=US
Validity:
    Not Before: Mon Oct 11 16:46:44 2021 UTC
    Not After : Sat Dec 15 23:59:59 2035 UTC
Subject: CN=., C=US
Subject Public Key Info:
    Public Key Algorithm: ECDSA (256 bit)
X:
    xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
    xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
Y:
    xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:
    xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx:xx
Curve: P-256

Thumbprint: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Fingerprint: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

```

Example 2: To import `ssl/nmc.crt`, enter:

```

apc> ssl cert -i
E000: Success

```

Example 2: To import another certificate (`other.crt`), enter:

```

apc> ssl cert -i other.crt
E000: Success

```

Error Messages: E000, E102

snmptrap

Access: Super User, Administrator

Description: Enable or disable SNMP trap generation

Parameters:

Option	Arguments
-c[n]	<Community>
-r[n]	<Receiver NMS IP>
-l[n]	<Language> [language code]
-t[n]	<Trap Type> [snmpV1 snmpV3]
-g[n]	<Generation> [enable disable]
-a[n]	<Auth Trap> [enable disable]
-u[n]	<profile1 profile2 profile3 profile4 (User Name)>

n = Trap receiver # = 1, 2, through 8

Example:

```
apc> snmptrap
E000: Success

SNMP Trap Configuration

  Index:                1
  Receiver IP:          x.x.x.x
  Community:            public
  Trap Type:            SNMPV1
  Generation:           disabled
  Auth Traps:           enabled
  User Name:            apc snmp profile1
  Language:             enUs - English
```

Error Message: E000, E102

system

Access: Super User, Administrator

Description: View and set the system name, the contact, the location and view up time as well as the date and time, the logged-on user, and the high-level system status P, N, A. (See **About the Main Screen** in this manual for more information about system status.)

Parameters:

Option	Argument	Description
-n	<system-name>	Define the device name, the name of the person responsible for the device, and the physical location of the device. If you define a value with more than one word, you must enclose the value in quotation marks. These values are also used by the Rack ATS unit's SNMP agent.
-c	<system-contact>	
-l	<system-location>	
-m	<system-message>	When defined, a custom message will appear on the log on screen for all users.
-s	<enable disable>] (system-hostname sync)	Allow the host name to be synchronized with the system name so both fields automatically contain the same value. When enabling this feature, the system name identifier can no longer contain a space character (since it will be synchronized to the host name field).

Example 1: To set the device location as Test Lab, type:

```
apc> system -l "Test Lab"
E000: Success
```

Example 2: To view the device name, type:

```
apc> system -n
E000: Success
Name:      : Rack 2 in Room #222
```

Error Message: E000, E102

tcpip

Access: Super User, Administrator

Description: View and manually configure these network settings for the Rack ATS:

Parameters:

Option	Argument	Description
-l	<IP address>	Type the IP address of the Rack ATS, using the format <code>xxx.xxx.xxx.xxx</code>
-s	<subnet mask>	Type the subnet mask for the Rack ATS.
-g	<gateway>	Type the IP address of the default gateway. Do not use the loopback address (127.0.0.1) as the default gateway.
-d	<domain name>	Type the DNS name configured by the DNS server.
-h	<host name>	Type the host name that the Rack ATS will use.
-S	enable disable	Enable or disable IPv4.

Example 1: To view the network settings of the Rack ATS, type `tcpip` and press ENTER.

```
apc> tcpip
E000: Success
IP Address:      192.168.1.50
MAC Address:     XX XX XX XX XX XX
Subnet Mask:     255.255.255.0
Gateway:         192.168.1.1
Domain Name:     example.com
Host Name:       HostName
```

Example 2: To view the IP address of the Rack ATS, type:

```
apc> tcpip -i
E000: Success
IP Address:      192.168.1.50
```

Example 3: To manually configure an IP address of `192.168.1.49` for the Rack ATS, type:

```
apc> tcpip -i 192.168.1.49
E000: Success
Reboot required for change to take effect
```

Error Message: E000, E102

tcpip6

Access: Super User, Administrator

Description: Enable IPv6. View and manually configure these network settings for the Rack ATS:

Parameters:

Option	Argument	Description
-s	enable disable	Enable or disable IPv6.
-man	enable disable	Enable manual addressing for the IPv6 address of the Rack ATS.
-auto	enable disable	Enable the Rack ATS to automatically configure the IPv6 address
-i	<IPv6 address>	Set the IPv6 address of the Rack ATS
-g	<IPv6 gateway>	Set the IPv6 address of the default gateway
-d6	router stateful stateless never	Set the DHCPv6 mode, with parameters of router controlled stateful (for address and other information, they maintain their status), stateless (for information other than address, the status is not maintained), never.

Example: To view the network settings of the Rack ATS, type `tcpip6` and press ENTER.

```
apc> tcpip6
E000: Success

IPv6:                enabled
Manual Settings:    disabled

IPv6 Address:        ::/64
MAC Address:         XX XX XX XX XX XX
Gateway:             ::
IPv6 Manual Address: disabled
IPv6 Autoconfiguration: enabled
DHCPv6 Mode:        router controlled
```

Error Message: E000, E102

user

Access: Super User, Administrator

Description: Configure the user name, password, and inactivity timeout for each account type. You can't edit a user name, you must delete it and then create a new user.

Parameters:

Option	Argument	Description
-n	<user>	Specify these options for a user.
-pw	<user password>	
-pe	<user permission>	
-d	<user description>	
-e	enable disable	Enable overall access.
-st	<session timeout>	Specify how long a session lasts when the keyboard is idle before the user is automatically logged off.
-sr	enable disable	Bypass RADIUS by using the serial console (CLI) connection, also known as Serial Remote Authentication Override
-el	enable disable	Indicate the Event Log color coding.
-lf	tab csv	Indicate the format for exporting a log file.
-ts	us metric	Indicate the temperature scale, Fahrenheit or Celsius.
-df	<mm/dd/yyyy dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd>	Specify a date format.
-lg	<language code (e.g. enUs)>	Specify a user language.
-del	<user name>	Delete a user.
-l	<i>none</i>	Display the current user list.

Example:

```

apc> user -n apc
E000: Success
Access: Enabled
User Name: apc
Password: <hidden>
User Permission: Super User
User Description: User Description
Session Timeout: 3 minutes
Serial Remote Authentication Override: Disabled
Event Log Color Coding: Enabled
Export Log Format: Tab
Temperature Scale: Metric
Date Format: mm/dd/yyyy
Language: English (enUs)
Outlets: All

```

Error Message: E000, E102

userdfilt

Access: Super User, Administrator

Description: Complimentary function to “user” establishing default user preferences. There are two main features for the default user settings:

- Determine the default values to populate in each of the fields when the Super User or Administrator-level account creates a new user. These values can be changed before the settings are applied to the system.
- For remote users (user accounts not stored in the system that are remotely authenticated such as RADIUS) these are the values used for those that are not provided by the authenticating server. For example, if a RADIUS server does not provide the user with a temperature preference, the value defined in this section will be used.

Parameters:

Options	Argument	Description
-e	<enable disable>	By default, user will be enabled or disabled upon creation.
-pe	<Administrator Device Read-Only Network-Only>	Specify the user's permission level and account type.
-d	<user description>	Provide a user description.
-st	<session timeout> minute(s)	Provide a default session timeout.
-bl	<bad login attempts>	Number of incorrect login attempts a user has before the system disables their account. Upon reaching this limit, a message is displayed informing the user the account has been locked. The Super User or an Administrator-level account is needed to re-enable the account to allow the user to log back in. NOTE: A Super User account cannot be locked out, but can be manually disabled if necessary.
-el	<enable disable> (Event Log Color Coding)	Enable or disable Event Log color coding.
-lf	<tab csv> (Export Log Format)	Specify the log export format, tab or CSV.
-ts	<us metrics> (Temperature Scale)	Specify the user's temperature scale. This setting is also used by the system when a user preference is not available (for example, email notifications).
-df	<mm/dd/yyyy dd.mm.yyyy mmm-dd-yy dd-mmm-yy yyyy-mm-dd> (Date Format)	Specify the user's preferred date format.
-lg	<language code (enUs, etc)>	User language. Only enUs is supported at this time.
-sp	<enable disable>	Strong password requirements. When enabled: <ul style="list-style-type: none"> • The password must be 8–64 characters long. • The password must contain at least one lowercase letter, one uppercase letter, one number, and one symbol (! " # \$ % & ' () * + , - . / : ; < = > ? @ [\] ^ _ ` { } ~).
-pp	<interval in days>	Required password change interval

Example:

```
apc> userdfilt
E000: Success
Access: Disabled
User Permission: Administrator
Session Timeout: 3 minutes
Bad Login Attempts: 0
Event Log Color Coding: Enabled
Export Log Format: Tab
Temperature Scale: Metric
Date Format: mm/dd/yyyy
Language: English (enUs)
Strong Passwords: Disabled
Require Password Change: 0 day(s) (Disabled)
```

Error Message: E000, E102

web

Access: Super User, Administrator

Description: Enable access to the Web UI using HTTP or HTTPS.

For additional security, you can change the port setting for HTTP and HTTPS to any unused port from 5000 to 32768. 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, type:

```
http://152.214.12.114:5000
```

Parameters:

Option	Argument	Definition
-h	enable disable	Enable or disable access to the user interface for HTTP. HTTP is disabled by default.
-s	enable disable	Enable or disable access to the user interface for HTTPS. HTTPS is enabled by default. When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate.
-ph	<http port #>	Specify the TCP/IP port used by HTTP to communicate with the Rack ATS (80 by default). The other available range is 5000–32768.
-ps	<https port #>	Specify the TCP/IP port used by HTTPS to communicate with the Rack ATS (443 by default). The other available range is 5000–32768.
-mp	<minimum protocol>	Choices are: SSL3.0 TLS1.0 TLS1.1 TLS1.2

Example 1: To prevent all access to the Web UI, type:

```
apc> web -h disable -s disable
apc> web -h disable -s disable
```

Example 2: To define the TCP/IP port used by HTTP, type:

```
apc> web
E000: Success
Http:          enabled
Https:         disabled
Http Port:     80
Https Port:    443
Minimum Protocol: TLS1.1

apc> web -ph 80
E000: Success
```

Error Message: E000, E102

whoami

Access: Super User, Administrator, Device Only, Read Only

Description: Provides login information on the current user.

Parameters: None

Example:

```
apc> whoami
E000: Success
admin
```

Error Message: E000, E102

wifi

Reserved for future use.

xferINI

Access: Super User, Administrator

Description: Use XMODEM to upload an INI file while you are accessing the Command Line Interface through a serial connection. After the upload completes:

- If there are any system or network changes, the Command Line Interface restarts and you must log on again.
- If you selected a baud rate for the file transfer that is not the same as the default baud rate for the NMC, you must reset the baud rate to the default to reestablish communication with the NMC.

Parameters: None

Example:

```
apc> xferINI
Enter 'YES' or 'Y' to continue or <ENTER> to cancel: <user
enters 'YES' or 'Y'>
---- File Transfer Baud Rate-----
      1- 2400
      2- 9600
      3- 19200
      4- 38400
> <user enters baudrate selection>
Transferring at current baud rate (9600), press <ENTER>...
<user presses <ENTER>>
Start XMODEM-CRC Transfer Now!
CC
<user starts sending INI>
150 bytes have successfully been transmitted.

apc>
```

Error Message: None

xferStatus

Access: Super User, Administrator

Description: View the result of the last file transfer.

Parameters: None

Example:

```
apc> xferStatus
E000: Success
```

Result of last file transfer: Failure unknown

Error Message: E000

Device Command Descriptions

Network Port Sharing Commands

The CLI allows commands to be sent to guest Rack ATS units. The user may specify the Display ID of the Rack ATS to be commanded, followed by a colon, before the first argument (or as the first argument, if the command does not normally have arguments). If a Display ID is optional, omitting it will simply command the host Rack ATS.

For example: `<command> [<id#>:]<arg1> <arg2>`

This will send `<command> <arg1> <arg2>` to the Rack ATS with the Display ID specified by `[<id#>:]`. The Display ID is followed by a colon (:), which is followed by `arg1` with no spaces. Spaces are used to delimit arguments.

aboutATS

Access: Super User, Administrator, Device User, Read Only User

Description: Display ATS controller information.

Parameters: None

Example:

```
apc> aboutATS
E000: Success
Model:                AP4450A
Firmware Rev:         0.0.2.5
Firmware Date:        09/23/21
Hardware Rev:         R01
Manufacture Date:     02/04/2021
Serial Number:        XXXXXXXXXXX
```

Error Messages: E000, E102

atsMeasure

Access: Super User, Administrator, Device User, Read Only User

Description: Read source power measurements and ATS power measurements.

Parameters: None.

Example:

```
apc> atsMeasure
E000: Success
Source A Freq:           60 Hz
Source A Voltage:       121 V
Source B Freq:           60 Hz
Source B Voltage:       121 V
Total Output Power:     1.00 kVA
Source A 24V Power Supply: 24 V
Source B 24V Power Supply: 24 V
Source A Boost Voltage: 40 V
Source B Boost Voltage: 40 V
3.3 V Power Supply:     3.3 V
```

Error Messages: E000, E102

atsStatus

Access: Super User, Administrator, Device User, Read Only User

Description: Read Rack ATS status information.

Parameters: None.

Example:

```
apc> atsStatus
E000: Success
Communication Status:   OK
Selected Source:        Source B
Preferred Source:       Source B
Switch Status:          OK
Front Panel:            Unlocked
Source A:                OK
Source B:                Selected
Phase Synchronization: Sync
Source A 24V Power Supply: OK
Source B 24V Power Supply: OK
Source A 24V Boost Voltage: OK
Source B 24V Boost Voltage: OK
3.3V Power Supply:     OK
```

Error Messages: E000, E102

bkLowLoad

Access: Super User, Administrator, Device User

Description: Set or view the bank low-load threshold current in amps. Only single phase SKUs with two or more circuit breakers support this command.

Parameters:

Argument	Description
<id#>	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<all bank#>	all = all bank numbers bank# = a single number, a range of numbers separated with a dash, or a comma-separated list of single bank number and/or number ranges
<current>	The new bank threshold (Amps)

NOTE: The maximum bank number is 2. If the Rack ATS has two circuit breakers, a total bank threshold is provided.

Example 1: View low-load thresholds for all banks.

```
apc> bkLowLoad all
E000: Success
total:    0 A
1:        0 A
2:        0 A
```

Example 2: View and set the low-load threshold for bank 1.

```
apc> bkLowLoad 1
E000: Success
1: 0 A

apc> bkLowLoad 1 1
E000: Success
```

Example 2: View and set the low-load thresholds for banks 1–2.

```
apc> bkLowLoad 1-2
E000: Success
total:    2 A
1:        1 A
2:        1 A

apc> bkLowLoad 1-2 1
E000: Success
```

Error Messages: E000, E102

bkNearOver

Access: Super User, Administrator, Device User

Description: Set or view the bank near-overload threshold current in amps. Only single phase models with two or more circuit breakers support this command. You can specify all banks, a single bank, a range, or a comma-separated list of single banks and/or ranges.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<all bank#>	all = all bank numbers bank#: = a single number, a range of numbers separated with a dash, or a comma-separated list of single bank number and/or number ranges
<current>	The new bank threshold (Amps)

NOTE: The maximum bank number is 2. If the Rack ATS has two circuit breakers, a total bank threshold is provided.

Example 1: View and set the near-overload threshold for all banks.

```
apc> bkNearOver all
E000: Success
total:    10 A
1:        10 A
2:        10 A

apc> bkNearOver all 10
E000: Success
E000: Success
E000: Success
```

Example 2: View and set the near-overload threshold for bank 1.

```
apc> bkNearOver 1
E000: Success
1: 10 A

apc> bkNearOver 1 12
E000: Success

apc> bkNearOver all
E000: Success
total:    12 A
1:        12 A
2:        10 A
```

Example 3: View the near-overload threshold setting for banks 1 and 2 on guest unit 3.

```
apc> bkNearOver 3:1-2
E000: Success
1: 16 A
2: 16 A
```

Error Messages: E000, E102

bkOverLoad

Access: Super User, Administrator, Device User

Description: Set or view the bank overload threshold current in amps. Only single phase SKUs with two or more circuit breakers support this command.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<all bank#>	all = all bank numbers bank#: = a single number, a range of numbers separated with a dash, or a comma-separated list of single bank number and/or number ranges
<current>	The new bank threshold (Amps)

NOTE: The maximum bank number is 2. If the Rack ATS has two circuit breakers, a total bank threshold is provided.

Example 1: View bank overload thresholds for all banks.

```
apc> bkOverLoad all
E000: Success
total:    24 A
1:        14 A
2:        14 A
```

Example 2: View the overload threshold for bank 1.

```
apc> bkOverLoad 1
E000: Success
1: 14 A
```

Example 3: Set the overload threshold for banks 1 and 2.

```
apc> bkOverLoad 1-2 16
E000: Success

apc> bkOverLoad all
E000: Success
total:    32 A
1:        16 A
2:        16 A
```

Error Messages: E000, E102

bkPeakLoad

Access: Super User, Administrator, Device User

Description: Display the peak load measurement from a bank(s). Only single phase SKUs with two or more circuit breakers support this command.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<all bank#>	all = all bank numbers bank#: = a single number, a range of numbers separated with a dash, or a comma-separated list of single bank number and/or number ranges
<current>	The new bank threshold (Amps)

NOTE: The maximum bank number is 2. If the Rack ATS has two circuit breakers, a total bank threshold is provided.

Example:

```
apc> bkPeakLoad all
E000: Success
total:    11.0 A
1:        5.0 A
2:        5.0 A
```

```
apc> bkPeakLoad 1
E000: Success
1: 5.0 A
```

```
apc> bkPeakLoad 1-2
E000: Success
1: 5.0 A
2: 6.0 A
```

Error Messages: E000, E102

bkReading

Access: Super User, Administrator, Device User, Read Only

Description: View the current reading (measurement) in amps for a bank. Only single phase models with two or more circuit breakers support this command.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<all bank#>	all = all bank numbers bank#: = a single number, a range of numbers separated with a dash, or a comma-separated list of single bank number and/or number ranges
<current>	The new bank threshold (Amps)

NOTE: The maximum bank number is 2. If the Rack ATS has two circuit breakers, a total bank threshold is provided.

Example :

```
apc> bkReading 1
E000: Success
1: 6.3 A

apc> bkReading all
E000: Success
total:    11.4 A
1:        6.3 A
2:        5.1 A

apc> bkReading 1-2
E000: Success
1: 6.3 A
2: 5.1 A
```

Error Messages: E000, E102

eventCounts

Access: Super User, Administrator, Device User

Description: Display or clear the event counts reported from the Rack ATS controller.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<0>	Set all event counts to 0.

Example:

```

apc> eventCounts
E000: Success

Event Counts
-----
Redundancy Loss:           15
Source Switch:             80
Over Current:              0
Source Preference Change:  7
Spike/Dropout:            95
Surge/Droop:              0
Frequency out of Range:    9

```

Error Messages: E000, E100, E102

freqDeviat

Access: Super User, Administrator, Device User

Description: Read or set the range of acceptable frequency fluctuation (Hz).

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<3 5 10>	The new range of acceptable frequency deviation: 3, 5, or 10 Hz above or below the nominal frequency.

NOTE: If the frequency (see `atsMeasure`, page 87) is at 50 Hz and `vSensitivty` (see `vSensitivty`, page 115) is set to High, `freqDeviat` should be 3 or 5.

Example:

```

apc> freqDeviat
E000: Success

Frequency Deviation:      3 Hz

```

Error Messages: E000, E100, E102

frontPanel

Access: Super User, Administrator, Device User

Description: Set or view control for the source button on the front panel.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<locked unlocked>	Lock or unlock the front panel for use.

Example:

```
apc> frontPanel
E000: Success
Front Panel: unlocked

apc> frontPanel locked
E000: Success
```

Error Messages: E000, E100, E102

Humidity Sensor Note:

You must connect an optional APC Temperature/Humidity Sensor (AP9335TH) to your Rack ATS in order to use the Humidity related commands.

humAlGen

Access: Super User, Administrator, Device User

Description: Sets and reads whether humidity alarms are enabled or disabled.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size).
<enable disable>	enable = enable humidity alarms. disable = disable humidity alarms.

Example:

```
apc> humAlGen enable
E000: Success
```

```
apc> humAlGen disable
E000: Success
```

Error Message: E000, E102

humHyst

Access: Super User, Administrator, Device User

Description: Sets and reads the humidity threshold hysteresis value.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<value>	new threshold hysteresis value (% RH)

Example:

```
apc> humHyst
E000: Success
6 %RH
```

```
apc> humHyst 5
E000: Success
```

Error Message: E000, E102

humLow

Access: Super User, Administrator, Device User

Description: Set or view the low humidity threshold as a percent of the relative humidity.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<humidity>	New low humidity threshold

Example 1: To view the low humidity threshold, type:

```
apc> humLow
E000: Success
10 %RH
```

Example 2: To set the low humidity threshold, type:

```
apc> humLow 12
E000: Success
```

Example 3: To view the low humidity threshold on guest Rack ATS 3, type:

```
apc> humLow 3:
E000: Success
10 %RH
```

Error Message: E000, E102

humMin

Access: Super User, Administrator, Device User

Description: Set or view the minimum humidity threshold as a percent of the relative humidity.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<humidity>	New minimum humidity threshold

Example 1: To view the minimum humidity threshold, type:

```
apc> humMin
E000: Success
6 %RH
```

Example 2: To set the minimum humidity threshold, type:

```
apc> humMin 8
E000: Success
```

Example 3: To view the humidity value on guest Rack ATS 2, type:

```
apc> humReading 2:
E000: Success
48 %RH
```

Error Message: E000, E102

humReading

Access: Super User, Administrator, Device User, Read Only

Description: View the humidity value from the sensor.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)

Example 1: To view the humidity value, type:

```
apc> humReading
E000: Success
25 %RH
```

Example 2: To view the humidity value on guest Rack ATS 2, type:

```
apc> humReading 2:
E000: Success
48 %RH
```

Error Message: E000, E102, E201

humStatus

Access: Super User, Administrator, Device User, Read Only

Description: Displays the status of the sensor. Responses: Not Connected, Min Threshold Violation, Low Threshold Violation, Normal.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)

Example: To view the status of the humidity sensor, type:

```
apc> humStatus 1
Not Connected
```

Error Message: None

Icd

Access: Super User, Administrator, Device User

Description: Turn the LCD On or Off.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<on off>	Turn the LCD on or off.

Example:

```
apc> lcd off
E000: Success
apc> lcd 1 on
E000: Success
```

Error Messages: E000, E100, E102

IcdBlink

Access: Super User, Administrator

Description: Specify a number of minutes to blink the display. This command can be canceled by pressing a button on the LCD.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size).
<time>	number of minutes to blink the display. Valid range is [1-10].

Example:

```
apc> lcdBlink 2
E000: Success
```

Error Messages: E000, E102

lineVRMS

Access: Super User, Administrator

Description: Read or set the nominal source line voltage (V). Acceptable values depend on Rack ATS model.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<voltage>	Set the nominal source line voltage (V).

Model	Acceptable voltages
AP4421A, AP4422A, AP4423A, AP4424A	230
AP4430A, AP4432A	200 or 208
AP4431A, AP4433A, AP4434A	208
AP4450A	100 or 120
AP4452A, AP4453A	120
AP4452AJ	100

Example:

```
apc> lineVRMS
E000: Success
Nominal Line Voltage: 120

apc> lineVRMS 124
E000: Success
```

Error Messages: E000, E100, E102

logToFlash

Access: Super User, Administrator

Description: Export the log files to a USB flash drive. The file will be a compressed file. It will contain event.txt, config.ini, debug.txt, data.txt. If an exception occurs, it will also contain dump.txt.

Parameters: [<filename>] = the appendix to the debug file tar name. If no name is entered, the serial number of the device will be used as the name for the file.

Example 1:

```
apc>logToFlash 01292018
Creating report file: /debug_01292018.tar
Press <ESC> to abort
0% completed...
Exporting logs... please do not remove USB flash
12% completed...Exporting logs... please do not remove USB flash...
Exporting logs... please do not remove USB
flash 60% completed...
Logs export completed. You may remove USB flash now
```

Example 2:

```
apc>logToFlash
Creating report file:
/debug_ZA1234567890.tar Press <ESC> to abort
0% completed...Exporting logs... please do not remove USB flash
12% completed...Exporting logs... please do not remove USB flash...
Exporting logs... please do not remove USB flash
60% completed...Logs export completed. You may remove USB flash now
```

Error Messages: E000, E102

phLowLoad

NOTE: Only units without circuit breakers are supported by this command.

Access: Super User, Administrator, Device User

Description: Set or view the phase low-load threshold in Amps.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<current>	New low-load threshold (Amps)

Example:

```
apc> phLowLoad
E000: Success
0 A
```

```
apc> phLowLoad 3
E000: Success
```

Error Messages: E000, E102

phNearOver

NOTE: Only units without circuit breakers are supported by this command.

Access: Super User, Administrator, Device User

Description: Set or view the phase near-overload threshold in Amps.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<current>	New near-overload threshold (Amps)

Example:

```
apc> phNearOver
E000: Success
8 A
```

```
apc> phNearOver 9
E000: Success
```

Error Messages: E000, E102

phOverLoad

NOTE: Only units without circuit breakers are supported by this command.

Access: Super User, Administrator, Device User

Description: Set or view the phase overload threshold in amps.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<current>	New overload threshold (Amps)

Example: To view the overload threshold, enter

```
apc> phOverLoad
E000: Success
10 A
```

To set the overload threshold for all phases to 10 A, enter

```
apc> phOverLoad
E000: Success
10 A
```

Error Messages: E000, E102

phPeakLoad

NOTE: Only units without circuit breakers are supported by this command.

Access: Super User, Administrator, Device User, Read Only User

Description: View the phase peak load.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)

Example:

```
apc> phPeakLoad
E000: Success
4.0 A
```

Error Messages: E000, E102

phReading

NOTE: Only units without circuit breakers are supported by this command.

Access: Super User, Administrator, Device User

Description: View the phase load in Amps.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)

Example:

```
apc> phReading
E000: Success
4.0 A
```

Error Messages: E000, E102

prodInfo

Access: Super User, Administrator, Device User, Read Only

Description: View information about the Rack ATS.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)

Example:

```
apc> prodInfo 2:
E000: Success
AOS:                               1.0.0.3
APP:                               0.0.2.5
Model:                             AP4452A
Name:                              apcRack_01
Location:                          Data Center Row 3
Contact:                           Don Adams
Outlets:                            10
Rated Load:                        16 A
Phases:                             1
Uptime:                            15 Days 1 Hours 8 Minutes
Network Link:                       Link Active
NPS Type:                           Host
NPS Status:                         Active
```

Error Messages: E000, E102

sensorName

Access: Super User, Administrator, Device User

Description: Set or view the name assigned to the Rack ATS Universal I/O port (the connection point for the Temp/Humidity sensor).

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<newname>	The new name for the Universal I/O port

Example 1: To set the name for the port to “Sensor1,” type:

```
apc> sensorName Sensor1
E000: Success
```

Example 2: To then view the name for the sensor port, type:

```
apc> sensorName
E000: Success
Sensor1
```

Example 3: To set the name for the sensor port on guest Rack ATS 2 to “Sensor1,” type:

```
apc> sensorName 2:Sensor1
E000: Success
```

Error Message: E000, E102

sourceAName

Access: Super User, Administrator, Device User

Description: Set or view the name assigned to power source A.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<sourceAName>	Name for source A

Example:

```
apc> sourceAName
E000: Success
Wall Box Phase L1

apc> sourceAName "Wall Box N2 Phase L2"
E000: Success
```

Error Messages: E000, E102

sourceBName

Access: Super User, Administrator, Device User

Description: Set or view the name of power Source B.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<sourceBName>	Name for source B

Example:

```
apc> sourceBName
E000: Success
Wall Box Phase L2

apc> sourceBName "Wall Box N2 Phase L3"
E000: Success
```

Error Messages: E000, E102

sourcePref

Access: Super User, Administrator, Device User

Description: Set or view the desired source preference.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<A B None>	A = Prefer Source A. B = Prefer Source B. None = No preference

Example:

```
apc> sourcePref
E000: Success
Preferred Source: Source A

apc> sourcePref B
E000: Success
```

Error Messages: E000, E102

Temperature Sensor Note:

You must connect an optional APC Temperature/Humidity Sensor (AP9335T/ AP9335TH) to your Rack ATS in order to use the Temperature related commands.

tempAlGen

Access: Super User, Administrator, Device User

Description: Sets or reads whether temperature alarms are enabled or disabled.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<enable disable>	enable = enable temperature alarms. disable = disable temperature alarms.

Example:

```
apc> tempAlGen enable
E000: Success
```

```
apc> tempAlGen disable
E000: Success
```

Error Message: E000, E102

tempHigh

Access: Super User, Administrator, Device User

Description: Set or view the high-temperature threshold in either Fahrenheit or Celsius.

Parameters:

Argument	Description
<id#>	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<F C>	Fahrenheit (F) or Celsius (C)
<temperature>	New high temperature threshold

Example 1: To set the high-temperature threshold to 70° Fahrenheit, type:

```
apc> tempHigh F 70
E000: Success
```

Example 2: To view the high-temperature threshold in Celsius, type:

```
apc> tempHigh C
E000: Success
21 C
```

Example 3: To view the high-temperature threshold of guest Rack ATS 2 in Fahrenheit, type:

```
apc> tempHigh 2:F
E000: Success
70 F
```

Error Message: E000, E102

tempHyst

Access: Super User, Administrator, Device User

Description: Set and displays the temperature threshold hysteresis.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<F C>	Fahrenheit (F) or Celsius (C)
<temperature>	New temperature hysteresis value

Example:

```
apc> tempHyst F 6
E000: Success
```

```
apc> tempHyst C
E000: Success
3 C
```

Error Message: E000, E102

tempMax

Access: Super User, Administrator, Device User

Description: Set or view the max-temperature threshold in either Fahrenheit or Celsius. The id# may be from 1 to 32 depending on the group size.

Parameters:

Argument	Description
<id#>	The id of a unit in the NPS group (can be 1–32 depending on the group size)
< F C >	Fahrenheit (F) or Celsius (C)
<temperature>	New max temperature threshold

Example 1: To set the max-temperature threshold to 80° Fahrenheit, type:

```
apc> tempMax F 80
E000: Success
```

Example 2: To view the max-temperature threshold in Celsius, type:

```
apc> tempMax C
E000: Success
27 C
```

Example 3: To view the max-temperature threshold of guest Rack PDU 3 in Fahrenheit, type:

```
apc> tempMax 3:F
E000: Success
95 F
```

Error Message: E000, E102

tempPeak

Access: Super User, Administrator, Device User

Description: Display the peak temperature reading of the sensor.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<F C>	Fahrenheit (F) or Celsius (C)

Example:

```
apc> tempPeak F
E000: Success
77.5 F
```

Error Message: E000, E102

tempReading

Access: Super User, Administrator, Device User, Read Only

Description: View the temperature value in either Fahrenheit or Celsius from the sensor.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
< F C >	Fahrenheit (F) or Celsius (C)

Example 1: To view the temperature value in Fahrenheit, type:

```
apc> tempReading F
E000: Success
51.1 F
```

Example 2: To view the temperature value of guest Rack ATS 3 in Celsius, type:

```
apc> tempReading 3:C
E000: Success
23.5 C
```

Error Message: E000, E102, E201

vMediumLimit

Access: Super User, Administrator, Device User

Description: Set or view the voltage range to use when the Voltage Transfer Range is set to Medium. This value must be greater than the Narrow Transfer Limit and less than the Wide Limit (V).

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
[<limit>]	Medium voltage transfer range. Acceptable values depend on the Rack ATS model.

Model	Acceptable range values
AP4421A, AP4422A, AP4423A, AP4424A	16–25
AP4430A, AP4432A, AP4433A, AP4434A	15–30
AP4452AJ	10–15
AP4450A, AP4452A, AP4453A	10–23

Example:

```
apc> vMediumLmt
E000: Success
Voltage Medium Limit: 12 V

apc> vMediumLmt 14
E000: Success
```

Error Messages: E000, E100, E102

vNarrowLmt

Access: Super User, Administrator, Device User

Description: Set or view the voltage range to use when the Voltage Transfer Range is set to Narrow. This value must be less than the Medium Limit.

Parameters:

Argument	Description
<id#>	The id of a unit in the NPS group (can be 1–32 depending on the group size)
[<limit>]	Narrow voltage transfer range. Acceptable values depend on the Rack ATS model.

Model	Acceptable range values
AP4421A, AP4422A, AP4423A, AP4424A	16–25
AP4430A, AP4432A, AP4433A, AP4434	15–30
AP4452JA	10–15
AP4450A, AP4452A, AP4453	10–23

Example:

```
apc> vNarrowLmt
E000: Success
Voltage Narrow Limit: 15 V
```

Error Messages: E000, E100, E102

vSensitvty

Access: Super User, Administrator, Device User

Description: Set or view the sensitivity.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<High Low>	Set the sensitivity of the Rack ATS. High = The Rack ATS will switch power sources after 2 ms when there is a disturbance in the power supply. Low = The Rack ATS will switch sources after 4 ms when there is a disturbance in the power supply.

NOTE: If the **Frequency** is at 50 Hz (see **atsMeasure**, page 87) and **FreqDeviat** (see **freqDeviat**, page 93) is set to 10, **vSensitvty** should be set to **Low**.

Example:

```
apc> vSensitvty
E000: Success
Voltage Sensitivity: Low

apc> vSensitvty High
E000: Success
```

Error Messages: E000, E100, E102

vWideLmt

Access: Super User, Administrator, Device User

Description: Set or view the voltage range to use when Voltage Transfer Range is set to Wide. This value must be greater than the Medium Limit.

Parameters:

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
[<limit>]	Wide voltage transfer range. Acceptable values depend on the Rack ATS model.

Model	Acceptable range values
AP4421A, AP4422A, AP4423A, AP4424A	16–25
AP4430A, AP4432A, AP4433A, AP4434A	15–30
AP4452AJ	10–15
AP4450A, AP4452A, AP4453A	10–23

Example:

```
apc> vWideLmt
E000: Success
Voltage Wide Limit: 20

apc> vWideLmt 24
E000: Success
```

Error Messages: E000, E102

vXferRange

Access: Super User, Administrator, Device User

Description: Set or view the Voltage Transfer Range. If the voltage of an Rack ATS exceeds the Transfer Range, it generates an alarm.

Parameters: Voltage transfer range.

Argument	Description
<id#>:	The id of a unit in the NPS group (can be 1–32 depending on the group size)
<Wide Medium Narrow>	Wide: corresponds to configured values for vWideLmt Medium: corresponds to configured values for vMediumLmt Narrow: corresponds to configured values for vNarrowLmt

Example:

```
apc> vXferRange
E000: Success
Voltage Transfer Range: Medium

apc> vXferRange Wide
E000: Success
```

Error Messages: E000, E102

Web User Interface

You can use the latest version of Microsoft Internet Explorer® (IE) or Edge®, Google Chrome®, Apple Safari®, or Mozilla Firefox® to access the Rack ATS through its Web UI. Other commonly available browsers and versions may work but have not been fully tested.

To access the Web UI on any operating system, use the latest releases of Mozilla Firefox®, or Google Chrome®. Other commonly available browsers also may work but have not been fully tested by Schneider Electric.

The Rack ATS cannot work with a proxy server. Before accessing the Web UI of the Rack ATS, do one of the following:

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

Log on to the Web UI

To access the Web UI and configure the security settings of your Rack ATS on the network:

1. Type the DNS name or IP address of the Rack ATS in the Web browser's URL address field and press ENTER.

NOTE: If you are using HTTPS (SSL/TLS) as your access protocol, your login credentials are compared with information in a server certificate. If the certificate was created with the 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.

You may receive a message that the Web page is not secure. This is normal, and you can continue to the Web UI. The warning is generated because your Web browser does not recognize the default certificate used for encryption over HTTPS. However, information transmitted over HTTPS is still encrypted. See the *Security Handbook* on www.apc.com for more details on HTTPS and instructions to resolve the warning.

2. Enter the user name and password. (By default, both values are **apc** for the Super User and Administrator. The Super User, or an Administrator created by the Super User, should define the user name, password, and account characteristics for other users).

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. Until HTTP is enabled, you must include `https://` in the URL. When you specify a non-default Web server port in Internet Explorer, you must include `http://` or `https://` in the URL.

Common Browser Error Messages at Log On

Error Message	Browser	Cause of the Error
"This page cannot be displayed."	Internet Explorer	Web access is disabled, or the URL was not correct.
"Unable to connect."	Firefox	

URL Format Examples

NOTE: HTTP is disabled by default, and HTTPS is enabled by default.

- For a DNS name of Web1:
 - `http://Web1` if HTTP is your access mode
 - `https://Web1` if HTTPS (HTTP with SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133 and the default Web server port (80):
 - `http://139.225.6.133` if HTTP is your access mode
 - `https://139.225.6.133` if HTTPS (HTTP with SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133 and a non-default Web server port (5000):
 - `http://139.225.6.133:5000` if HTTP is your access mode
 - `https://139.225.6.133:5000` if HTTPS (HTTP with SSL/TLS) is your access mode
- For a System IPv6 address of 2001:db8:1::2c0:b7ff:fe00:1100 and a non-default Web server port (5000):
 - `http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000` if HTTP is your access mode
 - `https://[2001:db8:1::2c0:b7ff:fe00:1100]:5000` if HTTPS (HTTP with SSL/TLS) is your access mode

First Log On



When you log on to the Rack ATS for the first time, you will be prompted to change the default Super User account password (**apc**). After you log in, you will be directed to the **Configuration Summary** screen. This screen is an overview of all system protocols, and their current values (e.g. enabled/disabled). You can access this screen at any time afterwards from **Configuration > Network > Summary**.

Web UI Features

Read the following to familiarize yourself with basic Web UI features for your Rack ATS.

Tabs

The following tabs are available:

- **Home:** Appears when you log on. View active alarms, the load status of the Rack ATS, and the most recent Rack ATS events. For more information, see Home Tab, page 123.
NOTE: Home is the default page when you log on. To change the login page, go to the desired login page and then click the pushpin icon  at the top right of the browser window. To change the login page back to Home, click the home target icon .
- **Status:** Gives the user the status of the **ATS** and **Network**. The **ATS** tab covers the status of **Alarms, Device, Unit, Load, Measurement, and Environment**. The **Network** tab only covers the **Network**. For more information, see Status Tab, page 124.
- **Control:** The **Control** tab covers **Security** and **Network**. Much more information is covered under these tabs and will be described under Control Tab, page 130.
- **Configuration:** The **Configuration** tab covers **ATS, Security, Network, Notification, General** and **Logs**. Much more information is covered under each of these tabs and will be under Configuration Tab, page 132.
- **Tests:** The **Tests** tab covers **ATS** and **Network**. The **ATS** tab covers LCD Blink and the **Network** tab covers **LED Blink**. Both will be further described under Tests Tab, page 171.
- **Logs:** The **Logs** section covers **Event, Data** and **Firewall**. The **Event** and **Data** tabs cover more information which will be further discussed under Logs Tab, page 172.
- **About:** The **About** section covers **ATS, Network, and Support**, which will be further discussed under About Tab, page 179.

Limited Status Access




When enabled, the Limited Status page allows you to use a Web browser to view limited information about the Rack ATS without requiring a login. A link to the Login page is available at the top left of the Limited Status page.

To enable the Limited Status page, go to **Configuration > Network > Web > Access** in the Web UI.

- If you only select **Enable**, a **Limited Status** hyperlink appears towards the lower left corner of the Login page. You can click this link to view the Limited Status page without logging in to the Rack ATS.
- If you select both **Enable** and **Use as default**, the Limited Status page appears by default when you enter the IP address of the Rack ATS in the URL address bar of your Web browser.

Device Status Icons

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

Icon	Description
	No Alarms: No alarms are present, and the Rack ATS and NMC are operating normally.
	Warning: An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed.
	Critical: A critical alarm exists, which requires immediate action.

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

- The **No Alarms** icon is displayed if no alarms exist.
- One or both of the other icons (**Critical** and **Warning**) are displayed if any alarms exist. After each icon, the number of active alarms of that severity is also displayed.

You can click any icon in the quick status area to navigate to the **Home** screen.



Quick Links

There are three configurable links at the lower-left corner of each Web UI page. By default, the links access these Web pages:

- Link 1: The home page of APC website
- Link 2: Information on EcoStruxure™ IT
- Link 3: Additional information on IT Power Distribution equipment

You can configure these links under **Configuration > General > Quick Links**.

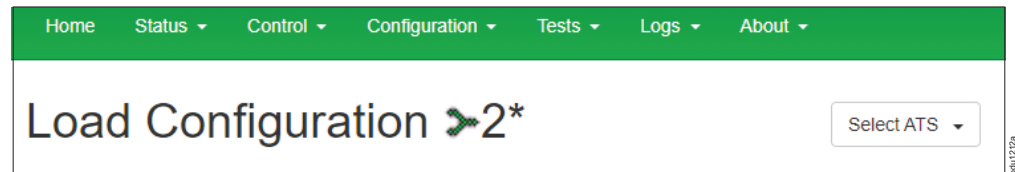
The following links are located in the upper-right corner of each Web UI page:

- **Your user name:** Select this link to change user preferences.
- **Current language:** Only English is supported at this time.
- **Log Off:** Select this link to log the current user off of the Web UI.
- **Help:** Select this link to view context-sensitive information.
- Pushpin icon : Click the pushpin icon to set the current Web page to be the page that displays when you first log on. Click the home target icon  to set the **Home** page as the page that displays when you first log on.

Network Port Sharing (NPS) on the Web UI

The Web UI of the Rack ATS will have additional capabilities if the Rack ATS is part of an NPS group. This includes an NPS Group Status page (**Status > ATS > Group Status**) and an NPS Group Configuration page **Configuration > ATS > Group**. Additionally, for Web pages that support NPS features, you can view a different Rack ATS in the group by selecting the Display ID of that unit.

Each Rack ATS in the NPS group is denoted with a Rack ATS icon ➤ followed by its Display ID (1 to 32). The Rack ATS that you are logged into is displayed with an additional asterisk (*) following the Display ID.



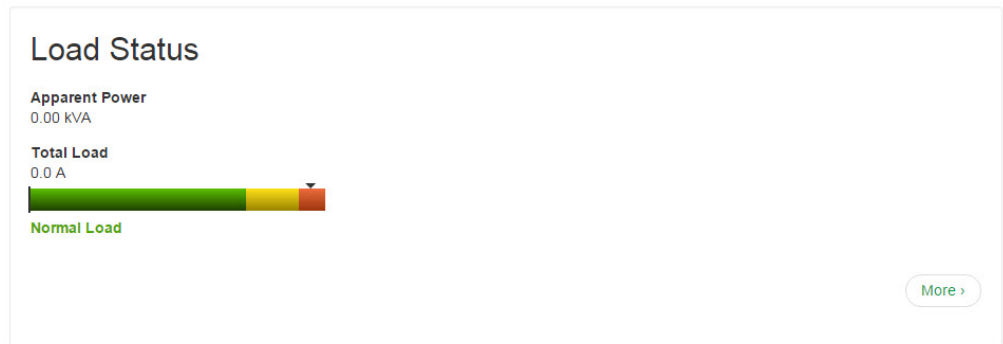
Home Tab

Active Alarms: View active alarms, which will also be displayed at the top right of every page. If no alarms exist, a green check mark with the words “No Alarms Present” will show.

Switch/Source Status: Shows the selected source and whether switchover is possible.

Load Status: View the load for the device in kVA and the load for the phases and banks in A, as applicable. The meter shows the current load status: Normal (green), Near Overload (yellow), or Overload (red). Click **More** to go to the **Load Status** page (see [View Load Status](#), page 126 for more information).

NOTE: If a low load threshold is configured, the meter will also include a blue segment on the left.



Parameters

- **Name:** The configured name for the Rack ATS.
- **Location:** The physical location of the Rack ATS.
- **Contact:** The person responsible for the Rack ATS.
- **Model Number:** Also called SKU or part number. Acceptable voltage configurations are specific to model numbers. For details, see the *Specification Sheet* for your Rack ATS model on www.apc.com.
- **Rating:** Provides the number of metered phases and banks on the unit, in addition to the phase rating of the Rack ATS.
- **User Type:** Type of user account accessing the Rack ATS. Your user type defines what permissions you have. See [Types of User Accounts](#), page 15 for details.
- **Uptime:** Amount of time the Rack ATS has been operating since the last reboot from either a power cycle or a reboot of the Management Interface.

Recent Device Events: View the most recent events, including the dates and times they occurred. A maximum of five events are shown at one time. Click **More Events** to go to the **Logs** tab and view the entire Event Log.

Status Tab

Use the Status tab to view information for the Rack ATS and the network:

- **ATS:** View NPS Groups (**Group Status**) active alarms (**Alarms**), general configuration information for the Rack ATS (**Device Status**), power supply information and event counts (**Unit Status**), Load Status (**Load**), and Power Measurements (**Measurement**).
- **Network:** View IPv4/IPv6 settings, Domain Name System Status, and Port Speed.

View NPS Groups

Status > ATS > Group Status

You can use this page to do the following:

- View general information about each unit in an NPS Group. Select each unit to show or hide specific information about that unit, and options to change the settings for the individual unit.
- Use the **Reset/Reboot** options to return the Network Management Interfaces in the NPS group to their defaults, including TCP/IP and EAPoL settings.
 - TCP/IP and EAPoL (By default, TCP/IP is set to DHCP and EAPoL is disabled.)
 - LCD On/Off preference
 - Names for source A and B, source preference, and front panel locking
 - Frequency deviation, voltage transfer limits, transfer range, and sensitivity
 - Load thresholds, peak current measurement and timestamp
 - Event counts and timestamps for event counts
 - Wired environmental sensor: name and location, peak temperature and timestamps, alarm status (disabled/enabled), temperature/humidity thresholds and hysteresis values

This option will cause the NMC to reboot. You will be required to change the default user name and password (**apc** and **apc**) after initial log on.

- Use the **ATS to defaults** options to return Network Management Interfaces in the NPS group to their defaults, excluding TCP/IP and EAPoL settings:
 - TCP/IP and EAPoL
 - LCD On/Off preference
 - Names for source A and B, source preference, and front panel locking
 - Frequency deviation, voltage transfer limits, transfer range, and sensitivity
 - Load thresholds, peak current measurement and timestamp
 - Event counts and timestamps for event counts
 - Wired environmental sensor: name and location, peak temperature and timestamps, alarm status (disabled/enabled), temperature/humidity thresholds and hysteresis values
- Remove disconnected guests from the NPS group.

NOTE: To change the host unit, go to **Configuration > ATS > Groups**.

View Device Alarms

Path: Status > ATS > Alarms

View current device alarms, including alarm status icons (see Device Status Icons, page 121) and descriptions.

View Device Status

Path: Status > ATS > Device

The screenshot shows the Schneider Electric Automatic Transfer Switch Application interface. At the top, there is a navigation bar with the Schneider Electric logo, the text "Automatic Transfer Switch Application", the EcoStruxure IT logo with the tagline "Innovation At Every Level" and "Mobile visibility into your devices", and a "No Alarms" status indicator. Below the navigation bar is a green menu bar with options: Home, Status, Control, Configuration, Tests, Logs, and About. The main content area is titled "Status" and contains a "Device Status" section. This section includes a "Total Load" gauge showing 0.0 A, a "Total Output Power" gauge showing 0.00 kVA, and a "Normal Load" indicator. Below these are two sections: "Properties" and "Configuration". The "Properties" section lists Model Number (AP4432A), Serial Number (ATS012345GL22), and Outlets (18). The "Configuration" section lists Name (apc20CAC1), Location (Unknown), and Contact (Unknown). A link "Configure device settings" is provided at the bottom of the configuration section.

View the **Device Status**, **Properties**, and **Configuration** information. Select **Configure device settings** to edit the **Name**, **Location**, or **Contact** information.

View The Unit Status

Path: Status > ATS > Unit

The screenshot shows the 'Unit Status' page of the Schneider Electric Automatic Transfer Switch Application. The page is organized into several sections:

- Unit Status:** A green checkmark indicates 'Source A selected, Switchover Possible'.
- Source Status:**
 - Selected Source: Source A
 - Preferred Source: Source A
 - Source A: Selected
 - Source B: OK
- Power Supplies:**
 - Source A 24V: OK
 - Source B 24V: OK
 - Source A Boost Voltage: OK
 - Source B Boost Voltage: OK
 - 3.3V: OK
- Others:**
 - Phase Synchronization: Sync
 - Front Panel: Unlocked
- Event Counts:**
 - Redundancy Loss: 5
 - Source Switch: 27
 - Over Current: 0
 - Source Preference Change: 0
 - Spike/Dropout: 0
 - Surge/Droop: 30
 - Freq Out of Range: 0

At the bottom of the event counts section, there is a checkbox for 'Reset Event Count (last reset at 12/20/2016 18:00:53)' and 'Apply' and 'Cancel' buttons.

Footer text includes: APC's Web Site | Testdrive Demo | EcoStruxure™ IT | © 2020, Schneider Electric. All rights reserved. | Site Map | Updated: 01/13/2022 at 12:18 (apc2R91c.us.ddns.schneider-electric.com)

View the status of the primary and secondary power source, available power supplies, phase synchronization, and other available features.

View the following Event counts: **Redundancy Loss**, **Source Switch**, **Over Current**, **Source Preference Change**, **Spike/Dropout**, **Surge/Droop**, and **Frequency Out of Range**. To reset these counts to 0, select **Reset Event Count** and click **Apply**. Event counts are set to zero automatically if power is removed from the device or if the Rack ATS controller is updated.

View Load Status

Path: Status > ATS > Load

A marker on a colored green, yellow, and red sliding bar represents the Rack ATS load.

- Green: Normal load range
- Yellow: Near overload range
- Red: Overload range

View Power Measurements

Path: Status > ATS > Measurement

Schneider Electric Automatic Transfer Switch Application EcoStruxure IT Innovation At Every Level Mobile visibility into your devices No Alarms
apc | English | Log Off | Help

Home Status Control Configuration Tests Logs About

Status

ATS Measurement

Input Frequency	
Source A 60 Hz	Source B 60 Hz
Input Voltage (AC)	
Source A 226 V	Source B 223 V
Power Supplies (DC)	
Source A 24V Power Supply 24 V	Source B 24V Power Supply 23 V
Source A Boost Voltage 48 V	Source B Boost Voltage 48 V
3.3V Power Supply 3.4 V	

APC's Web Site | Testdrive Demo | EcoStruxure™ IT © 2021, Schneider Electric. All rights reserved. Site Map | Updated: 09/09/2021 at 20:13 (apc20ca01.us.ddns.schneider-electric.com)

View measurements for **Input Frequency**, **Input Voltage (AC)**, and **Power Supplies (DC)**.

NOTE: The **Power Supplies (DC)** are internal to the Rack ATS—they do not come from connected hardware. Customer support may use these readings for troubleshooting.

View Environment Status

This page allows you to view the following settings and feedback from a connected Temperature Sensor (AP9335T) or Temperature/Humidity Sensor (AP9335TH): **Sensor Name**, **Sensor Location**, **Sensor Type**, **Alarm Status**, **Temperature**, **Peak Temperature**, **Peak Time**, **Reset Time**, **Humidity**, and whether the **Temperature Alarms** and **Humidity Alarms** have been **Enabled** or **Disabled**.

You can configure these settings by clicking **Configure environment settings** or going to **Configuration > ATS > Environment**. See *Configure Temperature and Humidity Sensors*, page 139 for more information.

View Network Status

Path: Status > Network > Network



Automatic Transfer Switch Application



No Alarms

apc | English | Log Off | Help

Home Status Control Configuration Tests Logs About

Status

Current IPv4 Settings

System IP 10.218.117.199	Subnet Mask 255.255.255.0	Default Gateway 10.218.117.1	MAC Address 00 C0 B7 D8 F0 74
Mode DHCP	DHCP Server: 10.218.99.23	Lease Acquired 09/17/2020 09:38	Lease Expires 09/20/2020 09:37

Current IPv6 Settings

Type	IP Address	Prefix Length
Auto	FE80::2C0:B7FF:FED8:F074	64

Domain Name System Status

Active Primary DNS Server 10.169.10.10	Active Secondary DNS Server 10.218.99.55	Active Host Name apcD8F074
Active Domain Name (IPv4/IPv6) nam.gad.schneider-electric.com	Active Domain Name (IPv6) example.com	

Port Speed

Current Speed
100 Full-Duplex

[APC's Web Site](#) | [Testdrive Demo](#) | [EcoStruxure™ IT](#)

© 2020, Schneider Electric. All rights reserved.
[Site Map](#) | Updated: 09/17/2020 at 10:12 (apcs074.us.ddns.schneider-electric.com)

Current IPv4 Settings

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

Current IPv6 Settings

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

Domain Name System Status

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

Port Speed

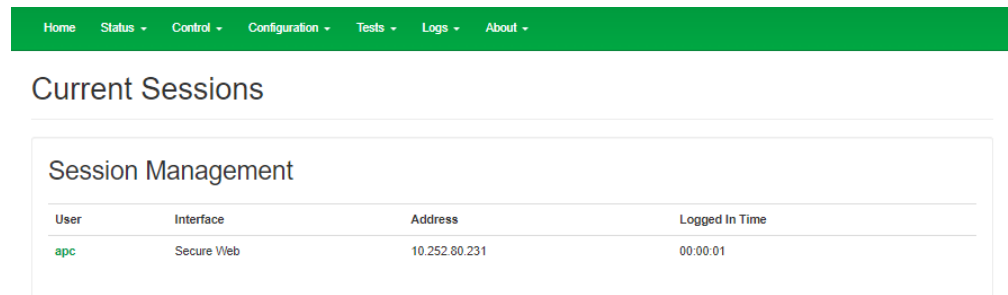
Current Speed: The current speed assigned to the Ethernet port in Mbps, with the option of **half-duplex** (communication in only one direction at a time) or **full-duplex** (communication in both directions on the same channel simultaneously).

Control Tab

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

Manage User Sessions

Path: Control > Security > Session Management



The screenshot shows the Control Tab interface. At the top, there is a green navigation bar with the following menu items: Home, Status, Control, Configuration, Tests, Logs, and About. Below the navigation bar, the text "Current Sessions" is displayed. Underneath, there is a "Session Management" section containing a table with the following data:

User	Interface	Address	Logged In Time
apc	Secure Web	10.252.80.231	00:00:01

The **Session Management** menu displays all active users currently connected to the Rack ATS. To view Information about a user, select their user name. The **Session Details** screen displays basic information about the user including the interface they are logged in to, their IP address, and log in time. At the bottom of the **Session Details** page, there is a **Terminate Session** button. The Administrator can terminate the session of another user.

Reset the Network Interface

Path: Control > Network > Reset/Reboot

APC's Web Site | Testdrive Demo | EcoStruxure™ IT

© 2020, Schneider Electric. All rights reserved.
Site Map | Updated: 09/17/2020 at 11:11 (apcd81074.us.ddns.schneider-electric.com)

This menu gives you the option to reset and reboot various components of the network interface.

Setting	Description
Reboot Management Interface	Rebooting only restarts the Rack ATS unit's Network Management Interface; it does not affect the ON/Off status of the Rack ATS.
Reset All	Returns all Network interfaces to their default settings. Use the default user name and password (apc) to log on after a reset. You will then be required to change your user name and password. Clear the Exclude TCP/IP checkbox to reset all configuration values; mark the Exclude TCP/IP checkbox to reset all values except TCP/IP and EAPoL. The default TCP/IP setting is DHCP. The default for EAPoL access is Disabled .
Reset Only	Reset one or both of the following settings: <ul style="list-style-type: none"> • TCP/IP: Resets only the setting that determines how the Rack ATS must obtain its TCP/IP configuration values, including the EAPoL configuration. The default TCP/IP setting is DHCP. The default for EAPoL access is Disabled. • Event Configuration: Resets events to their default configuration. Any specially configured event or group will also revert to the default value. • Transfer Switch Configuration: Resets the following configurations without changing network configurations such as enabled interfaces and login credentials: <ul style="list-style-type: none"> ◦ LCD On/Off preference ◦ Names for source A and B, source preference, and front panel locking ◦ Frequency deviation, voltage transfer limits, transfer range, and sensitivity ◦ Load thresholds, peak current measurement and timestamp ◦ Event counts and timestamps for event counts ◦ Wired environmental sensor: name and location, peak temperature and timestamps, alarm status (disabled/enabled), temperature/humidity thresholds and hysteresis values Resetting may take up to a minute.

NOTE: This page only resets the current Rack ATS. For options to Reset/Reboot units in an NPS group, see **Configuration > ATS > Groups** and **Status > ATS > Group Status**.

Configuration Tab

Use the Configuration tab to do any of the following:

- Configure settings related to NPS groups, unit identification, power settings, and switching behavior (see [Configure the Rack ATS](#), page 133).
- Configure settings related to security and user management (see [Manage Security Settings](#), page 141).
- Configure settings related to Network connectivity and access to the Web UI/CLI ([Configure Network Settings](#), page 150).
- Configure Notifications (see [Configure Notifications](#), page 161).
- Configure general settings related to the Network Management Interface (see [General Configuration](#), page 166).

Configure the Rack ATS

Configure NPS Groups

Configuration > ATS > Groups

The screenshot shows the Schneider Electric Automatic Transfer Switch Application web interface. The page title is "Group Configuration" and the main content area is titled "Network Port Sharing (NPS) Host Configuration".

Note:

- When resetting to defaults for a guest device with active alarms, these alarms may continue to be reported as active by the host until the host has rebooted.
- In order to change the host designation in an NPS group, the guest unit that will be selected to become the host must have an active network link.


Below the note, there are three buttons: "Host 1" (selected), "Guest 2", and "Guest 3". Below these are two buttons: "Reset/Reboot all" and "ATS to defaults all".

At the bottom of the page, there is a footer with the following text: "APC's Web Site | EcoStruxure™ IT | Product Information" and "© 2022, Schneider Electric. All rights reserved. Site Map | Updated: 07/27/2022 at 15:17 (apc2fadf2.us.ddns.schneider-electric.com)".

You can use this page to do the following:

- View general information about each unit in an NPS Group. Select each unit to show or hide specific information about that unit, and options to change the settings for the individual unit.
- Use the **Reset/Reboot** options to return the Network Management Interfaces in the NPS group to their defaults, including TCP/IP and EAPoL settings.
 - TCP/IP and EAPoL (By default, TCP/IP is set to DHCP and EAPoL is disabled.)
 - LCD On/Off preference
 - Names for source A and B, source preference, and front panel locking
 - Frequency deviation, voltage transfer limits, transfer range, and sensitivity
 - Load thresholds, peak current measurement and timestamp
 - Event counts and timestamps for event counts
 - Wired environmental sensor: name and location, peak temperature and timestamps, alarm status (disabled/enabled), temperature/humidity thresholds and hysteresis values

This option will cause the NMC to reboot. You will be required to change the default user name and password (**apc** and **apc**) after initial log on.

- Use the **ATS to defaults** options to return Network Management Interfaces in the NPS group to their defaults, excluding TCP/IP and EAPoL settings:
 - TCP/IP and EAPoL
 - LCD On/Off preference
 - Names for source A and B, source preference, and front panel locking
 - Frequency deviation, voltage transfer limits, transfer range, and sensitivity
 - Load thresholds, peak current measurement and timestamp
 - Event counts and timestamps for event counts
 - Wired environmental sensor: name and location, peak temperature and timestamps, alarm status (disabled/enabled), temperature/humidity thresholds and hysteresis values
- Remove disconnected guests from the NPS group.
- Select a new host unit by using the **Select Host** option. This option is only available when the target host has a network connection, indicated by a link icon .

Configure Rack ATS Name and Location

Path: Configuration > ATS > Device

Status: View the Rack ATS load in A and the Output Power in kVA.

Name: Enter a descriptive name for the Rack ATS. This will appear on the **Home** tab.

Location: Enter the physical location of the Rack ATS. This will appear on the **Home** tab.

Contact: Enter the person responsible for the Rack ATS. This will appear on the **Home** tab.

Click **Apply** to save your changes or **Cancel** to discard your changes.

Set Preferred Power Source

Path: Configuration > ATS > Source

Status: View the status of the preferred power source.

Source A Name, Source B Name: Enter names of your choice for Source A and Source B.

Preferred Source: Select the power source the Rack ATS will draw from when both sources are available.

Front Panel: Lock or unlock the Front Panel.

Click **Apply** to save your changes or **Cancel** to discard your changes.

Configure Switching Behavior

Path: Configuration > ATS > Frequency/Voltage

DANGER

HAZARDOUS VOLTAGE

Do not operate the Rack ATS outside Rated Voltage (+/- 10%). Voltage limits and transfer ranges represent software control of switching behavior, not input voltages for use.

Failure to follow these instructions will result in death or serious injury.

Model	Rated Voltage (VAC)	Configurable Ranges (VAC)	Narrow Default Range (VAC)	Medium Default Range (VAC)	Wide Default Range (VAC)
AP4421A	230 (L-N)	± 16–25 V	± 16 V	± 20 V	± 25 V
AP4422A	230* (L-N)	± 16–25 V	± 16 V	± 20 V	± 25 V
AP4423A	230* (L-N)	± 16–25 V	± 16 V	± 20 V	± 25 V
AP4424A	230 (L-N)	± 16–25 V	± 16 V	± 20 V	± 25 V
AP4430A	200/208 (L-L)	± 15–30 V	± 15 V	± 22 V	± 30 V
AP4431A	208 (L-L)	± 15–30 V	± 15 V	± 22 V	± 30 V
AP4432A	200/208 (L-L)	± 15–30 V	± 15 V	± 22 V	± 30 V
AP4433A	208 (L-L)	± 15–30 V	± 15 V	± 22 V	± 30 V
AP4434A	208 (L-L)	± 15–30 V	± 15 V	± 22 V	± 30 V
AP4450A	100/120 (L-N)	± 10–23 V	± 10 V	± 16 V	± 23 V
AP4450AJ	100 (L-N)	± 10–15 V	± 10 V	± 12 V	± 15 V
AP4452A	120 (L-N)	± 10–23 V	± 10 V	± 16 V	± 23 V
AP4452AJ	100 (L-N)	± 10–15 V	± 10 V	± 12 V	± 15 V
AP4453A	120 (L-N)	± 10–23 V	± 10 V	± 16 V	± 23 V

*220 V, Korea only.

The voltage transfer range determines the switching behavior for the Rack ATS based on source voltage. When the source voltage goes outside the specified range, the Rack ATS switches to the secondary power source. You can configure Narrow, Medium, or Wide voltage ranges and then set the Rack ATS to the desired range. Ensure that your power sources provide the appropriate power for the Rack ATS (+/- 10% of the Rated Voltage), and use the voltage transfer range to ensure that the Rack ATS does not operate outside the appropriate voltage for extended periods of time.

Frequency/Voltage Configuration

Configuration

Line Frequency
60 Hz

Frequency Deviation
 3 Hz
 5 Hz
 10 Hz

Line VRMS [108 to 132]
 Vrms

VRMS Wide Limit [10 to 23]
 V

VRMS Medium Limit [10 to 23]
 V

VRMS Narrow Limit [10 to 23]
 V

Sensitivity
 High
 Low

Voltage Transfer Range
 Wide
 Medium
 Narrow

Frequency Deviation: Frequency deviation beyond the set value will cause the Rack ATS to switch power sources.

NOTE: If the frequency is at 50 Hz (see [View Power Measurements](#), page 127) and the **Sensitivity** is set to **High**, this value should be 3 or 5.

Line VRMS: Rated voltage for the Rack ATS (also called Nominal Input). VRMS limits and transfer ranges are based on this value.

Sensitivity: Control how much power fluctuation the Rack ATS tolerates before switching to the secondary power source. With a **Low** sensitivity, the Rack ATS waits 4 milliseconds (ms) before switching to the alternate power source. (This can help prevent excessive switching if your source voltage has excessive or frequent fluctuation.) With a **High** sensitivity, the Rack ATS waits 2 ms before switching to the alternate power source.

NOTE: If the frequency is at 50 Hz and the **Frequency Deviation** is set to 10, **Sensitivity** should be set to **Low**.

Limits and Transfer Range: The **Transfer Range** is the **Line VRMS** plus or minus a configured Limit (**Wide**, **Medium**, or **Narrow**). The **Transfer Range** determines the switching behavior for the Rack ATS based on source voltage: when the source voltage moves outside the **Transfer Range**, the Rack ATS switches to the secondary power source.

- **VRMS Wide, Medium, and Narrow Limit:** set configuration options for the **Transfer Range**.
- **Transfer Range:** Decide whether the Rack ATS will switch power sources based on the **Wide**, **Medium**, or **Narrow VRMS Limit**. The **Transfer Range** can only be set to one **Limit** at a time.

NOTE: The **Voltage Transfer Range** and **Limit** must remain within the absolute maximum ratings of the Rack ATS: 85–265 VRMS. At any voltage below 85 VRMS or above 265 VRMS, the Rack ATS will switch power sources regardless of configuration.

Example: A Rack ATS is set to the following configuration:

Line VRMS = 208,

VRMS Wide Limit = 10,

Transfer Range = Wide.

The Rack ATS will switch sources when the voltage goes below 198 VRMS or above 218 VRMS (208 ±10 VRMS).

Click **Apply** to save your changes or **Cancel** to discard your changes.

Configure Load Thresholds

Path: Configuration > ATS > Load

The screenshot shows the 'Load Configuration' page in the Schneider Electric Automatic Transfer Switch Application. The page is divided into two main sections: 'Status' and 'Configuration'.

Status Section:

- Current:** 0.5 A
- Normal Load:** Indicated by a green bar on the meter.
- Peak Current:** 0.7 A

Configuration Section:

- Low Load Warning [0 to 16]:** 0 A
- Near Overload Warning [0 to 16]:** 12 A
- Overload Alarm [0 to 16]:** 16 A
- Peak Current:** Reset (last reset at 09/17/2020 09:30:34)
- Buttons:** Apply, Cancel

Footer information includes: APC's Web Site | Testdrive Demo | EcoStruxure™ IT, © 2020, Schneider Electric. All rights reserved. Site Map | Updated: 09/17/2020 at 09:54 (apcd9074.us.doms.schneider-electric.com)

Status: View the current in A, and the Peak Current in kVA, for the device, phases, and banks. The indicator in the green, yellow, and red meter shows the load status: normal, near overload, or overload.

Load Thresholds: The Rack ATS generates an alarm when any bank exceeds its rated value. Set the number of amps to trigger a **Low Load Warning**, **Near Overload Warning**, and **Overload Alarm**.

NOTE: If a circuit breaker trips, there is no definitive indication that the circuit breaker is open. However, the current for that bank will drop. Set the **Low Load Warning** to 1 A for these reasons :

- The default setting for the **Low Load Warning** is 0 amps. This effectively disables the warning; with this setting, the Web UI will not indicate that a circuit breaker may have been tripped.
- A 1-A detection threshold for the **Low Load Warning** will help to indicate that a circuit breaker may have tripped.

Peak Current: Reset the peak current.

Click **Apply** to save your changes or **Cancel** to discard your changes.

Turn the LCD Display On or Off


Path: Configuration > ATS > LCD On/Off

Select whether you want the LCD Screen to be **On** or **Off**, then click **Apply**.

Configure Temperature and Humidity Sensors

Path: Configuration > ATS > Environment

NOTE: To use this feature, you must have connected an optional APC Temperature Sensor (AP9335T) or APC Temperature/Humidity Sensor (AP9335TH) to the Rack ATS.

At the top of this page, you can see whether a Temperature or Temperature and Humidity sensor is connected (**Sensor Type**), the current **Temperature** and/or **Humidity** readings from the sensor, and the **Alarm Status** of the sensor. You can also click the thermometer icon  in the upper-right corner of the page to toggle between Fahrenheit and Celsius.

About Temperature and Humidity Settings

General settings:

- **Sensor Name:** Enter a custom name for the sensor.
- **Sensor Location:** Enter the location of the sensor.

Temperature settings:

- If the **High Temperature Threshold** is reached and **Temperature Alarms** are set to **Enabled**, the system generates a Warning alarm.
- If the **Maximum Temperature Threshold** is reached and **Temperature Alarms** are set to **Enabled**, the system generates a Critical alarm.
- The **Peak Temperature** is the highest temperature recorded since the last **Reset**. **Peak Time** shows the time and date when the **Peak Temperature** was recorded.

Humidity settings:

- If the **Low Humidity** threshold is reached and **Humidity Alarms** are set to **Enabled**, the system generates a Warning alarm.
- If the **Minimum Humidity** threshold is reached and **Humidity Alarms** are set to **Enabled**, the system generates a Critical alarm.

Hysteresis: This value specifies how far past a threshold the temperature or humidity must return to clear a threshold violation.

- For Maximum and High temperature threshold violations, the clearing point is the threshold minus the hysteresis.
- For Minimum and Low humidity threshold violations, the clearing point is the threshold plus the hysteresis.

Increase the value for Temperature Hysteresis or Humidity Hysteresis to avoid multiple alarms if temperature or humidity that has caused a violation then wavers slightly up and down. If the hysteresis value is too low, such wavering can cause and clear a threshold violation repeatedly.

Example of rising but wavering temperature: The maximum temperature threshold is 85 °F, and the temperature hysteresis is 3 °F. The temperature rises above 85 °F, violating the threshold. It then wavers down to 84 °F and then up to 86 °F repeatedly, but no clearing event and no new violation occur. For the existing violation to clear, the temperature would have to drop to 82 °F (3 °F below the threshold).

Example of falling but wavering humidity: The minimum humidity threshold is 18%, and the humidity hysteresis is 8%. The humidity falls below 18%, violating the threshold. It then wavers up to 24% and down to 13% repeatedly, but no clearing event and no new violation occur. For the existing violation to clear, the humidity would have to rise to above 26% (8% past the threshold).

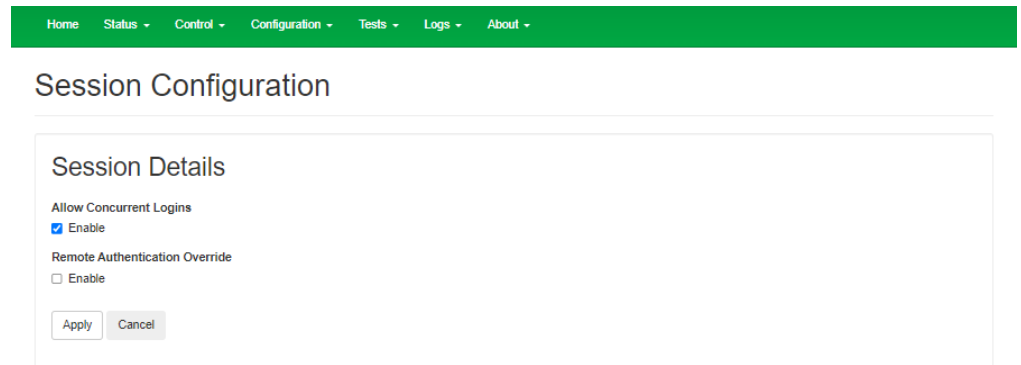
To Configure Temperature and Humidity Sensors

1. Enter values for the Temperature and Humidity thresholds.
2. Enter the **Hysteresis** values.
3. Enable alarm generation as desired.
4. Click **Apply**.

Manage Security Settings

Manage Settings for User Sessions

Path: Configuration > Security > Session Management



The screenshot shows a web interface for Session Configuration. At the top is a green navigation bar with links: Home, Status, Control, Configuration, Tests, Logs, and About. Below the navigation bar is the title "Session Configuration". The main content area is titled "Session Details" and contains two settings:

- Allow Concurrent Logins:** A checkbox labeled "Enable" is checked.
- Remote Authentication Override:** A checkbox labeled "Enable" is unchecked.

At the bottom of the settings area are two buttons: "Apply" and "Cancel".

Allow Concurrent Logins: Select **Enable** to allow two or more users to log on at the same time. Each user has equal access and each interface (HTTP, FTP, telnet, serial connection, etc.) counts as a logged-in user.

Remote Authentication Override: The Rack ATS supports RADIUS storage of passwords on a server. However, if you enable this override, the Rack ATS will allow a local user to log on using the password stored locally on the Rack ATS. For more information, see [Manage Local User Settings](#), page 142 and [Manage Remote User Settings](#), page 145.

Enable Ping Response

Path: Configuration > Security > Ping Response

IPv4 Ping Response: Select the **Enable** check box to allow the Rack ATS to respond to network pings. Clear the check box to disable a Rack ATS response. If the ping response is enabled and the Rack ATS does not respond, see “Unable to ping the ATS”, page 185 under Rack ATS Access Problems, page 185.

This does not apply to IPv6.

Manage Local User Settings

Path: Configuration > Security > Local Users > Management

Home Status Control Configuration Tests Logs About

User Management Configuration

Super User Management

User Name	User Type	User Description
apc	Super User	User Description

General User Management

User Name	User Type	User Description
device	Device	User Description
readonly	Read-Only	User Description

Add User

Click **Add User** to add a new user, or select a **User Name** to edit that user's configuration:

- **Access:** Select the **Enable** check box to allow access to the Rack ATS.
- **User Name:** Enter a new user name.
- **Current Password, New Password, Confirm Password:** Enter a new password in both the New Password and Confirm Password fields. You must enter a password for new users. Blank passwords, (passwords with no characters) are not allowed.

NOTE: The maximum length for both the name and password is 64 bytes, with less than 64 characters for multi-byte characters. Values greater than 64 bytes for **Name** and **Password** may be truncated. To change an Administrator/Super User setting, you must enter all three fields.

- **User Type:** Select the user type from the drop-down list.

Option	Description
Administrator	Read-write access to all menus.
Device	Read-write access to device-related menus. Can be enabled or disabled by Administrators.
Read-Only	Read-only access. Can be enabled or disabled by Administrators.
Network-Only	Read-write access to network-related menus. Can be enabled or disabled by Administrators.

- **User Description:** Enter any additional identification details here.
- **Session Timeout:** Enter the number of minutes (3 by default) the Rack ATS waits before logging off an inactive user. If you change this value, you must log off for the change to take effect.

NOTE: If a user closes the Web UI without logging off, they are still considered logged on for the time specified in the **Session Timeout** field. This can help prevent other users from taking the place of a user who leaves the Web UI.

- **Serial Remote Authentication Override:** Use Serial Remote Authentication Override to bypass RADIUS by using the serial console (CLI) connection. This screen enables Serial Remote Authentication Override for the selected user, but, in order to work, it must also be enabled globally through the Session Management screen (see *Manage User Sessions*, page 130).
- **User Preferences:**

Option	Description
Event Log Color Coding	Mark the 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. Red: Alarm Severity = Critical. A critical alarm exists, which requires immediate action. Orange: Alarm Severity = Warning. An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed. Green: Alarm Cleared. The conditions that caused the alarm have improved. Black: No alarms are present. The Rack ATS and all connected devices are operating normally.
Export Log Format	Configure which format the Event Log should be displayed in when exported (downloaded). Tab (default) allows fields to be tab-delimited whereas CSV is comma-separated.
Temperature scale	Select the default temperature scale, US Customary (Fahrenheit) or Metric (Celsius).
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.

Click **Next**, and then click **Apply** to save or **Cancel** to return to the User Management Configuration page.

Configure Default User Settings

Path: Configuration > Security > Local Users > Default Settings

Determine the default values to populate in each of the fields when the Super User or Administrator-level account creates a new user. These values can be changed before the settings are applied to the system.

For remote users (user accounts not stored in the system that are remotely authenticated such as RADIUS) these are the values used for those that are not provided by the authenticating server. For example, if a RADIUS server does not provide the user with a temperature preference, the value defined in this section will be used.

- **Access:** Select the **Enable** check box to allow access to the Rack ATS.
- **User Type:** Select the user type from the drop-down list.

Option	Description
Administrator	Read-write access to all menus.
Device	Read-write access to device-related menus. Can be enabled or disabled by Administrators.
Read-Only	Read-only access. Can be enabled or disabled by Administrators.
Network-Only	Read-write access to network-related menus. Can be enabled or disabled by Administrators.

- **User Description:** Enter any additional identification details here.
- **Session Timeout:** Enter the number of minutes (3 by default) the Rack ATS waits before logging off an inactive user. If you change this value, you must log off for the change to take effect.

NOTE: If a user closes the Web UI without logging off, they are still considered logged on for the time specified in the **Session Timeout** field. This can help prevent other users from taking the place of a user who leaves the Web UI.

- **Bad Login Attempts:** Set the number of failed login attempts the user can have. Select from 0 to 99 attempts. 0 = unlimited.
- **User Preferences:**

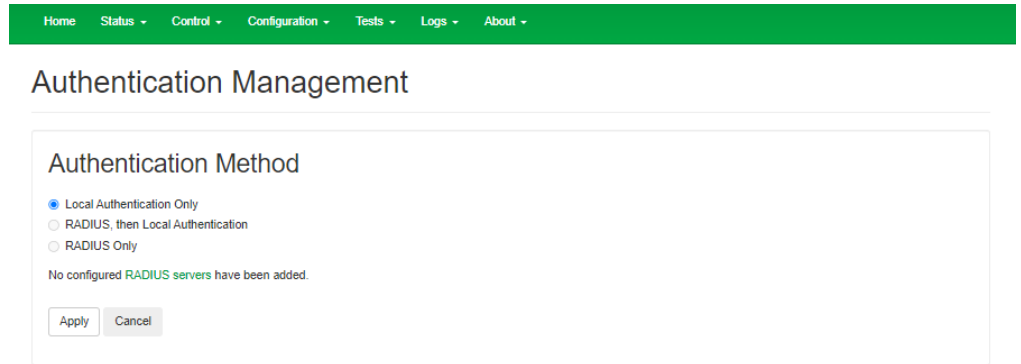
Option	Description
Event Log Color Coding	Mark the check box to enable color-coding of alarm text recorded in the Event Log. System event entries and configuration change entries do not change color. Red: Alarm Severity = Critical. A critical alarm exists, which requires immediate action. Orange: Alarm Severity = Warning. An alarm condition requires attention and could jeopardize your data or equipment if its cause is not addressed. Green: Alarm Cleared. The conditions that caused the alarm have improved. Black: No alarms are present. The Rack ATS and all connected devices are operating normally.
Export Log Format	Configure which format the Event Log should be displayed in when exported (downloaded). Tab (default) allows fields to be tab-delimited whereas CSV is comma-separated.
Temperature scale	Select the default temperature scale, US Customary (Fahrenheit) or Metric (Celsius).
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.

- **Password Requirements:**

Option	Description
Strong Passwords	Configure whether new passwords created for user accounts will require at least one lowercase character, one uppercase character, one number, and one symbol.
Password Policy	Enter the number of days after which users will be required to change their passwords. A value of 0 days (the default) disables this feature.

Manage Remote User Settings

Path: Configuration > Security > Remote Users > Authentication



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

- When a user accesses a Rack ATS 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 Rack ATS are case-sensitive, and have a 64 byte maximum, supporting up to 64 ASCII characters; less for multi-byte languages. Passwords with no characters (blank passwords) are not allowed.

Specify how you want remote users to be authenticated at logon. 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. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used.
- **RADIUS Only:** RADIUS is enabled. Local authentication is disabled.

NOTE: If **RADIUS Only** is selected, and the RADIUS server is unavailable or improperly configured, remote access is unavailable to all users. You must use a serial connection to the CLI and change the **access** setting to **local** or **radiusLocal** to regain access. For example, the command to change the access setting to **local** would be `radius -a local`.

For information about local authentication (not using the centralized authentication of a RADIUS server), see the *Security Handbook* on www.apc.com.

Configure a RADIUS Server

Path: Configuration > Security > Remote Users > RADIUS

Use this option to do the following:

- List the RADIUS servers (a maximum of two) available to the Rack ATS and the Reply Timeout period for each.
- Select a server, and configure the parameters for authentication by a new RADIUS server.
- Select a listed RADIUS server to display and modify its parameters.

Setting	Definition
RADIUS Server	The server name or IP address (IPv4 or IPv6) of the RADIUS server. Select a link to configure the server.
Port	The port the RADIUS server uses to authenticate users (1812 by default). The Rack ATS supports ports 1812, and 5000 to 32768.
Secret	The shared secret between the RADIUS server and the Rack ATS.
Reply Timeout	The time in seconds that the Rack ATS waits for a response from the RADIUS server.
Test Settings	Enter the Super User or 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. (Not recommended)

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 *Security Handbook* on www.apc.com.

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 UI only). See your RADIUS server documentation for information about the RADIUS users file, and see the *Security Handbook* (on www.apc.com) for an example.
3. 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 names for ATTRIBUTE and VALUE keywords, but not for 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`.

```
DEFAULTAuth-Type = System
APC-Service-Type = Admin
```

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

```
bconnersAuth-Type = System
APC-Service-Type = Admin
thawkAuth-Type = System
APC-Service-Type = Device
```

Supported RADIUS servers: FreeRADIUS v1.x and v2.x, and Microsoft Server 2008 and 2012 Network Policy Server (NPS) are supported. Other commonly available RADIUS applications may work but may not have been fully tested.

NOTE: See the *Security Handbook* for more information on using RADIUS.

Firewall Menus

Path: Configuration > Security > Firewall > Configuration

Enable or disable the firewall functionality. The configured policy is listed by default. Select the **Enable** check box to enable the firewall. The check box is un-checked by default.

- Click **Apply** to confirm a firewall policy you have selected to enable. The **Firewall Confirmation** page will open.
 - The **Confirmation** page contains a recommendation to test the firewall before enabling. It is not mandatory.
 - The first hyperlink goes to the **Firewall Policy** page.
 - The second hyperlink goes to the **Firewall Test** page.
 - Click **Apply** to enable the firewall and return to the **Configuration** page.
 - Click **Cancel** to return to the **Configuration** page without enabling the firewall.
- Click **Cancel**: No new selection will be enabled. You stay on the **Configuration** page.

Active Policy

Path: Configuration > Security > Firewall > Active Policy

Select an active policy from the **Available Policies** drop-down list, and view the validity of that policy. The current active policy is displayed by default; you can select another from the list.

- Click **Apply** to enable your changes. If a different firewall was selected and enabled, the change is effective immediately. If a newly configured firewall policy has been selected, it is recommended that you test the new firewall before enabling it. (You can test the new firewall from **Configuration > Security > Firewall > Configuration**.)
- Click **Cancel** to restore the original active policy and stay on the **Active Policy** page.

Active Rules

Path: Configuration > Security > Firewall > Active Rules

When a firewall is enabled, this read-only page lists the individual rules that are being enforced by a current active policy. See [Create/Edit Policy](#), page 147 for descriptions of the fields (**Priority, Destination, Source, Protocol, Action, and Log**).

Create/Edit Policy

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

Use this page to create a new policy, or delete or edit an existing policy.

You cannot delete an active, enabled firewall policy. You can edit a running policy, but it is not recommended as changes are applied immediately. Instead, disable the firewall, edit the policy, test it, and then re-enable the policy.

Create a new policy

Click **Add Policy**, and type in the file name for the new firewall file. The filename should have a .fwl file extension. If left without a file extension, .fwl will be appended to the name automatically.

- Click **Apply**: If the filename is legal, the empty file firewall policy file will be created. It will be located in the /fwl folder with the other policies on the system.
- Click **Cancel** to return to the previous page without creating a new firewall file.

Edit an existing policy

Select **Edit Policy** to go to the edit page. You can edit an firewall policy which is not active.

Warning page: If you attempt to edit the active enabled policy, a warning page will open. **Editing the active firewall policy will cause all changes made to be applied immediately. It is recommended to disable the firewall and test the policy before enabling it.**

- Click **Apply** to leave the Warning page and return to the **Edit Policy** page.
 - Click **Cancel** to leave the Warning page and return to the **Create/Edit Policy** page.
1. Select the policy you want to edit from the **Policy Name** drop-down list, and click **Edit Policy**.
 2. Click **Add Rule** or select the **Priority** of an existing rule to go to the **Edit Rule** page. From this page, you can change the rule settings or delete the selected rule.

Setting	Description
Priority	If two rules conflict, the rule with the higher priority will determine what happens. The highest priority is 1; the lowest is 250.
Type	host : In the IP/any field, you will enter a single IP address. subnet : In the IP/any field, you will enter a subnet address. range : In the IP/any field, you will enter a range of IP addresses.
IP/any	Specify the IP address or range of addresses this rule applies to, or select one of the following: - any : The rule applies regardless of the IP address. - anyipv4 : The rule applies for any IPv4 address. - anyipv6 : The rule applies for any IPv6 address.
Port	Specify a port the rule will apply to: - None : The rule will apply to any port. - Common Configured ports : Select a standard port. - Other : Specify a non-standard port number.
Protocol	Specify which protocol the rule applies to: - any : any protocol. - tcp : used for more reliable information transfer between applications. - udp : alternative to TCP using for faster, lower bandwidth information. transfer. Though it has fewer delays, UDP is less reliable than TCP. - icmp : used to report errors for troubleshooting. - icmpv6 : used to report errors for troubleshooting on applications using IPv6.
Action	allow : Allow the packet that matches this rule. discard : Discard the packet that matches this rule.
Log	If this rule applied to a packet, regardless of whether the packet is blocked or allowed, this will add an entry to the Firewall Log (see "Firewall log" on page 123).

It is recommended that you add one of the following as the lowest priority rule in your firewall policy:

- To use the firewall as a white list, add
250 Dest any / Source any / protocol any / discard
- To use the firewall as a black list, add
250 Dest any / Source any / protocol any / allow

Delete a policy

Select **Delete Policy** to open the Confirm Deletion page.

Click **Apply** to confirm and the selected firewall file is removed from the file system.

Load Policy

Path: Configuration > Security > Firewall > Load Policy

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

Test

Path: Configuration > Security > Firewall > Test

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

802.1X Security Configuration

Path: Configuration > Security > 802.1X Security

The NMC takes the role of a supplicant in an EAPoL (Extensible Authentication Protocol over LAN) architecture used in IEEE 802.1X port-based network access control. The NMC supports EAP-TLS as an authentication method which requires the user to upload 3 client-side certificates. The private key is stored in an encrypted format. The user needs to provide a valid passphrase to be able to enable 802.1X security access.

NOTE: The NMC supports only EAP-TLS authentication method.

The Web UI offers the following options for EAPoL configuration:

Setting	Description
EAPoL Access	Used to enable or disable 802.1X Security Access. NOTE: The 802.1X security access is disabled by default. The user can enable only when valid certificates and a valid passphrase for the private key are provided by the user.
Supplicant Identifier	Allows the users to set their own supplicant identifier (up to 32 characters including whitespace). NOTE: By default, the supplicant identifier is set to "NMC-Supplicantxx: xx:xx:xx:xx:xx:xx" where six octets of 'xx' are the MAC ID of the NMC.
CA Certificate	Upload/replace or remove a CA root certificate. The supported file formats are PEM (Privacy Enhanced Mail) or the DER (Distinguished Encoding Rules) format with permitted file extensions .pem, .PEM, .der, or .DER.
Private Key Certificate	Upload/replace or remove an encrypted private key. The supported file formats are PEM (Privacy Enhanced Mail) or the DER (Distinguished Encoding Rules) format with permitted file extensions .key or .KEY. NOTE: Unencrypted private key is not accepted.
Private Key Passphrase	Provide the passphrase to decrypt the encrypted private key. Allows up to 64 characters including whitespace.
User/Public Certificate	Upload/replace or remove a user/public certificate. The supported file formats are PEM (Privacy Enhanced Mail) or the DER (Distinguished Encoding Rules) format with permitted file extensions .pem, .PEM, .der, or .DER.

Configure Network Settings

Protocol Configuration Summary

Path: Configuration > Network > Summary

Home	Status	Control	Configuration	Tests	Logs	About
Configuration Summary						
IPv4	Enabled	Configure				
IPv6	Enabled	Configure				
Ping Response	Enabled	Configure				
HTTP	Disabled	Configure				
HTTPS	Enabled	Access	SSL Certificate			
FTP	Enabled	Configure				
Telnet	Disabled	Configure				
SSH/SCP	Enabled	Access	SSH Host Key			
SNMPv1	Disabled	Access	Access Control			
SNMPv3	Disabled	Access	Access Control	User Profiles		
Super User	Enabled	Configure				
RADIUS	Disabled	Authentication	RADIUS			
Administrator	Disabled	Configure				
Device User	Disabled	Configure				
Read-Only User	Disabled	Configure				
Network-Only User	Disabled	Configure				

You can use this page to view all protocols enabled or disabled on your Rack ATS. Select a link for any protocol to go to the appropriate configuration page.

Configure TCP/IP and Communication Settings for IPv4 and IPv6

Path: Configuration > Network > TCP/IP > IPv4

View the current IPv4 address, subnet mask, default gateway, MAC address, and boot mode of the Rack ATS. For information on DHCP and DHCP options, see RFC2131 and RFC2132.

Setting	Description
Enable	Enable or disable IPv4 with this check box.
Manual	Configure IPv4 manually by entering the IP address, subnet mask, and default gateway.
BOOTP	<p>A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Rack ATS requests network assignment from any BOOTP server:</p> <ul style="list-style-type: none"> If the Rack ATS receives a valid response, it starts the network services. If the Rack ATS 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), it uses the previously configured settings so that it remains accessible. <p>Click Next>> to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail:</p> <ul style="list-style-type: none"> Maximum retries: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries. If retries fail: Select Use prior settings (the default) or Stop BOOTP request.
DHCP	<p>The default setting. At 32-second intervals, the Rack ATS requests network assignment from any DHCP server.</p> <ul style="list-style-type: none"> If the Rack ATS receives a valid response, it does not (as previously) require 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.¹ <p>Require vendor specific cookie to accept DHCP Address: By selecting this check box, you can require the DHCP server to provide a cookie which supplies information to the Rack ATS.</p>
<p>NOTE: The default values for these three settings on configuration pages generally do not need to be changed:</p> <ul style="list-style-type: none"> Vendor Class: APC Client ID: The MAC address of the Rack ATS, 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 operation of the Rack ATS.

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 an APC-specific option in a TAG/LEN/DATA format, called the APC Cookie. This is disabled by default.

- APC Cookie. Tag 1, Len 4, Data "1APC"

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

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

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

TCP/IP options

The 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 NTP servers (primary and secondary) that the Rack ATS can use.
- **Time Offset** (option 2): The offset of the Rack ATS unit's subnet, in seconds, from Coordinated Universal Time (UTC).
- **Domain Name Server** (option 6): Up to two Domain Name System (DNS) servers (primary and secondary) that the 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 a user configuration file (.ini file) to download. The **siaddr** field of the DHCP response specifies the IP address of the server from which the Rack ATS will download the .ini file. After the download, the .ini file is used as a boot file to reconfigure the settings.

Configure Network Port Speed

Path: Configuration > 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).

Configure DNS

Path: Configuration > Network > DNS > Configuration

Use the options under **Configuration** to configure the Domain Name System (DNS):

- **Override Manual DNS Settings:** When enabled, configuration data from other sources (typically DHCP) takes precedence over the manual configurations set here.
- **Primary DNS Server or Secondary DNS Server:** Select one of these to specify the IPv4 or IPv6 addresses of the primary and optional secondary DNS server. For the Rack ATS to send e-mail, you must at least define the IP address of the primary DNS server.
 - The Rack ATS waits up to 15 seconds for a response from the primary DNS server or secondary DNS server (if specified). If the Rack ATS does not receive a response within that time, e-mail cannot be sent. Use DNS servers on the same segment as the Rack ATS or on a nearby segment (but not across a wide-area network [WAN]).
 - Define the IP addresses of the DNS servers, then enter the DNS name of a computer on your network to look up the IP address for that computer to verify correct operation.
- **System Name Synchronization:** Allow the system name to be synchronized with the host name so both fields automatically contain the same value.

NOTE: When enabling this feature, the system name identifier can no longer contain a space character (since it will be synchronized to the **Host Name** field).
- **Host Name:** Configure a host name here and a domain name in the **Domain Name** field. Users can then enter a host name in any field in the NMC interface (except e-mail addresses) that accepts a domain name.
- **Domain Name (IPv4/IPv6):** Configure the domain name here only. In all other fields in the NMC interface (except e-mail addresses) that accept domain names, the Rack ATS 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, include a trailing period. The NMC recognizes a host name with a trailing period (such as `mySnmpServer.`) as if it were a fullyqualified domain name and does not append the domain name.
- **Domain Name (IPv6):** Specify the IPv6 domain name here.

Test DNS Configuration

Path: Configuration > Network > DNS > Test

Use this option to send a DNS query that tests the setup of your DNS servers by looking up the IP address. View the result of a test in the **Last Query Response** field, or identify the value to be used for the selected query type:

Query Type Selected	Query Question to Use
by Host	The URL name of the server
by FQDN	The fully qualified domain name of the server, <code>my_server.my_domain</code>
by IP	The IP address of the server
by MX	The mail exchange address of the server

Configure Web Access

Path: Configuration > Network > Web > Access

To activate changes to any of these selections, all users must log off:

Setting	Description
Enable HTTP	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. HTTP is disabled by default.
Enable HTTPS:	Enables Hypertext Transfer Protocol (HTTPS) over Secure Sockets Layer (SSL)/ Transport Layer Security (TLS). SSL and TLS encrypt user names, passwords, and data during transmission, and authenticate the Rack ATS by digital certificate. When HTTPS is enabled, your browser displays a small lock icon. For more information on HTTPS, see "Creating and Installing Digital Certificates" in the <i>Security Handbook</i> , available at www.apc.com . HTTPS is enabled by default.
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. NOTE: For either port, 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: <code>http://152.214.12.114:5000</code> <code>https://152.214.12.114:5000</code>
Minimum Protocol	Select minimum HTTPS security protocol from the drop-down list.
Require Authentication cookie	When the cookie is enabled, the user accessing the unit must have the correct session ID (present in the Web URL), the same remote IP address used to create the session, and the cookie present. When the cookie is disabled or has been deleted, a user can copy and paste the same URL with session ID to a new tab in the same Web browser without being required to log in. For more information, see FAQ article FA235784: <i>Network Management Card 2 (NMC2) "Require Authentication Cookie"</i> .
Limited Status Access	Select Enable to display a public, read-only Web page with basic device status. Select Use as Default Page to make this status page the landing page for the Rack ATS.

NOTE: To find an FAQ article, go to www.apc.com/support, select **FAQS** under Resources and Tools, then enter the article number or title in the Search bar.

Configure SSL Certificate for Web Access

Path: Configuration > Network > Web > SSL Certificate

View current certificate status. Add, replace, or remove a security certificate.

Setting	Description
Status	<ul style="list-style-type: none"> • Not installed: A certificate is not installed, or was installed by FTP or SCP to an incorrect location. Using Add or Replace Certificate File installs the certificate to the correct location, /ssl on the Rack ATS. • Generating: The Rack ATS 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. Select this link to view the contents of the certificate. <p>NOTE: If you install an invalid certificate, or if no certificate is loaded when you enable SSL/TLS, the Rack ATS generates a default certificate, a process which delays access to the interface for up to one minute. You can use the default certificate for basic encryption-based security measures, but a security alert message displays whenever you log on.</p>
Certificate Action:	<ul style="list-style-type: none"> • Add or Replace: Enter or browse to the certificate file created with the Security Wizard. See "Creating and Installing Digital Certificates" in the <i>Security Handbook</i>, available at www.apc.com, to choose a method for using digital certificates created by the Security Wizard or generated by the Rack ATS. • Remove: Delete the current certificate.

Configure CLI Access

Path: Configuration > Network > Console > Access

Enable Telnet: Telnet transmits user names, passwords, and data without encryption. Telnet is disabled by default.

Enable SSH: SSH transmits user names, passwords, and data in encrypted form, which helps to protect against attempts to intercept, forge, or alter data during transmission. SSH is enabled by default.

Telnet Port: The Telnet port (23 by default) is used to communicate with the Rack ATS. 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 (22 by default) is used to communicate with the Rack ATS. 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.

Configure SSH Host Key

Path: Configuration > Network > Console > 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 `/ssh` directory (the required location on the Rack ATS):
 - A 1024-bit or 2048-bit host key created by the Security Wizard
 - A 2048-bit RSA host key generated by the Rack ATS

Certificate Action:

- **Add or Replace:** Browse to and upload a host key file created by the Security Wizard. To use the Security Wizard, see the *Security Handbook*, available at www.apc.com.

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 one minute to create a host key, and the SSH server is not accessible during that time.
- **Host Key Fingerprint:** A fingerprint helps authenticate a server. If the Security Wizard is used to generate the host key, it also generates the fingerprint, which is displayed here when SSH is enabled and the host key is in use. When you first connect to the device using SSH, compare the fingerprint presented by the SSH client to the fingerprint that the Security Wizard generated to ensure that they match. (Almost all SSH clients display the fingerprint.)
- **Remove:** Remove the current host key.

NOTE: 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 Options

All user names, passwords, and community names for SNMPv1 are transferred over the network as plain text. If your network requires the high security of encryption, disable SNMPv1 access and use SNMPv3 instead.

When using Data Center Expert to manage a Rack ATS on the public network, you must have the same version of SNMP (1 or 3) enabled on both the Rack ATS interface and the Data Center Expert interface. Read access will allow the Data Center Expert to receive traps from the Rack ATS, but Write access is required while you set the Data Center Expert as a trap receiver.

For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available at www.apc.com.

Network Port Sharing

All Rack ATS units in a group can be accessed through the Host Rack ATS via SNMP "ats5g" OIDs available in our PowerNet-MIB.

The full path to these OIDs is: iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).apc(318).products(1).hardware(1).ats5g(33)

Individual Rack ATS units can be identified in the SNMP MIB tables by viewing the corresponding "Module" OIDs in each table. These Module OIDs will return the Display ID of the Rack ATS.

Example Module OIDs: ats5gIdentConfigModuleID, ats5gSwitchModuleID, ats5gEnvModuleID, ats5gBankModuleID

In order to be backwards compatible with previous versions, the Host Rack ATS will always be the first index in any table that supports multiple Rack ATS units. In addition, after the Rack ATS group is set up, the index order of guest Rack ATS units should not change even if the Display ID is changed or a unit temporarily loses communication. The index order should only change if you manually remove a Rack ATS from the group.

An MIB table walk should skip the indexes associated with a Rack ATS that has temporarily lost communication.

SNMPv1

SNMPv1 is disabled by default. SNMPv2c is supported under SNMPv1 in this configuration.

Access

Path: Configuration > Network > SNMPv1 > Access

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

Access Control

Path: Configuration > Network > SNMPv1 > Access Control

You can configure up to four access control entries to specify which Network Management Systems (NMSs) 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 IPv4 and IPv6 addresses, host names, or IP address masks. To edit the access control settings for a community, select its community name.

NOTE: 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.

NOTE: 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.

Setting	Description
Community Name	The name that an NMS must use to access the community. The maximum length is 16 ASCII characters.
NMS IP/ Host Name	The IPv4 or IPv6 address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows: <ul style="list-style-type: none"> - 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) or 255.255.255.255: Access by any NMS on any segment.
Access Type	The actions an NMS can perform through the community. <ul style="list-style-type: none"> - Read: GETs only, at any time - Write: GETs at any time, and SETs when no user is logged onto the Web UI or CLI. - Write+: GETs and SETs at any time. - Disable: No GETs or SETs at any time.

SNMPv3

SNMPv3 is disabled by default.

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

NOTE: To use SNMPv3, you must have an MIB program that supports SNMPv3.

Access

Path: Configuration > Network > SNMPv3 > Access

SNMPv3 Access: Enables SNMPv3 as a method of communication with this device.

User Profiles

Path: Configuration > Network > SNMPv3 > User Profiles

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

Setting	Description
User Name	The identifier of the user profile. SNMPv3 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 (<code>hidden crypt .phrase</code> , by default) that increases the privacy of the data (by means of encryption) that an NMS is sending to this device or receiving from this device through SNMPv3.
Authentication Protocol	The APC implementation of SNMPv3 supports SHA or MD5 authentication. Authentication will not occur unless an authentication protocol is selected.
Privacy Protocol	The implementation of SNMPv3 supports AES or DES as the protocols for encrypting and decrypting data. Privacy of transmitted data requires that a privacy protocol is selected and that a privacy passphrase is provided in the request from the NMS. When a privacy protocol is enabled but the NMS does not provide a privacy passphrase, the SNMP request is not encrypted. NOTE: You cannot select the privacy protocol if no authentication protocol is selected.

Access Control

Path: Configuration > Network > SNMPv3 > Access Control

You can configure up to four access control entries to specify which Network Management Systems (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.

NOTE: If you leave the default access control entry unchanged for a user profile, all Network Management Systems using that profile have access to this device.

NOTE: 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, select its user name.

Setting	Description
Access	Select Enable to activate the access control specified by the parameters in this access control entry.
User Name	Select the user profile to which this access control entry will apply. The choices available are the four user names that you configure on the user profiles page (under Configuration > Network > SNMPv3 > User Profiles).
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: <ul style="list-style-type: none"> - 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) or 255.255.255.255: Access by any NMS on any segment.

Configure FTP Server

Path: Configuration > Network > FTP Server

The FTP Server settings enable or disable access to the FTP server. FTP is disabled by default.

By default, the FTP server communicates with the Rack ATS through TCP/IP port 21. The FTP server uses both the specified port and the port one number lower than the specified port.

You can change the **Port** setting to the number of any unused port from 5001 to 32768 for added security. Users must then use a colon (:) to specify the non-default port number.

For example, for port 5001 and IP address 152.214.12.114, the command would be `ftp 152.214.12.114:5001`.

NOTE: FTP transfers files without encryption. For higher security, transfer files with Secure CoPy (SCP). Secure SHell (*SSH*) is enabled by default, and enables SCP automatically. However, SCP will not allow a file transfer until the Super User default password (**apc**) is changed. At any time that you want a Rack ATS to be accessible for management by Data Center Expert, FTP server access must be enabled in the Rack ATS interface.

NOTE: You can use FTP or SCP to configure and update the Rack ATS with Data Center Expert or EcoStruxure IT as long as the same protocol is enabled on both the Rack ATS and Data Center Expert or EcoStruxure IT. See your Data Center Expert or EcoStruxure IT documentation for details.

For detailed information on enhancing and managing the security of your system, see the *Security Handbook*, available at www.apc.com.

Wi-Fi Configuration with AP9834

Path: Configuration > Network > Wi-Fi

Reserved for future use.

Configure Notifications

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
 - SNMP traps
 - Syslog notification
- Indirect notification
 - Event log. If no direct notification is configured, users must check the log to determine which events have occurred.

You can also log system performance data to use for device monitoring. See [Configure Logs, page 169](#) for information on how to configure and use this data logging option.

- Queries (SNMP GETs).

SNMP enables an NMS to perform informational queries. For SNMPv1, which does not encrypt data before transmission, configuring the most restrictive SNMP access type (READ) enables informational queries without the risk of allowing remote configuration changes. You can configure the access type under

For more information on SNMP, see [SNMP Options, page 157](#).

Configure Notifications By Event

Path: Configuration > Notification > Event Actions > By Event

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

1. Select an event category or sub-category to see the related event lists.
2. Select an event name to view the current configuration, such as recipients to be notified by email, or Network Management Systems (NMSs) to be notified by SNMP traps. If no Syslog server is configured, items related to Syslog configuration are not displayed. You can also disable event logging or Syslog, or disable notification for specific e-mail recipients or trap receivers.

NOTE: When viewing details of an event configuration, you cannot add or remove recipients or receivers. To add or remove recipients or receivers, see the following sections:

- [Identify Syslog Servers, page 169](#)
- [Recipients, page 164](#)
- [Configure Trap Receivers, page 165](#)

Configure Notifications By Group

Path: Configuration > Notification > Event Actions > By Group

To configure a group of events simultaneously:

1. Select how to group events for configuration:
 - You can select events by **Severity**, and then select one or more severity levels. You cannot change the severity of an event.
 - You can select events by **Category**, and then select events in one or more pre-defined categories.
2. Click **Next** to select an event action.

To select any action except **Logging** (the default), you must first have at least one relevant recipient or receiver configured.
3. Click **Next** to do one of the following:
 - If you selected **Logging** on the previous screen and have not configured a Syslog server, select **Configure Event Log**.
 - If you selected **Logging** on the previous screen and have configured a Syslog server, select **Event Log** or **Syslog**.
 - If you selected **Email Recipients** on the previous screen, select the e-mail recipients to configure.
 - If you selected **Trap Receivers** on the previous screen, select the trap receiver to configure.
4. Click **Next** to configure notification parameters. These configuration fields define e-mail parameters to send notifications:
 - If you are configuring **Logging** settings, select **Enable Notification** or **Disable Notification**.
 - If you are configuring **Email Recipients** or **Trap Receivers**, select **Enable Notification** or **Disable Notification** and set the notification parameters.
5. Click **Next** to view pending actions and do one of the following:
 - Click **Apply** to accept the changes.
 - Click **Cancel** to revert to the previous settings.

Email Notification Parameters: These configuration fields define e-mail parameters for sending notifications of events. You can access notification parameters by selecting the receiver or recipient name.

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

NOTE: You can also set notification parameters for events that have an associated clearing event.

Set Up E-mail Notifications

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

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

Server

Path: Configuration > Notification > E-mail > Server

This screen lists your primary and secondary DNS servers and displays the following fields:

Select **Active Primary DNS Server** or **Active Secondary DNS Server** to configure the DNS Servers (from the **Configuration > Network > DNS > Configuration**) page.

Setting	Description
From Address	<p>The contents of the From field in e-mail messages sent by the Rack ATS.</p> <ul style="list-style-type: none"> • Use the format <i>user@[IP_address]</i> if an IP address is specified as Local SMTP Server. • Use the format <i>user@domain</i> if DNS is configured and the DNS name is specified as Local SMTP Server. <p>NOTE: The local SMTP server may require that you use a valid user account on the server for this setting. Check the server documentation.</p>
SMTP Server	<p>The IPv4/ IPv6 address or DNS name of the local SMTP server.</p> <p>NOTE: This definition is required only when the SMTP server is set to Local.</p>
Port	<p>The SMTP port number, with a default of 25. Supported ports include 25, 465, 587, 2525, and 5000 to 32768.</p>
Authentication	<p>Select Enable if the SMTP server requires authentication.</p> <p>User Name, Password, and Confirm Password: If your mail server requires authentication, enter your user name and password here. This performs a simple authentication, not SSL/TLS.</p>
Use SSL/TLS	<p>Select when encryption is used.</p> <ul style="list-style-type: none"> • Never: The SMTP server does neither requires nor supports encryption. • If Supported: The SMTP server advertises support for STARTTLS but doesn't require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given. • Always: The SMTP server requires the STARTTLS command to be sent on connection to it. • Implicitly: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server.
Require CA Root Certificate	<p>This should only be enabled if the security policy of your organization does not allow for implicit trust of SSL/TLS connections. If this is enabled, a valid root CA certificate must be loaded onto the Rack ATS for encrypted e-mails to be sent.</p>
File Name	<p>This field is dependent on the root CA certificates installed on the Rack ATS and whether or not a root CA certificate is required.</p>

Recipients

Path: Configuration > Notification > E-mail > Recipients

Specify up to four e-mail recipients. Click **Add Recipient**, or select a name to configure the settings.

Setting	Description
E-mail Recipient	
Generation	Enable (default) or disable sending e-mail to the recipient.
To Address	<p>The user name and domain name 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.</p> <p>To bypass the DNS lookup of the IP address of the mail server, type 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.</p>
Format	The Long format contains name, location, contact, IP address, serial number of the device, date and time, event code, and event description. The Short format provides only the event description.
Language:	The language the e-mail notification will be sent in. This depends on the installed language pack (if applicable).
Server	<p>Select one of the following methods for routing e-mail:</p> <ul style="list-style-type: none"> • Local: This is through the site-local SMTP server. This recommended setting uses a site-local SMTP server to send e-mail. Choosing this setting limits delays and network outages and retries sending e-mail for many hours. When choosing the Local setting you must also enable forwarding at the SMTP server of your device and set up a special external e-mail account to receive the forwarded e-mail. Check with your SMTP server administrator before making these changes. • Recipient: This is the SMTP server of the recipient. The Rack ATS performs an MX record look-up on the recipients e-mail address and uses that as its SMTP server. The e-mail is only sent once so it could easily be lost. • Custom: This setting enables each e-mail recipient to have its own server settings. These settings are independent of the local SMTP server settings (configured under Configuration > Notification > E-mail > Server).
Custom E-mail server Settings	
From Address:	<p>The contents of the From field in e-mail messages sent by the Rack ATS:</p> <ul style="list-style-type: none"> • In the format user@[IP_address] (if an IP address is specified as Local SMTP Server) • In the format user@domain (if DNS is configured and the DNS name is specified as Local SMTP Server) in the e-mail messages. <p>NOTE: The local SMTP server may require that you use a valid user account on the server for this setting. See the server documentation.</p>
SMTP Server:	<p>The IPv4/ IPv6 address or DNS name of the local SMTP server.</p> <p>NOTE: This definition is required only when the SMTP server is set to Local.</p>
Port	The SMTP port number, with a default of 25. Supported ports include 25, 465, 587, 2525, and 5000 to 32768.
Authentication	Enable this if the SMTP server requires authentication.
User Name, Password, and Confirm Password	If your mail server requires authentication, enter your user name and password here. This performs a simple authentication, not SSL/TLS.
Advanced	
Use SSL/TLS	<p>Select when encryption is used.</p> <ul style="list-style-type: none"> • Never: The SMTP server does not require nor support encryption. • If Supported: The SMTP server advertises support for STARTTLS but doesn't require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given. • Always: The SMTP server requires the STARTTLS command to be sent on connection to it. • Implicitly: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server.
Require CA Root Certificate	This should only be enabled if the security policy of your organization does not allow for implicit trust of SSL/TLS connections. If this is enabled, a valid root CA certificate must be loaded onto the Rack ATS for encrypted e-mails to be sent.
File Name	This field is dependent on the root CA certificates installed on the Rack ATS and whether or not a root CA certificate is required.

SSL Certificates

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

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

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

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

Test

Path: Configuration > Notification > E-mail > Test

Send a test message to a configured recipient.

SNMP Traps

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

Configure Trap Receivers

Path: Configuration > Notification > SNMP Traps > Trap Receivers

The trap receivers are displayed by **NMS IP/Host Name**, (NMS stands for Network Management System). You can configure up to six trap receivers. To configure a new trap receiver, click **Add Trap Receiver**. To edit (or delete) a trap receiver, select its IP address/host name.

Trap Generation: Enable (the default) or disable trap generation for this trap receiver.

NMS IP/Host Name: The IPv4/ IPv6 address or host name of this trap receiver. The default, 0.0.0.0, leaves the trap receiver undefined.

Language: Select a language from the drop-down list. This can differ from the Web UI and from other trap receivers.

Select either **SNMPv1** or **SNMPv3** to specify the trap type. For an NMS to receive both types of traps, you must separately configure two trap receivers for that NMS, one for each trap type.

SNMPv1: Settings for SNMPv1.

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

SNMPv3: Settings for SNMPv3.

- **User Name:** Select the identifier of the user profile for this trap receiver.

If you delete a trap receiver, all notification settings configured under “Configuring event actions” for the deleted trap receiver are set to their default values.

Test SNMP Traps

Path: Configuration > Notification > SNMP Traps > Test

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

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

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

General Configuration

This menu contains miscellaneous configuration items including device identification, date and time, exporting and importing your Rack ATS configuration options, quick links, and data consolidation for troubleshooting.

Configure identification

Path: Configuration > General > Identification

Host Name Synchronization: Allows the host name to be synchronized with the system name so both fields automatically contain the same value.

NOTE: When enabling this feature, the system name identifier can no longer contain a space character (since it will be synchronized to the host name field).

Name, Contact, and Location: Define the **Name**, the **Contact** (the person responsible for the device), and the **Location** (the physical location), used by the SNMP agent of the Rack ATS and Data Center Expert.

These fields are used by the **sysName**, **sysContact**, and **sysLocation** object identifiers (OIDs) in the SNMP agent of the Rack ATS. For more information about MIB-II OIDs, see the PowerNet® *SNMP Management Information Base (MIB) Reference Guide*, available at www.apc.com.

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

System Message: When defined, a custom message will appear on the log on screen for all users.

Configure Date, Time, and Daylight Savings

Path: Configuration > 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:

Time Zone: This is your local time difference with Coordinated Universal Time (UTC), also known as Greenwich Mean Time (GMT).

Manual Mode: Do one of the following:

- Enter the date and time for the Rack ATS.
- Select the **Apply Local Computer Time** check box to apply the date and time settings of the computer you are using.

Synchronize with NTP Server: Have an NTP (Network Time Protocol) Server define the date and time for the Rack ATS. By default, any Rack ATS on the private side of Data Center Expert Server obtains its time settings by using Data Center Expert as an NTP server.

- **Override Manual NTP Settings:** If you select this, data from other sources (typically DHCP) take precedence over the NTP configurations you set here.
- **Primary NTP Server:** Enter the IP address or domain name of the primary NTP server.
- **Secondary NTP Server:** Enter the IP address or domain name of the secondary NTP server, when a secondary server is available.
- **Update Interval:** Define, in hours, how often the Rack ATS accesses the NTP Server for an update. Minimum: 1; Maximum: 8760 (1 year).
- **Update Using NTP Now:** Initiate an immediate update of the date and time by the NTP Server.

Daylight Saving

Path: Configuration > General > Date /Time > Daylight Saving

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

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

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

Create and Import Settings with the Config File

Path: Configuration > General > User Config File

Use the settings from one Rack ATS to configure another. Retrieve the configuration file (*config.ini*) from the configured Rack ATS, customize that file (e.g., 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	<p>Reports the progress of the upload.</p> <ul style="list-style-type: none"> • No configuration file uploaded: The Rack ATS has not been configured with a <i>config.ini</i> file. • Configuration file successfully uploaded: The Rack ATS has been configured with a <i>config.ini</i> file. You may need to refresh the page to see this message. <p>NOTE: The upload succeeds even if the file contains errors, but a system event reports the errors in the Event Log.</p>
Upload	Browse to the customized file and upload it so that the current Rack ATS can use it to set its own configuration.
Download	Allows the download of the <i>config.ini</i> file directly through the Web browser to your computer.

Instead of uploading the file to one Rack ATS, you can export the file to multiple Rack ATS units by using an FTP or SCP script.

NOTE: To retrieve and customize the file of a configured Rack ATS, see [How to Export Configuration Settings](#), page 181.

Configure Quick Links

Path: Configuration > General > Quick Links

View and change the URL links displayed at the lower-left of each page of the interface.

By default, these links access the following Web pages:

- Link 1: The home page of APC website
- Link 2: Information on EcoStruxure™ IT
- Link 3: Additional information on IT Power Distribution equipment

Configure Logs

Identify Syslog Servers

Path: Configuration > Logs > Syslog > Servers

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

Syslog Server: Uses IPv4/ IPv6 addresses or host names to identify from one to four servers to receive Syslog messages sent by the Rack ATS.

Port: The port that the Rack ATS will use to send Syslog messages. The default UDP port assigned to Syslog is 514.

Language: Select the language for any Syslog messages. (Only English is available at this time.)

Protocol: Select either UDP or TCP.

Click **Apply** to save or **Cancel** to leave without saving.

Configure Syslog Settings

Path: Configuration > Logs > Syslog > Settings

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

Facility Code: Selects the facility code assigned to the Syslog messages of the Rack ATS (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.

Severity Mapping: This section maps each severity level of the Rack ATS or environment events to available Syslog priorities. The local options are **Critical**, **Warning**, and **Informational**. You should not need to change the mappings.

- **Emergency:** The system is unusable
- **Alert:** Action must be taken immediately
- **Critical:** Critical conditions
- **Error:** Error conditions
- **Warning:** Warning conditions
- **Notice:** Normal but significant conditions
- **Info:** Informational messages
- **Debug:** Debug-level messages

The following are the default settings for **Local Priority**:

- **Critical** is mapped to **Critical**
- **Warning** is mapped to **Warning**
- **Informational** is mapped to **Info**

Test Syslog Servers

Path: Configuration > Logs > Syslog > Test

Send a test message to the Syslog servers (configured through the “Syslog servers” page). The result will be sent to all configured Syslog servers.

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

- The priority (PRI): the Syslog priority assigned to the message event, and the facility code of messages sent by the 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.

Example: APC: Test Syslog is valid.

Tests Tab

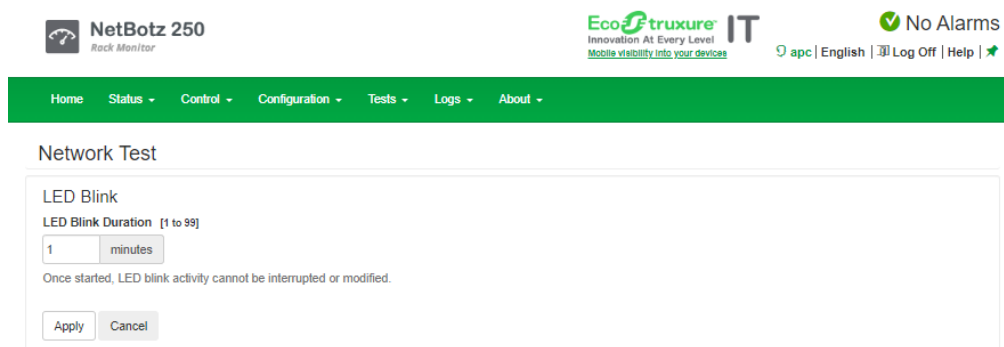
Set the LCD Light to Blink

Path: Tests > ATS > LCD Blink

If you are having trouble finding your Rack ATS, enter a number of minutes in the **LCD Blink Duration** field, and click **Apply**. The LCD display will blink for the specified number of minutes.

Set the LED Light to Blink

Path: Tests > Network > LED Blink



The screenshot shows the NetBotz 250 Rack Monitor web interface. The top navigation bar is green and contains the following items: Home, Status, Control, Configuration, Tests, Logs, and About. The main content area is titled "Network Test" and contains a form for "LED Blink". The form has a label "LED Blink Duration [1 to 99]" and a text input field containing the number "1" followed by the word "minutes". Below the input field is a note: "Once started, LED blink activity cannot be interrupted or modified." At the bottom of the form are two buttons: "Apply" and "Cancel".

If you are having trouble finding your Rack ATS, enter a number of minutes in the **LED Blink Duration** field, and click **Apply**. The 10/100/1000 Status LED light on the display will blink for the specified number of minutes.

Logs Tab

View and Configure the Event Log

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

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

You can enable color coding for events on the **Local User Management** screen (under **Configuration > Security > Local Users > Management**).

Viewing the Event Log

Path: **Logs > Events > Log**

Event Log Filtering

Event Time

Last

2 days


From

10/08/2022 11:05 to 10/10/2022 11:05

Apply Clear Log Filter Log Launch Log in New Window

Event Log

Date	Time	User	Event
10/10/2022	11:05:02	apc	Configuration change. Event log web display time selection.
10/10/2022	11:04:53	apc	Configuration change. Event log web display time selection.
10/10/2022	11:04:47	apc	Configuration change. Event log web display time selection.
10/10/2022	11:04:43	apc	Configuration change. Event log web display time selection.
10/10/2022	11:04:35	apc	Configuration change. Event log web display time selection.
10/10/2022	10:55:21	apc	Web user 'apc' logged in from 10.252.80.231.
10/10/2022	10:23:01	System	Web user 'apc' logged out from 10.252.80.231.
10/10/2022	09:23:00	apc	Web user 'apc' logged in from 10.252.80.231.

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

To see the events listed together on a Web page, click **Launch Log in New Window**.

You can also use FTP or Secure CoPy (SCP) to view the Event Log. See [Use FTP or SCP to Retrieve Log Files](#), page 177.

Event Log Filtering: Use filtering to omit information you don't want to display.

- To filter the log by date or time: Use **Last** or **From** to define the time in which the events were logged. (The filter configuration is saved until the Rack ATS restarts.)

- To filter the log by event severity or category:
 1. Click **Filter Log**.
 2. Clear a check box to remove it from view.
 3. Click **Apply**. Text at the upper right corner of the **Event Log** page indicates that a filter is active. The filter is active until you clear it or until the Rack ATS restarts.
 4. A Super User or Administrator can click **Save As Default** to save this filter as the new default log view for all users.
- To remove an active filter:
 1. Click **Filter Log**.
 2. Click **Clear Filter (Show All)**.

Important points on filtering:

- Events are processed through the filter using OR logic. If you apply a filter, it works regardless of the other filters.
- Events that you cleared in the **Filter By Severity** list do not display in the filtered **Event Log**, even if selected in the **Filter by Category** list.
- Similarly, events that you clear in the **Filter by Category** list do not display in the filtered **Event Log**.

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

To disable the logging of events based on their assigned severity level or their event category, see [Configure Notifications](#), page 161.

Reverse Lookup

Path: Logs > Events > Reverse Lookup

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

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

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

Change the Log Size

Path: Logs > Events > Size

Event Log Size: Specify the maximum number of log entries (25–30000).

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

Network Port Sharing Event Logs and Traps

Rack ATS events from guest units are sent to the host unit for inclusion into its log. The log entry will include the Display ID of the unit that the event occurred on. These events are then handled the same as local events from the host unit. Therefore alarms, SNMP traps, emails, Syslog, etc., will support Rack ATS events and alarms from all Rack ATS units in a group.

Example event log: Rack ATS 4: Device low load.

NOTE: System events will only be logged for the host Rack ATS. System events from guest Rack ATS units will not be logged on the host Rack ATS.

View and Configure the Data Log

Use the Data Log to display measurements about the Rack ATS, the power input to the Rack ATS, and the ambient temperature of the Rack ATS.

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

NOTE: The Data Log does not display information from NPS guest units.

Log

Path: Logs > Data > Log

View the log by date or time: Use **Last** or **From** to define the time in which the data was logged, and click **Apply** to save your changes. (The filter configuration is saved until the unit restarts.)

Clear Data Log: Delete all Data Log records. Deleted Data Log records cannot be retrieved.

Launch Log in New Window: View the log on a separate Web page.

Click **Apply** to save your changes, or **Cancel** to discard them.

Graphing

Path: Logs > Data > Graphing

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

NOTE: JavaScript® must be enabled in your browser to use the graphing feature. Alternatively, you can use FTP or SCP to download the Data Log and copy the information into a spreadsheet application.

Graph Data: Scroll through the list and select the data you would like to graph. Click **Apply** to save your changes.

Filter the graph by date and time: Use **Last** or **From** to define the date and time in which the events were logged. Click **Apply** to save your changes. (The filter configuration is saved until the Rack ATS restarts.)

Launch Graph in New Window: Open the graph on a separate Web page for a larger, more detailed view.

Click **Apply** to save your changes or **Cancel** to discard them.

Set Logging Intervals

Path: Logs > Data > Interval

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

NOTE: Because the interval specifies how often the data is recorded, small intervals will cause data to be recorded more quickly and thus to hold entries for shorter periods of time.

Configure Rotation Settings

Path: Logs > Data > Rotation

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

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

Click **Apply** to save these settings, **Cancel** to discard your changes, or **Upload Now!** to rotate log data.

Specify Data Log Size

Path: Logs > Data > Size

Data Log Size: specify the maximum number of log entries (25-1,000).

NOTE: When you change the maximum log size, all existing entries are deleted. When the log subsequently reaches the maximum size, the older entries are deleted.

Firewall Log

Path: Logs > Firewall

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

A firewall log contains up to 50 of the most recent events. The firewall log is cleared when the management interface reboots.

For more information on firewall policies, see [Firewall Menus](#), page 147.

Use FTP or SCP to Retrieve Log Files

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

- The file reports all recent stored events. If the log has been deleted or truncated because it reached maximum size, the deleted or truncated information will not be included in the file.
- 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)

NOTE: 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.

NOTE: By default, FTP is disabled and SCP (via SSH) is enabled.

See the *Security Handbook* on www.apc.com for information on available security protocols and methods to set up the type of security you need.

Use SCP to retrieve the files

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

```
scp -c <cipher> username@hostname_or_ip_address:event.txt  
./event.txt
```

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

```
scp -c <cipher> username@hostname_or_ip_address:data.txt ./data.  
txt
```

NOTE:

- This SCP command is for OpenSSH. The command may differ depending on the SSH tool used.
- When using OpenSSH, *<cipher>* can be either *aes256-cbc* or *3des-cbc*.

Use FTP to retrieve the event.txt or data.txt files

1. At a command prompt, type `ftp` and the IP address of the Rack ATS, 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
```

You can set a non-default port value to enhance security for the FTP Server under **Configuration > Network > Port > FTP Server**. 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. Type `quit` at the `ftp>` prompt to exit from FTP.

Download Log Files to a USB Flash Drive

1. Insert a USB Flash drive to the USB port on the Display Interface of the Rack ATS. Before starting the transfer, make sure the USB drive is formatted in FAT32.
2. Scroll to **Log to Flash** on the Display Screen and press the **Select** button.
3. Press the **Select** button again to export the Log files to your Flash drive.

You may abort the download by pressing the **Select** button at any time during the download process.

NOTE: If a `debug.txt` file or a `dump.txt` file does not exist on the Rack ATS, it cannot be downloaded to the USB Flash drive. These files are only created following an unexpected system crash or a Network Management Card (NMC) reset. The `debug.txt` and `dump.txt` files are used for technical support only.

About Tab

About the Rack ATS

Path: About > ATS

The screenshot shows the Schneider Electric Automatic Transfer Switch Application web interface. The page title is 'Automatic Transfer Switch Application'. The top navigation bar includes 'Home', 'Status', 'Control', 'Configuration', 'Tests', 'Logs', and 'About'. The right side of the page shows 'EcoStruxure IT' logo, 'Innovation At Every Level', 'Mobile visibility into your devices', and 'No Alarms' status. The main content area is titled 'About' and contains two sections: 'Automatic Transfer Switch' and 'ATS Controller Firmware'.

Automatic Transfer Switch		
Name	Location	Contact
apcD8F074	Unknown	Unknown
Model Number	Rating	Serial Number
AP4452	1ø, 16 A	5A1713T59925
Hardware Revision	Manufacture Date	Phases
R01	07/17/2019	1
Circuit Breakers	Outlets	NMC Serial Number
0	10	AABBAA
NMC Uptime	Network Link	
0 Days 0 Hours 29 Minutes	Link Active	

ATS Controller Firmware		
Firmware Version	Firmware Date	Downloader Version
4.3.4	09/24/19	4.0

APC's Web Site | Testdrive Demo | EcoStruxure™ IT

© 2020, Schneider Electric. All rights reserved. Site Map | Updated: 09/17/2020 at 10:07 (apc08f074.us.ddns.schneider-electric.com)

The hardware information is useful to APC Customer Support for troubleshooting problems with the Rack ATS. The serial number and MAC address are also available on the Rack ATS itself.

Management Uptime is the length of time the network management interface has been running continuously.

About the Network

Path: About > Network

Information for the Application Module, APC OS (AOS), and APC Boot Monitor 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 website, www.apc.com.

Support Resources

Path: About > Support

This page provides links to multiple support resources:

- **Knowledge Base:** Direct link to FAQs on the APC website.
- **Company Contact Information:** Provides phone numbers for multiple support services provided by APC.
- **Software & Firmware Downloads:** Download software upgrades for your product.

Technical Support Debug Information Download: With this option, you can consolidate various data in this interface into a single zipped file for troubleshooting purposes and customer support. The data includes the Event and Data logs, the configuration file and complex debugging information. Click **Generate Logs** to create the file, and **Download** to download them. You will be asked whether you want to view or save the zipped file.

How to Export Configuration Settings

Summary of the Procedure

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

1. Configure a Rack ATS with the desired settings, and retrieve the .ini file from that Rack ATS.
2. If desired, you can edit the .ini file with any text editor before uploading it to another device. Data entries may not be moved between sections. Lines will not be processed if they start with a semicolon (;).
3. Use a file transfer protocol supported by the Rack ATS to transfer a copy to one or more other devices. For a transfer to multiple Rack ATS units, use an FTP or SCP script or the .ini file utility. Each receiving unit uses the file to re-configure its own settings and then deletes it.

NOTE: FTP is disabled by default. If needed, you can enable FTP under **Configuration > Network > FTP Server**.

NOTE: Managing Users via the config.ini - Users are no longer managed via the config.ini in any form. Users are now managed via a separate file with the .csf extension. For further information on this topic, refer to FAQ article FA156117: How can I mass configure a Network Management Card (NMC) or NMC embedded product? To find an FAQ article, go to www.apc.com/support, select **FAQS** under Resources and Tools, then enter the article number or title in the Search bar.

Contents of the .ini File

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

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

.ini and Network Port Sharing

The .ini configuration utility is able to get and set values for all devices in a group. In order to be backwards compatible, the host Rack ATS will always be designated as first, "ATS_A". Any guest Rack ATS units are then designated "ATS_B", "ATS_C", and "ATS_D" based on their Display ID in ascending order up to ATS_Z. After that, further PDUs are designated ATS_AA, up to ATS_FF. Therefore, "ATS_A" will not necessarily correlate to Display ID 1, and so on.

NOTE: Because of the large number of configuration values possible in a Rack ATS group, it may take a very long time to process an INI file set. For example, a Rack ATS group of 4 units with all values changing may take 30 minutes to complete processing.

Detailed Procedures

Retrieve .ini File

If possible, use the interface of a Rack ATS to configure it with the settings to export. (Directly editing the .ini file risks introducing errors).

Then retrieve *config.ini* from the configured Rack ATS via FTP, SCP, or the Web UI:

To use FTP

1. Open a connection to the Rack ATS using its IP address:

```
ftp> open ip_address
```

2. Log on using the Super User/Administrator user name and password.
3. Retrieve the *config.ini* file containing the settings of the Rack ATS:

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

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

To export configuration settings to multiple Rack ATS units, see FAQ article FA156117: *How can I mass configure a Network Management Card (NMC) or NMC embedded product?* To find an FAQ article, go to www.apc.com/support, select **FAQS** under Resources and Tools, then enter the article number or title in the Search bar.

To use SCP

Use the following command:

```
scp -c <cipher> username@hostname_or_ip_address:config.ini  
./config.ini
```

Then enter the correct password.

NOTE:

- This SCP command is for OpenSSH. The command may differ depending on the SSH tool used.
- When using OpenSSH, <cipher> can be either aes256-cbc or 3des-cbc. Aes256 is more secure.

To use the Web UI:

Navigate to **Configuration > General > User Config File** and select **Download**.

Edit .ini File

Edit the file carefully before you transfer it to other Rack ATS units.

1. Use a text editor to make your changes.
 - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
 - Use adjacent quotation marks to indicate no value. For example, `LinkURL1=""` indicates that the URL is intentionally undefined.
 - Enclose in quotation marks any values that contain leading or trailing spaces or are already enclosed in quotation marks.
 - To export scheduled events, configure the values directly in the .ini file.
 - To export a system time with the greatest accuracy, if the receiving Rack ATS units can access a Network Time Protocol server, configure `enabled` for `NTPEnable`:

```
NTPEnable=enabled
```

Alternatively, reduce transmission time by exporting the `[SystemDate/Time]` section as a separate .ini file.
 - To add comments, start each comment line with a semicolon (;).
2. Copy the customized file to another file name in the same folder:
 - The file name can have up to 64 characters and must have the .ini suffix.
 - Retain the original customized file for future use. **The file that you retain is the only record of your comments.**

Transfer the File To a Single Rack ATS

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

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

```
ftp> open ip_address
```
 2. Export the copy of the customized .ini file to the root directory of the receiving Rack ATS:

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

Transfer the File To Multiple Rack ATS Units

To transfer the .ini file to multiple Rack ATS units, do one of the following:

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

To create the batch file and use the utility, see FAQ article FA156117: *How can I mass configure a Network Management Card (NMC) or NMC embedded product?* To find an FAQ article, go to www.apc.com/support, select **FAQS** under Resources and Tools, then enter the article number or title in the Search bar.

The Upload Event and Error Messages

The Event and Its Error Messages

The following event occurs when the receiving Rack ATS completes using the .ini file to update its settings.

Configuration file upload complete, with number valid values

If a keyword, section name, or value is invalid, the upload by the receiving 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, an incomplete upload occurs. Reduce the size of the file, or divide it into two files, and try uploading again.

Messages in Config.ini

A Rack ATS from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the Rack ATS is not present or is not discovered, the config.ini file contains a message under the appropriate section name, instead of keywords and values. For example: Rack ATS not discovered

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

Errors Generated By Overridden Values

The `Override` keyword and its value will generate error messages in the Event Log when it blocks the exporting of values. See [Contents of the .ini File, page 181](#) for information about which values are overridden.

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

Related Topics

On Windows operating systems, instead of transferring .ini files, you can use the Device IP Configuration Wizard to update the basic TCP/IP settings of the Rack ATS and configure other settings through its user interface. See [Device IP Configuration Utility, page 20](#) for instructions to download and install the Device IP Configuration Wizard.

Troubleshooting

Rack ATS Access Problems

For problems that persist or are not described here, contact the APC Customer Care at www.apc.com.

Problem	Solution
After a Network Port Sharing host is updated to new firmware, the guest Rack ATS units show a "firmware version does not match" alarm.	This will be automatically resolved by the host unit, given time. Events are logged in this order : "Remote RATS 2 (SN: xxxxxxxxxxxx) firmware version does not match." > "Guest RATS firmware download started." > "Guest RATS firmware download completed." > "Remote RATS 2 (SN: xxxxxxxxxxxx) firmware version alarm has been cleared." > "Remote RATS 2 (SN: xxxxxxxxxxxx) communication established."
Unable to ping the Rack ATS	If the Rack ATS unit's Status LED is green, try to ping another node on the same network segment as the Rack ATS. If that fails, it is not a problem with the Rack ATS. If the Status LED is not green, or if the ping test succeeds, perform the following checks: <ul style="list-style-type: none"> • Verify all network connections. • Verify the IP addresses of the Rack ATS and the NMS. • If the NMS is on a different physical network (or subnet) from the Rack ATS, verify the IP address of the default gateway (or router). • Verify the number of subnet bits for the Rack ATS's subnet mask.
Cannot allocate the communications port through a terminal program	Before you can use a terminal program to configure the Rack ATS, you must shut down any application, service, or program using the communications port.
Cannot access the CLI through a serial connection	Make sure that you did not change the baud rate. Try 2400, 9600, 19200, or 38400.
Cannot access the CLI remotely	<ul style="list-style-type: none"> • Make sure you are using the correct access method, Telnet or Secure SHell (SSH). The Super User or an Administrator can enable these access methods. By default, Telnet is disabled, and SSH is enabled. SSH and Telnet can be enabled/disabled independently. • For SSH, the Rack ATS may be creating a host key. The Rack ATS can take up to one minute to create the host key, and SSH is inaccessible for that time.
Cannot access the Web UI	<ul style="list-style-type: none"> • Verify that HTTP or HTTPS access is enabled. • Make sure you are specifying the correct URL — one that is consistent with the security system used by the Rack ATS. This requires https, not http, at the beginning of the URL. • Verify that you can ping the Rack ATS. • Verify that you are using a Web browser supported for the Rack ATS. See <i>Web User Interface</i>, page 118. • If the Rack ATS has just restarted and SSL/TLS security is being set up, the Rack ATS may be generating a server certificate. The Rack ATS can take up to one minute to create this certificate, and the SSL/TLS server is not available during that time.
Cannot communicate using Network Port Sharing (NPS)	<ul style="list-style-type: none"> • If you are having communications problems with Network Port Sharing, check that the total length of network cable between up to 32 units is not more than 10 meters. • If you are using Network Port Sharing and do not see one or more of the units in the group, check that all units in the group are using the same firmware revision. Guest Rack ATS units should receive firmware updates from their hosts, but manually updating units that seem to be completely unresponsive to the host's firmware revision may resolve the issue. You can download appropriate firmware revisions from the APC website, www.apc.com.

SNMP Problems

Problem	Solution
Unable to perform a GET	<ul style="list-style-type: none"> • Verify the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3). • Use the CLI or Web UI to confirm that the NMS has access. See <i>SNMP Options</i>, page 157.
Unable to perform a SET	<ul style="list-style-type: none"> • Verify that SNMP is enabled. SNMPv1 and SNMPv3 are disabled by default. • Verify the read/write (SET) community name (SNMPv1) or the user profile configuration (SNMPv3). • Use the CLI or Web UI to confirm that the NMS has write (SET) access (SNMPv1) or is granted access to the target IP address through the access control list (SNMPv3). See <i>SNMP Options</i>, page 157.
Unable to receive traps at the NMS	<ul style="list-style-type: none"> • Make sure the trap type (SNMPv1 or SNMPv3) is correctly configured for the NMS as a trap receiver. • For SNMP v1, query the mconfigTrapReceiverTable MIB OID to verify that the NMS IP address is listed correctly and that the community name defined for the NMS matches the community name in the table. If either is not correct, use SETs to the mconfigTrapReceiverTable OIDs, or use the CLI or Web UI to correct the trap receiver definition. • For SNMPv3, check the user profile configuration for the NMS, and run a trap test. See <i>SNMP Options</i>, page 157, <i>Configure Notifications</i>, page 161, and <i>SNMP Traps</i>, page 165 for more information on profiles and trap tests.
Traps received at an NMS are not identified	See your NMS documentation to verify that the traps are properly integrated in the alarm/ trap database.

Worldwide Customer Support

Support for this product is available at www.apc.com.

Source Code Copyright Notice

cryptlib copyright Digital Data Security New Zealand Ltd 1998.

Copyright © 1990, 1993, 1994 The Regents of the University of California. All rights reserved.

This code is derived from software contributed to Berkeley by Mike Olson.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

APC
70 Mechanic Street
02035 Foxboro, MA
USA

www.apc.com

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

© 2022 APC. All rights reserved.

990-91718A-001