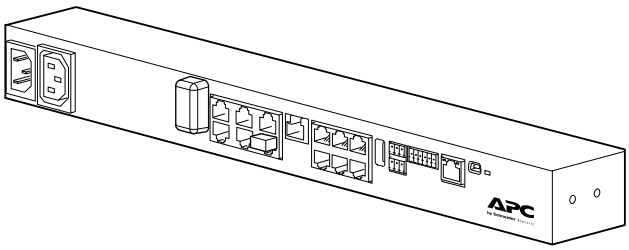
# NetBotz

## Rack Monitor 250 with NMC3

## User Guide

Release Date: June 2026

TME14430



www.apc.com

# Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

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

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document 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 document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

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

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time 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 document, as well as any non-intended use or misuse of the content thereof.**

# Table of Contents

Table of Contents ..... 3
Important Safety Instructions — SAVE THESE INSTRUCTIONS ..... 9
Safety Information for the Rack Monitor 250 ..... 10
Overview ..... 11
Additional Documentation ..... 11
User Comments ..... 11
About the Network Management Card ..... 12
NMC 3 Multifactor Authentication ..... 12
Standards and Protocols ..... 12
Physical Description ..... 13
Network Status LED ..... 14
10/100 Status LED ..... 14
Physical Security ..... 15
Types of User Accounts ..... 16
Watchdog Features ..... 16
Network Interface Watchdog Mechanism ..... 16
Resetting the Network Timer ..... 16
Getting Started ..... 17
Establish Network Settings ..... 17
About IPv4 Setup ..... 17
About IPv6 Setup ..... 17
TCP/IP Configuration Methods ..... 18
Network Management with Other Applications ..... 22
Connect Wired Sensors and Devices ..... 24
Cascade Sensors and Pods from A-Link Ports ..... 25
The Wireless Sensor Network ..... 27
ZigBee for the Wireless Sensor Network ..... 27
Devices on the Wireless Sensor Network ..... 28
Enhancing the Wireless Signal ..... 28
Connect the Wireless Sensor Network ..... 29
Troubleshooting the Wireless Sensor Network ..... 29
Recover from a Lost Password ..... 30
Web User Interface ..... 31
Log on to the Web UI ..... 31
URL address formats ..... 32
First Log On ..... 32
Web UI Features ..... 33
Menus ..... 33
Limited Status Access ..... 33
Device Status Icons ..... 34
Quick Links ..... 34
Home Page ..... 35
Configuring Modules, Sensors, Output Devices, and Alarms ..... 36
Filtering Module and Sensor Lists ..... 36
View and Configure Module Settings ..... 37
Manage Wired Sensors ..... 37

View Wired Sensors ..... 37
Mass-configure Sensor Settings ..... 38
Configure Wired Sensors ..... 38
Manage Rack Access ..... 40
Register a New User/Proximity Card ..... 41
Update A Registered User Account ..... 41
Configure Rack Access User Authentication ..... 42
Lock/Unlock Rack Access Handles ..... 43
Schedule an Automatic Unlocking Event ..... 43
Manage the Wireless Sensor Network ..... 44
Add Sensors to the Commission List ..... 44
Remove Sensors from the Commission List ..... 44
Disable or Enable the Wireless Sensor Network ..... 44
View Wireless Sensors ..... 45
Configure Wireless Sensors ..... 46
Update the Wireless Sensor Network ..... 47
Manage Output Devices ..... 48
Manage Active Alarms ..... 49
Configure Notifications ..... 49
Configure Notifications By Event ..... 50
Configure Notifications By Group ..... 51
Set Up E-mail Notifications ..... 52
SNMP Traps ..... 54
Configure Settings for Your Appliance and Web UI ..... 56
General Configuration ..... 56
Configure identification ..... 56
Configure Date, Time, and Daylight Savings ..... 57
Create and Import Settings with the Config File ..... 58
Configure Quick Links ..... 58
Manage Security Settings ..... 59
Manage Settings for User Sessions ..... 59
Manage User Sessions ..... 59
Enable Ping Response ..... 60
Manage Local User Settings ..... 60
Configure Default User Settings ..... 62
Manage Remote User Settings ..... 63
ldap ..... 64
Configure a RADIUS Server ..... 68
TACACS+ screen (v3.0.x and higher) ..... 69
Configure a TACACS+ Server ..... 70
Firewall Menus ..... 70
802.1X Security Configuration ..... 73
View Network Status ..... 74
Reset the Network Interface ..... 74
Configure Network Settings ..... 75
Protocol Configuration Summary ..... 75
Configure TCP/IP and Communication Settings for IPv4 and IPv6 ..... 76
Configure Network Port Speed ..... 77
Configure DNS ..... 78
Test DNS Configuration ..... 78

Configure Web Access ..... 79
Configure SSL Certificate for Web Access ..... 80
Configure CLI Access ..... 80
Configure SSH Host Key ..... 81
SNMP Options ..... 82
Configure FTP Server ..... 84
Set the LED Light to Blink ..... 85
Factory Information ..... 85
Support Resources ..... 85
Using the Logs ..... 86
Identify Syslog Servers ..... 86
Configure Syslog Settings ..... 86
Test Syslog Servers ..... 87
View and Configure the Event Log ..... 87
Viewing the Event Log ..... 87
Reverse Lookup ..... 88
Change the Log Size ..... 89
View and Configure the Data Log ..... 89
Log ..... 89
Graphing ..... 90
Set Logging Intervals ..... 90
Configure Rotation Settings ..... 91
Specify Data Log Size ..... 91
Firewall Log ..... 92
Use FTP or SCP to Retrieve Log Files ..... 92
Command Line Interface ..... 94
Log On to the CLI ..... 94
Local Access to the CLI ..... 94
Remote Access to the CLI ..... 95
About the Main Screen ..... 96
Using the CLI ..... 98
Command Syntax ..... 99
Command Response Codes ..... 100
Prompting for User Input during Command Execution ..... 100
Command Editing ..... 100
History ..... 101
Auto Completion ..... 101
Delimiter ..... 101
Options and Arguments Inputs ..... 101
Response Format and Message Codes ..... 102
Network Management Card Command Descriptions ..... 103
? ..... 103
about ..... 104
alarmcount ..... 104
boot ..... 105
bye ..... 106
cd ..... 106
clrrst ..... 106
console ..... 107
date ..... 108
delete ..... 108

dir ..... 109
dns ..... 110
eapol ..... 111
email ..... 112
eventlog ..... 114
exit ..... 115
firewall ..... 115
format ..... 115
ftp ..... 117
help ..... 117
lang ..... 117
lastrst ..... 118
ldap ..... 118
ledblink ..... 122
logzip ..... 122
netstat ..... 123
ntp ..... 123
ping ..... 124
portSpeed ..... 124
prompt ..... 125
pwd ..... 125
quit ..... 125
radius ..... 126
reboot ..... 127
resetToDef ..... 127
session ..... 128
smtp ..... 129
snmp ..... 130
snmpv3 ..... 131
snmptrap ..... 131
ssh ..... 132
ssl ..... 132
system ..... 134
tacacs+ ..... 136
tcpip ..... 136
tcpip6 ..... 137
user ..... 138
userauth ..... 139
userdflt ..... 139
web ..... 140
whoami ..... 141
xferINI ..... 142
xferStatus ..... 142
Device Command Descriptions ..... 143
modbus ..... 143
nbabout ..... 144
**nbbeacon** ..... 144
nboutlet ..... 145
nbrack ..... 146
nbrelay ..... 147
nbsensor ..... 147

spabout ..... 150
spsensor ..... 150
zw ..... 152
zwsyslog ..... 154
How to Export Configuration Settings ..... 155
Summary of the Procedure ..... 155
Contents of the .ini File ..... 155
Detailed Procedures ..... 156
Retrieve .ini File ..... 156
Edit .ini File ..... 157
Transfer the File To a Single Rack Monitor 250 ..... 157
Transfer the File To Multiple Rack Monitor 250s ..... 157
The Upload Event and Error Messages ..... 158
The Event and Its Error Messages ..... 158
Messages in Config.ini ..... 158
Errors Generated By Overridden Values ..... 158
Related Topics ..... 158
Updating Firmware ..... 159
Firmware File Transfer Methods ..... 159
Use the Firmware Update Utility ..... 160
Use FTP or SCP to Update One Rack Monitor 250 ..... 161
Use a USB Drive To Transfer and Update Files ..... 162
How To Update Multiple Rack Monitor 250s ..... 162
Verifying Upgrades and Updates ..... 163
Verify the Success Or Failure of the Transfer ..... 163
Last Transfer Result Codes ..... 163
Verify the Version of Installed Firmware ..... 163
Downgrading Installed Firmware ..... 164
Troubleshooting ..... 165
Access Problems ..... 165
SNMP Problems ..... 166
Specifications ..... 167
Two-year Factory Warranty ..... 169
Terms of Warranty ..... 169
Non-transferable Warranty ..... 169
Exclusions ..... 169
Warranty Claims ..... 170
Worldwide Customer Support ..... 171
Source Code Copyright Notice ..... 172

# 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 APC 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.

# Safety Information for the Rack Monitor 250

**⚠⚠WARNING**

**ELECTRIC SHOCK HAZARD**

- No user-serviceable parts inside. Refer servicing to qualified personnel.
- Use indoors only in a dry location.
- Ensure the power input for the Rack Monitor 250 has a reliable ground (earth) connection.
- The Rack Monitor 250 is intended to be installed and operated by a skilled person in a controlled location with restricted access.
- The switched outlet may have voltage potential when the outlet is set to "off." Always use a properly rated voltage sensing device to confirm there is no voltage in the outlet.
- Disconnect the load power cord from this product before servicing the load equipment or the power cord.

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

**⚠CAUTION**

**FALLING EQUIPMENT HAZARD**

- Do not create a hazardous condition due to uneven mechanical loading. For example, do not use the appliance as a shelf.
- Ensure the Rack Monitor 250 is mounted securely and evenly.

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

***NOTICE***

**EQUIPMENT DAMAGE HAZARD**

The ambient operating temperature of a closed or multi-unit rack environment may be greater than the ambient temperature of the room. Ensure the ambient operating temperature of your rack environment does not exceed the rated ambient operating temperature for the Rack Monitor 250.

**Failure to follow these instructions can result in equipment damage.**

# Overview

The NetBotz® Rack Monitor 250 is a rack-mountable central hardware appliance for an environmental monitoring and control system. Once installed, you can monitor and control your system using any of the following interfaces:

- Web User Interface (Web UI)
- Command Line Interface (CLI)
- Modbus (you must enable modbus through the Web UI or CLI)
- Data Center Expert

Only connect compatible sensors and devices to your NetBotz appliance. See Connect Wired Sensors and Devices, page 24 for a detailed list of devices that can be connected directly to the appliance. See Devices on the Wireless Sensor Network, page 28 for a list of compatible wireless devices.

**NOTE:** The Rack Monitor 250 is not a PoE compatible device. Do not connect a Rack Monitor 250 to a PoE (Power over Ethernet) switch.

**NOTE:** The Rack Monitor 250 uses unique software that is not compatible with other NetBotz appliances, such as the Rack Monitor 750.

# Additional Documentation

You can find the latest version of this manual and additional documentation on wwww.se.com.

- *Installation Sheet:* Describes the procedure for physical installation and initial setup of your Rack Monitor 250.
- *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 online,

1. Go to the Schneider Electric download center at www.se.com/ww/en/download.
2. Click **Select location** and select your location from the list.

   **NOTE:** You cannot download documentation until you have selected a location.
3. In the Search bar, enter the title of your document, the part number of your document, or the part number of your equipment. Press enter or click the magnifying glass icon to start the search.
4. Download the desired document from the search results. If needed, you can select the filters at the left of the web page to narrow the search results.

Alternatively, you can find all the documentation for a single product at www.go2se.com/ref=*product part number* **> Documentation > Product Documentation**.

# User Comments

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

# About the Network Management Card

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.

An NMC version 3 (NMC 3) is installed in the Rack Monitor 250 (NBRK0250A).

## NMC 3 Multifactor Authentication

NMC 3 version 3.4.0 introduced multifactor authentication (MFA) which requires a one-time password sent via email after successful username and password authentication.

Some features in EcoStruxure IT Expert and Data Center Expert do not work as expected when MFA is enabled on monitored NMC 3 devices and device user credentials used for communication with ITE and DCE have email addresses configured.

Before enabling MFA on any Rack Monitor 250A monitored by ITE or DCE, make sure that user credentials configured for discovery, file transfer, and device communication in ITE and DCE do not have email addresses configured.

To verify user credentials on the Rack Monitor 250A:

1. Log in to the device. Go to **Configuration** > **Security** > **Local Users** > **Management**.
2. Verify that the email address field is blank for the user credentials DCE and ITE use for communication.

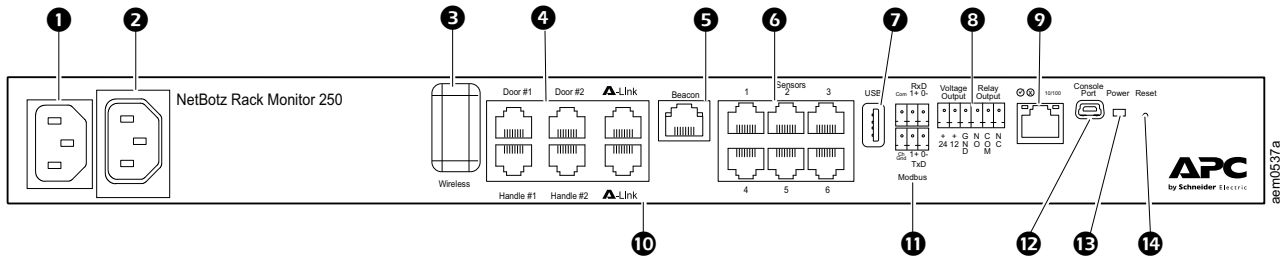
# Standards and Protocols

The Rack Monitor 250 uses the following standards and protocols:

- Hypertext Transfer Protocol (HTTP)
- HTTP over Secure Sockets Layer (HTTPS)
- File Transfer Protocol (FTP)
- Telnet
- Secure SHell (SSH)
- Simple Network Management Protocol (SNMP)
- Secure Copy (SCP)
- Modbus TCP and serial Modbus
- TCP/IP v4 and v6
- USB A-USB mini B serial connection
- SMTP-based secure email
- RADIUS (Remote Access Dial In User Service)
- LDAP (Lightweight Directory Access Protocol) — v3.1.x and higher
- TACACS+ (Terminal Access Controller Access Control System Plus) v3.0.x and higher
- Network Time Protocol (NTP)

# Physical Description

## Front




| Item | | Function |
|---|---|---|
| ❶ | AC Line Inlet | Input power connection, 100–240 VAC. |
| ❷ | Switched Outlet | Provides power to a device at a total maximum amperage of 10 A. Activates a connected device when configured events occur. (For example, a fan may be connected to this outlet, and the outlet may be configured to turn on when a high threshold violation occurs for a temperature sensor.) |
| ❸ | Wireless Network Coordinator | USB port with NetBotz USB Coordinator (NBWC100U) installed. Used with included Wireless Temperature Sensor (NBWS100T) to monitor temperature. Additional wireless sensors can be purchased separately. |
| ❹ | Rack Access ports | Ports for the door switch sensors on doors #1 and #2 Ports for the handle sensors on doors #1 and #2. |
| ❺ | Beacon port | Connection for an alarm beacon (AP9324). |
| ❻ | Universal sensor ports | Connections for APC sensors and third-party dry contact sensors. (See Connect Wired Sensors and Devices, page 24 for a list of compatible APC sensors.) Third-party dry contact sensors require a Dry Contact Cable (NBES0304), and third-party 0–5 V sensors require the NetBotz 0–5 V sensor cable (NBES0305). |
| ❼ | USB port | Used for firmware upgrades. |
| ❽ | Voltage Output | Provides 12 VDC or 24 VDC (75 mA) to a connected device. |
| | Relay Output | Connection for relay-controlled external devices. |
| ❾ | 10/100 Network Port | Connection to the network. Status and link LEDs indicate network traffic. See 10/100 Status LED, page 14 and Network Status LED, page 14 for descriptions of LED behavior. |
| ❿ | A-Link ports | Connection for Temperature/Humidity Sensors with Digital Displays (AP9520TH). Provides communications and power using standard CAT-5 cabling with straight-through wiring.<br><br>To cascade multiple devices, connect a supplemental power supply (100–240 VAC/24 VDC, part number AP9505i) to a NetBotz Rack Sensor Pod 150 or NetBotz Rack Access Pod 175. For instructions, see Cascade Sensors and Pods from A-Link Ports, page 25.<br>. |
| ⓫ | Modbus RS-485 port | Connection for a building management system using the Modbus protocol. |
| ⓬ | Console Port | Used to connect the USB A-USB mini B configuration cable when configuring initial network settings.<br>**NOTE:** If you are unable to access the appliance using the console port, you may need to install a serial-to-USB virtual COM port driver. The USB vendor is FTDI; the driver type is VCP. Driver downloads are available on the FTDI Chip website, ftdichip.com. |
| ⓭ | Power LED | Indicates whether the unit is receiving power (blue = receiving power; dark = not receiving power). |
| ⓮ | Reset button | Restarts the Rack Monitor 250 network management interface. |

## Rear

Toolless mounting pegs allow for installation in APC NetShelter® VX and SX racks and enclosures without using any U-spaces.

# Network Status LED

This LED indicates the network status.

| Condition | Description |
|---|---|
| Off | The Rack Monitor 250 is connected to an unknown network. |
| Solid green | The Rack Monitor 250 has valid TCP/IP settings. |
| Flashing green | The Rack Monitor 250 does not have valid TCP/IP settings.[1] |
| Solid orange | A hardware failure has been detected in the Rack Monitor 250. |
| Flashing orange | The Rack Monitor 250 is making BOOTP requests. |
| Flashing orange and green (alternating) | The Rack Monitor 250 is making DHCP requests. |
| [1]If you do not use a BOOTP or a DHCP server, see Local Access to the CLI, page 20 or Remote Access to the CLI, page 20 to configure the TCP/IP settings. | |

# 10/100 Status LED

This LED indicates the network status of the Rack Monitor 250.

| Condition | Description |
|---|---|
| Off | One or more of the following situations exists:<br>• The Rack Monitor 250 is not receiving input power.<br>• The cable that connects the Rack Monitor 250 to the network is disconnected or defective.<br>• The device that connects the Rack Monitor 250 to the network is turned off.<br>• The Rack Monitor 250 itself is not operating properly. It may need to be repaired or replaced. Contact Customer Support. |
| Solid Yellow | The Rack Monitor 250 is connected to a network operating at 100 Megabits per second (Mbps). |
| Solid Green | The Rack Monitor 250 is connected to a network operating at 10 Mbps. |
| Flashing Yellow | The Rack Monitor 250 is receiving or transmitting data packets at 100 Mbps. |
| Flashing Green | The Rack Monitor 250 is receiving or transmitting data packets at 10 Mbps. |

# Physical Security

Attackers with physical access to equipment can access your devices without authorization. To prevent physical attacks, and to prevent the physical connections from being used for a denial-of-service attack (DoS) on the system, secure the front panel of your device and deploy your devices in a secure location.

Recommendations to secure the front panel: Devices should be locked behind cabinets or protected by physical restraints that prevent unauthorized access or removal from restricted areas. Cabinets should be locked with a suitable key or other physical methods. Access to wires/cabling must also be secure.

Recommendations for secure locations:

- Clearly mark restricted areas for access to authorized personnel only.
- Secure restricted areas with locked doors.
- Only grant access to areas containing covered equipment to personnel who require access based on their job function.
- Ensure facilities containing covered devices give minimum indication of their purpose, with no obvious signs identifying the presence of related functions.
- Test physical access control devices (key card readers, doors and cabinet locks, etc.) prior to use and on a periodic basis (e.g., annually).
- If you are a resource custodian,
  - Produce physical or electronic audit trails to record all personnel's physical access to restricted areas for security incident investigation.
  - Regularly review who has physical access to control devices, and remove any inappropriate access identified during the review.
- If any sensor data is considered critical, use a wired sensor instead of a wireless one. Wired connections are less susceptible to interference than wireless connections.

# Types of User Accounts

- 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 has read-write access to the network-related menus only. The Administrator can enable or disable the Network-Only user account.

# Watchdog Features

To detect internal problems and recover from unanticipated inputs, the Rack Monitor 250 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 Monitor 250 implements internal watchdog mechanisms to help protect itself from becoming inaccessible over the network. For example, if the Rack Monitor 250 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 Monitor 250 that discovers an active network interface connection at start-up.

## Resetting the Network Timer

To help ensure that the Rack Monitor 250 does not restart if the network is quiet for 9.5 minutes, the Rack Monitor 250 attempts to contact the default gateway every 4.5 minutes. If the gateway is present, it responds to the Rack Monitor 250, 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 Monitor 250 from restarting.

# Getting Started

To get started using the Rack Monitor 250:

1. Install the Rack Monitor 250 using the *Installation and Quick Start* sheet provided with the unit.
2. Provide the power and network connections.
3. Establish the network settings. See Establish Network Settings, page 17
4. Connect sensors and devices to the Rack Monitor 250. See Connect Wired Sensors and Devices, page 24.
5. Connect the wireless sensor network. See The Wireless Sensor Network, page 27.
6. Begin using the Rack Monitor 250 with one of the following interfaces:
   - The Web UI. See Web User Interface, page 31.
   - The CLI. See Command Line Interface, page 94.

# Establish Network Settings

EcoStruxure Data Center Expert™ (DCE) provides DHCP configuration for SNMPv1 devices discovered on the DCE private network. If your Rack Monitor 250 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 Monitor 250. Establish a local connection to the CLI (Local Access to the CLI, page 20) and use the `snmp` command to enable SNMPv1 (snmp, page 130).

## About IPv4 Setup

You must define three TCP/IP settings for the Rack Monitor 250 before it can operate on the network:

- The IP address of the Rack Monitor 250
- The subnet mask of the Rack Monitor 250
- 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 Monitor 250 and is usually running. The Rack Monitor 250 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 Monitor 250. 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 Monitor 250, see **DHCP Response Options** under Configure TCP/IP and Communication Settings for IPv4 and IPv6, page 76.

## 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 Monitor 250:

- BOOTP or DHCP server (see DHCP and BOOTP Configuration, page 18).

  **NOTE:** DHCP is the default method of network configuration for the Rack Monitor 250. Most networks are configured with a DHCP server.

- CLI (see Local Access to the CLI, page 20 or Remote Access to the CLI, page 20).
- Device IP Configuration Wizard (see ).

  **NOTE:** SNMP is disabled by default, and must be enabled for the Device IP configuration Utility to function. You can enable SNMP from the CLI.

- You can use the .ini file to export .ini file settings from a configured Rack Monitor 250 to one or more unconfigured Rack Monitor 250s. To do this from the Web UI, go to **Configuration > General > User Config File**. See How to Export Configuration Settings, page 155 for further options and detailed instructions on how to edit the .ini file.

## 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 Monitor 250. 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 20 for instructions) and view the IP address assigned to your Rack Monitor 250 (see View or Configure TCP/IP settings in the CLI, page 21 for instructions.)

### DHCP server configuration

You can use an RFC2131/RFC2132-compliant DHCP server to configure the TCP/IP settings for the Rack Monitor 250.

1. The Rack Monitor 250 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 Monitor 250)
   - A User Class Identifier (by default, the identification of the application firmware installed on the Rack Monitor 250)
   - A Host Name (by default, apcXXYYZZ with XXYYZZ being the last six digits of the Rack Monitor 250 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 Monitor 250 needs for network communication. The DHCP offer also includes the Vendor Specific Information option (DHCP option 43). The Rack Monitor 250 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 Monitor 250 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 Monitor 250.

For additional information on supported DHCP options, see Configure TCP/IP and Communication Settings for IPv4 and IPv6, page 76.

## BOOTP server configuration

For the Rack Monitor 250 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 Monitor 250 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 Monitor 250.
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 20 for detailed instructions to access the CLI.
3. Enter `-Y` to reboot the Rack Monitor 250.

   When the Rack Monitor 250 reboots, the BOOTP server provides it with the TCP/IP settings.

   - If you specified a bootup file name, the Rack Monitor 250 attempts to transfer that file from the BOOTP server using TFTP or FTP. The Rack Monitor 250 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 Monitor 250 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 Monitor 250 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 Monitor 250 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 Monitor 250.
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 21 to complete the configuration.

## Remote Access to the CLI

From any computer on the same network as the Rack Monitor 250, you can use ARP and Ping to assign an IP address to the Rack Monitor 250, and then use SSH or Telnet to access the CLI of that Rack Monitor 250 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 Monitor 250 is configured, you can access the Rack Monitor 250 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 Monitor 250 and use the MAC address of the Rack Monitor 250 in the ARP command. For example, to define an IP address of 156.205.14.141 for a Rack Monitor 250 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 Monitor 250.
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 Monitor 250 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 21 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 Monitor 250.
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 Monitor 250 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 Monitor 250.
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 Monitor 250 restarts to apply the changes.

For more detailed information on tcpip commands, see tcpip, page 136 or tcpip6, page 137.

# Network Management with Other Applications

These applications and utilities work with a Rack Monitor 250 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 Monitor 250 units over the network.
- Security Wizard: Create components needed to help with security for the Rack Monitor 250 units when you are using Secure Sockets Layer (SSL)/ Transport Layer Security (TLS) and related protocols and encryption routines.

# Wire the Modbus Interface

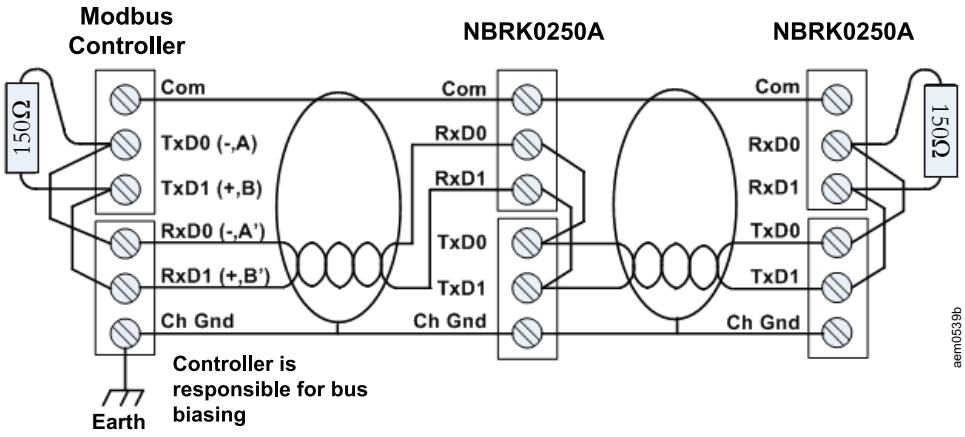
The NetBotz Rack Monitor 250 connects to your building management system using the Modbus RS-485 interface. The Modbus interface supports two-wire and four-wire RS-485, plus ground.

The Modbus standard specifies 150 ohm termination resistors at each end of a bus. Unless the bus is very long and operating at high data rates, these resistors are not needed. Busses under 2000 feet operating at 9600 baud, or under 1000 feet operating at 19,200 baud, should not require termination.

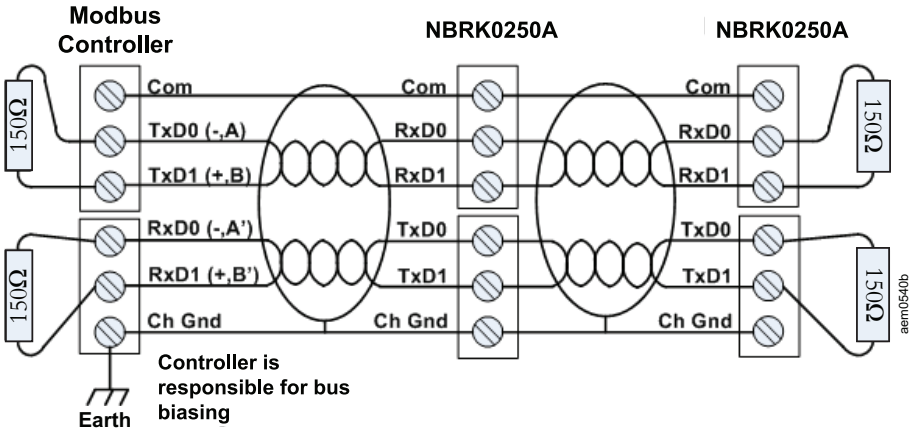
For more information on Modbus, see the Modbus standard at www.modbus.org.

For details on Modbus register settings, see the Modbus register map document for your appliance on www.apc.com.

**Two-wire (half-duplex) connection diagram**




**Four-wire (full-duplex) connection diagram**



# Connect Wired Sensors and Devices

| NOTICE |
| --- |
| **EQUIPMENT DAMAGE RISK**<br>Only connect approved devices to ports on the Rack Monitor 250 as directed in this manual.<br>**Failure to follow these instructions can result in equipment damage.** |

Connecting non-approved devices will cause the Rack Monitor 250 to reboot and may result in equipment damage.

The following sensors and devices connect to specific ports:

| Sensor/Device | Port/connection requirements |
| --- | --- |
| Door switch sensors<br>• NBES0302<br>• NBES0303 | Universal sensor ports |
| Sensor Pod150 (NBPD0150) | A-Link ports |
| Temperature sensors<br>• Temperature/Humidity Sensor with Display (AP9520TH)<br>• Temperature Sensor (AP9335T)<br>• Temperature/Humidity Sensor (AP9335TH) | A-Link ports<br>Universal sensor ports |
| Other NetBotz Sensors<br>• Spot Fluid Sensor (NBES0301)<br>• Dry Contact Cable (NBES0304)<br>• 0–5 V Sensor Cable (NBES0305)<br>• Vibration Sensor (NBES0306)<br>• Smoke Sensor (NBES0307)<br>• Leak Rope Sensor (NBES0308) | Universal sensor ports |
| Third-party 0–5 V sensors | Standard third-party 0–5 V sensors require the NetBotz 0–5 V Sensor Cable (NBES0305). To connect a sensor to the cable, follow the instructions provided with the sensor and the instructions provided with the cable. |
| Third-party dry contact sensors | Third-party dry contact sensors require the NetBotz Dry Contact Cable (NBES0304). To connect a sensor to the cable, follow the instructions provided with the sensor and the instructions provided with the cable. |

**NOTES:**

- The Rack Monitor 250 is not compatible with the Door switch cable included with the NetBotz Rack Access PX-HID (AP9361) or the NetBotz Sensor Pod 180 (NBPD0180).
- If a sensor cable is not long enough, use an RJ-45 coupling (provided with some sensors) and standard CAT-5 cabling to extend the cable. See Specifications, page 167 for maximum cable lengths.
- You can extend the total length of the Leak Rope Sensor (NBES0308) up to 30.5 m (100 ft) using the Leak Rope Sensor Extension (NBES0309).

# Cascade Sensors and Pods from A-Link Ports

**NOTICE**

**EQUIPMENT DAMAGE RISK**

- Do not use crossover cables.
- Do not cascade appliances. Use one appliance per system.
- Do not connect A-Link devices to an Ethernet bus.

**Failure to follow these instructions can result in equipment damage.**

A-Link is an APC proprietary Controller Area Network (CAN) bus. Devices compatible with A-Link are not Ethernet devices and cannot coexist on an Ethernet bus with other networking devices, such as hubs and switches.

Before performing this procedure, follow the installation instructions provided with the devices you plan to cascade. You can cascade any or all of the following:

- Up to eight (8) Temperature/Humidity Sensors with Digital Display (AP9520TH).
- A combined total of up to twelve (12) NetBotz Rack Sensor Pod 150 (NBPD0150) units and NetBotz Rack Access Pod 175 (NBPD0175) units. For example, six (6) Rack Sensor Pod 150 units and six (6) Rack Access Pod 175 units.
  Connect a supplemental power supply (AP9505i) to every third Rack Access Pod 175 and every fourth Rack Sensor Pod 150.

  OR

  A maximum of twelve (12) NetBotz Rack Access Pod 175 (NBPD0175) units, with Rack Access Handle Kit 125 (NBPD0125) and 1356 (NBPD1356).
  You can add up to 12 rack access pods by connecting a supplemental power supply (AP9505i) to every third pod. Otherwise, a communication loss may occur.

  OR

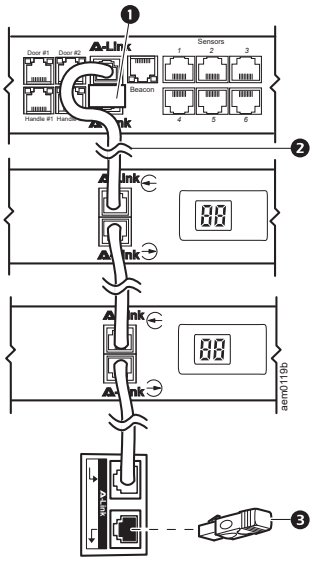
  A maximum of twelve (12) NetBotz Rack Sensor Pod 150 (NBPD0150) units.
  You can add up to 12 sensor pods by connecting a supplemental power supply (AP9505i) to every fourth pod.

  You can connect NetBotz Leak Rope Sensors (NBES0308) to the universal sensor ports on the appliance and to the ports on each connected NetBotz Rack Sensor Pod 150. You can extend the total length of the sensor up to 30.5 m (100 ft) using the Leak Rope Sensor Extension (NBES0309).

To connect sensors and sensor pods to A-Link ports,

1. Connect sensors and sensor pods to the appliance as shown.
   - Connect to in and out ports as shown.
   - The combined length of all A-Link cables (❷) must not exceed 1000 m (3,280 ft).
   - Use CAT-5 (or equivalent) Ethernet patch cables (❸).
2. Plug an A-Link terminator (❶) into the unused A-Link port.
3. Connect supplemental power supplies (AP9505i) to the 24 VDC Inputs on your devices as required.

   **NOTE:** The first time a sensor pod receives power, it obtains a unique identification address for communication over the A-Link bus. To avoid communication problems, complete steps 1 and 2 before you connect a supplemental power supply.



# The Wireless Sensor Network

The wireless sensor network is made of a host appliance, a coordinator, routers, and end devices.

- The **host appliance** (your NetBotz Rack Monitor or Room Monitor) collects data from the wireless sensor network and generates alerts based on sensor readings.
- The **coordinator** is connected directly to the host appliance via USB. It reports data from the sensors on the network and provides available firmware updates to the wireless network. Each wireless sensor network must have only one coordinator, which is connected to a dedicated USB Type A port on the appliance.
- **Routers** extend the range of the wireless sensor network. Routers pass information between themselves and the coordinator, and between the coordinator and end devices. Each router is powered by an AC-USB adapter, not directly connected to the host appliance.

  Routers are optional. In a data center environment where obstructions are common, routers are recommended if sensors are more than 15 m (50 ft) from the coordinator.
- **End devices** monitor attached and internal sensors and send data back to the host appliance. End devices are powered by batteries, and are not connected to the host appliance.

# ZigBee for the Wireless Sensor Network

Zigbee is a communication standard for wireless networks. NetBotz appliances use Zigbee to communicate with supported wireless sensors via a wireless coordinator. Communication between each Wireless Sensor and the Coordinator is encrypted using two different keys:

- A Master key programmed into each sensor. This is a Schneider Electric proprietary key, not the Zigbee Alliance's default global trust center link key.
- A Session key negotiated between each sensor and the coordinator. This key is used to encrypt all communication between that sensor and the coordinator.
- Wireless device auto-join is supported but disabled by default. By default, the user must join all wireless devices manually to the appliance through Advanced View.

# Devices on the Wireless Sensor Network

**NOTICE**

**EQUIPMENT DAMAGE RISK**

Only the devices listed here are compatible with the NetBotz wireless sensor network. Other devices may not function and may damage the appliance or other wireless devices.

**Failure to follow these instructions can result in equipment damage.**

| Device | Network Role |
|---|---|
| USB Coordinator & Router (NBWC100U) | Coordinator when connected to the appliance USB port<br>Router when connected wirelessly and powered by an AC-USB adaptor |
| Wireless Temperature Sensor (NBWS100T) | End device |
| Wireless Temperature/Humidity Sensor (NBWS100H) | End device |

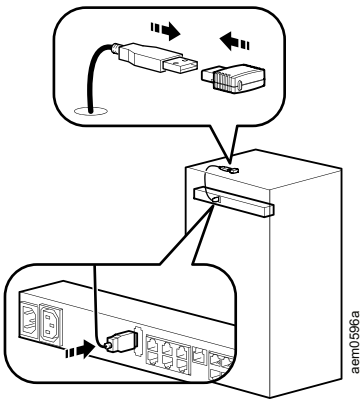
The network can support up to 47 wireless routers or end devices, plus one coordinator.

**NOTE:** Wireless devices have a range of up to 30.5 m (100 ft), line of sight. In a data center environment where obstructions are common, a range of 15 m (50 ft) is typical for any wireless device.

# Enhancing the Wireless Signal

It is recommended that you mount the routers and coordinator above the racks to reduce physical obstructions and increase signal coverage. Mounting the routers 3–4.5 m (10–15 ft) away from the coordinator also helps to increase the signal range. If the Received Signal Strength Indicator (RSSI) is still below 80 after adjusting the router placement, consider mounting the end devices on the outside of the rack to further reduce physical obstructions to the network.

You can use the NBWC100U USB-A extender cable to place the wireless coordinator on top of the rack or in a cable tray above the rack as needed.



# Connect the Wireless Sensor Network

The order in which you configure your wireless sensor network and apply power to your wireless devices is important:

1. Select the coordinator and routers. If you have a pre-installed USB Coordinator and Router on your appliance, it acts as the coordinator. Note the extended address of the coordinator. If necessary, choose one or more USB Coordinator & Routers to become routers.
2. Choose the locations for the routers and end devices. Do not turn on the routers or end devices at this time.
3. Connect the Coordinator to the designated USB port on the NetBotz appliance.
4. Use an AC-USB adapter to apply power to each router. Routers are not directly connected to the NetBotz appliance.
5. Turn on the end devices after the coordinator and routers. This helps to preserve battery life.
6. Add end devices (wireless sensors) to the wireless sensor network.

# Troubleshooting the Wireless Sensor Network

During the boot process, the Coordinator LED does the following:

1. Flashes a quick green, yellow, red sequence
2. Alternately flashes green and yellow for about 30 seconds
3. Flashes green 3 times
4. Turns solid yellow for 5 seconds
5. Flashes a quick green, yellow, green sequence

After the boot process is complete, LED activity on the Coordinator signifies its status:

| Condition | Description |
|---|---|
| Flashes green | Normal. The network was formed successfully. |
| Off | Forming a network.<br>or<br>Not communicating with the Rack Monitor 250. Reboot the Coordinator. |
| Solid red | Unable to form a network. Reboot the Coordinator.* |

To reboot the coordinator, remove the plastic cover, then press and hold the LED for up to three seconds.

If the LED flashes red three times, then slowly flashes red, contact Technical Support.

# Recover from a Lost Password

To recover from a lost password, you must reset the Rack Monitor 250 to its default configuration. Export the .ini file after configuring your Rack Monitor 250 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.

To reset the Rack Monitor 250:

1. On the display interface, 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 Monitor 250 to complete its reboot process.
2. Access the Rack Monitor 250 through a secure connection with the default username and password (**apc** and **apc**).

   Secure connections include a local connection to the CLI by serial cable, a remote connection to the CLI by SSH, or a connection to the web UI by HTTPS. Instructions for each of these secure connections are covered in this manual. Insecure connections are disabled by default.
3. Reset the username and password, then configure the Rack Monitor 250 settings as needed.

# 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 Monitor 250 through its Web UI. Other commonly available browsers and versions may work but have not been fully tested.

The Rack Monitor 250 cannot work with a proxy server. Before accessing the Web UI of the Rack Monitor 250, do one of the following:

- Configure the browser to disable the use of a proxy server for your Rack Monitor 250.
- Configure the proxy server so that it does not proxy the specific IP address of your Rack Monitor 250.

# Log on to the Web UI

To access the Web UI and configure the security settings of your Rack Monitor 250 on the network:

1. Type the DNS name or IP address of the Rack Monitor 250 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 Monitor 250. 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 Monitor 250 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:b7fSf:fe00:1100]:5000` if HTTPS (HTTP with SSL/TLS) is your access mode

# First Log On

When you log on to the Rack Monitor 250 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 Monitor 250.

## Menus

The following pages and menus are available:

- **Home Page:** View the status of connected sensors and recent events.

  **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 default page back to Home, click the home target icon .
- **Status Menu:** Provides the status of connected sensors, devices, and the Network.
- **Control:** Allows immediate action affecting security settings, network configuration, and devices connected to outputs.
- **Configuration:** Update the settings of the Rack Monitor 250 and connected devices.
- **Tests:** Allows you to run an LED Blink test.
- **Logs:** View the Event, Data, and Firewall Logs.
- **About:** View support information and information specific to your Rack Monitor 250 unit.

## Limited Status Access

When enabled, the Limited Status page allows you to use a Web browser to view limited information about the Rack Monitor 250 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 Monitor 250.
- 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 Monitor 250 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 Monitor 250.

| Icon | Description |
|---|---|
|  | **Informational**: Notification that a device event has occurred. |
| | **No Alarms:** No alarms are present, and the Rack Monitor 250 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 Monitor 250 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: APC Frequently Asked Questions (FAQ) page
- Link 3: Additional information on Security and Environmental Monitoring 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.

# Home Page

**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 default page back to Home, click the home target icon .

The Home page displays the alarm status of system devices: Critical (device requires immediate attention), Warning (attention required), Normal (no alarms), Informational, or Inactive.

A single status area appears for each sensor type. If more than one of each sensor is connected, you can select **More** to view all attached sensors. If only one sensor is attached, you can select **More** to view and edit the sensor settings.

There is only one of each output device (Beacon, Output Relay, and Switched Outlet). You can select the name of the output device to edit the output settings.

If Rack Access handles are connected to the Rack Monitor 250, the **Rack Access** status area shows the status of the Door 1/Door 2. You can select **Lock Control** to lock or unlock the doors.

**Reset Alarms**: If communication is lost with a device, or if a temperature sensor's rate-of-change is exceeded, a **Reset Alarms** link will appear. Click the link to clear the alarm if, for example, you intentionally disconnected a sensor or to acknowledge a rate of change.

A list of recent device events appears at the bottom of the Home page. Click **More Events** to open the Event Log.

# Configuring Modules, Sensors, Output Devices, and Alarms

A device refers to any equipment with a wired or wireless connection to the Rack Monitor 250. The following are general terms for kinds of devices that are compatible with the Rack Monitor 250:

- *Sensors* provide information to the Rack Monitor 250. Sensors can be wired or wireless.
- *Modules* are of sensor pods that provide feedback from multiple sensors to the Rack Monitor 250.
- *Output devices* are controlled by the outputs on the Rack Monitor 250.

In the Web UI, all devices are managed with Configuration pages and Information pages: Configuration pages allow you to change settings and set up alarms for connected devices, while Information pages provide a quick overview of devices connected to the appliance. The name for each device acts as a link to the configuration page for that device.

## Filtering Module and Sensor Lists

On the information pages for wired sensors and modules, you can click **Create Filter** to search for devices that match specific criteria. Click **Clear Filter** to return to the unfiltered list.

| Filter Setting | Description |
|---|---|
| **Status** | Select one or more alarm statuses to include in your search: **Lost Comm**(Lost Communication),**Critical**, **Warning**, **Information**, **Normal**, or **FW Upgrade**.<br><br>**Lost Comm**and **FW Upgrade** are only available for modules. |
| **Temperature**/ **Humidity** / **Voltage** | Enter a **Temperature**, **Humidity**, or **Voltage** value. Then select whether to view sensors that detect conditions **Less Than**, **Equal To**, or **Greater Than** the value you entered. |
| **State** | Search for the current state of a discrete-state sensor (for example, a smoke or vibration sensor). |
| **Name** / **Location** / **Module Name** | Search for one of these user-defined attributes. You can select the following parameters to narrow your search:<br>• **Case sensitive**<br>• **Whole Word:** Include only complete word matches. If this is not selected, the filter will include partial word matches. |
| **Module ID** | The module ID for a Sensor Pod 150 is displayed on the Identifier LED of the sensor pod. The module ID for the Rack Monitor 250 is always NB. |

# View and Configure Module Settings

Path: **Configuration > Device > NetBotz**

The module sensor information page allows you to view information for the Rack Monitor 250 and all connected modules, create a filter to show only specific modules, and use the mass configuration feature to configure multiple modules at a time.

The following information is available on the module information page.

| Setting | Description |
|---|---|
| **Status** | The alarm status of the module: **Lost Comm**(Lost Communication),**Critical**, **Warning**, **Information**, **Normal**, or **FW Upgrade**. |
| **Module Name / Location** | User defined name and location of the module (up to 20 characters). |

Click a module name to view the module's configuration page, which includes fields to edit the module **Name** and **Location**. The module configuration page also shows all devices connected to the module.

# Manage Wired Sensors

Wired sensors have a physical connection to the appliance.

## View Wired Sensors

The wired sensor information pages allow you to view information for all wired sensors of a single type, create a filter to show only specific sensors, and use the mass configuration feature to configure all sensors on a page.

You can reach the wired sensor information pages in several ways:

- Click **More >** under any status area for the desired sensor type. Status areas are visible from the **Home** page, and from **Status > Alarm Status**.
- Go to **Status > Wired Sensor >** *your sensor type*.
- Go to **Configuration > Device > Wired Sensor >** *your sensor type*.

Near the top right of the page, a temperature icon shows whether the current temperature is measured in Fahrenheit or Celsius. You can click this icon to toggle the temperature setting.



In addition to the sensor reading, the following information is available on the wired sensor information pages. Settings vary by sensor type.

| Setting | Description |
|---|---|
| **Status** | The current alarm status: **Critical** (immediate attention required), **Warning** (attention required), **Normal**, **Informational**, or **Inactive**. By default, all information is sorted by status. To sort by another column heading, click its name. |
| **Name** | User-defined name of the sensor (up to 20 characters). Click a sensor's name to configure its settings. |
| **State** | The current sensor state. |
| **Location** | User-defined location of each sensor (up to 20 characters). |
| **Module Name** | Name of the module to which the sensor is connected: the Rack Monitor 250 or the Sensor Pod 150. Click a module name to view the module's factory information and all devices connected to the module, or to configure the module's name and location. |

# Mass-configure Sensor Settings

You can use the mass configuration feature to update the settings for all sensors of a certain type at once.

Click **Mass Configuration**, then select the settings you want to configure. Click **Next** to configure those settings. Available settings vary by sensor type. You can click **Cancel** to discard your changes at any step in the procedure.

| Setting | Description |
|---|---|
| **General** | • **Name** and **Location:** User-defined name and location of the sensor (up to 20 characters). You can use these wild cards: `%m` (the parent module ID), `%p` (the sensor port number), and `%l` (the parent module location).<br>• **Alarm Generation:** When **Alarm Generation** is disabled, the system continues to monitor the state of the sensor, but does not generate alarms. Alarms are not recorded in the event log when **Alarm Generation** is disabled. |
| **State** | • **Normal State:** Select the normal state of a discrete-state sensor. An alarm is generated when the sensor changes to an abnormal state.<br>• **Severity:** Select the severity of alarms generated for discrete-state sensors. |
| **Temperature / Humidity Thresholds** | • **Maximum:** The maximum allowable value. If the temperature or humidity rises above this value, a critical alarm is generated.<br>• **High:** If the temperature or humidity rises above this value, a warning alarm is generated.<br>• **Low:** If the temperature or humidity falls below this value, a warning alarm is generated.<br>• **Minimum:** The minimum allowable value. If the temperature or humidity falls below this value, a critical alarm is generated.<br>• **Hysteresis:** This value specifies how much the temperature or humidity must change to clear a threshold violation. **Example:** The maximum temperature threshold is set to 45 °C, and hysteresis is set to 3. The temperature rises above 45 °C, so a critical alarm is generated. The temperature must fall below 42 °C (45–3) to clear the critical alarm. |
| **Voltage Thresholds** | • **Maximum:** If the voltage rises above this value, a critical alarm is generated.<br>• **Minimum:** If the voltage falls below this value, a critical alarm is generated. |
| **Temperature Rate of Change** | Configure the acceptable short-term and long-term changes in temperature. When the rate of change is exceeded, the appliance generates a critical alarm. Short-term changes are measured over minutes, while long-term changes are measured over hours.<br>• **S.T. Increase:** Short-term temperature increase<br>• **L.T. Increase:** Long-term temperature increase<br>• **S.T. Decrease:** Short-term temperature decrease<br>• **L.T. Decrease:** Long-term temperature decrease<br>• **Reset Rate Alarms:** Clear all existing rate of change alarms. |

# Configure Wired Sensors

The wired sensor configuration pages allow you to change the settings and configure alarm thresholds for a specific wired sensor.

You can reach the wired sensor configuration pages in several ways:

- Click **More >** under any status area for the desired sensor type to open the sensor information page. Status areas are visible from the **Home** page, and from **Status > Alarm Status**. On the sensor information page, click the name of the sensor you want to configure.
- Go to **Status > Wired Sensor >** *your sensor type*. Select the name of the sensor you want to configure.
- Go to **Configuration > Device > Wired Sensor >** *your sensor type*. Select the name of the sensor you want to configure.

Near the top right of the page, a temperature icon shows whether the current temperature is measured in Fahrenheit or Celsius. You can click this icon to toggle the temperature setting.



At the bottom of the page, you can click **Apply** to save your changes or **Cancel** to discard them.

You can configure the following settings from the wired sensor configuration pages. Available settings vary by sensor.

| Setting | Description |
|---|---|
| **Name** / **Location** | User-defined name and location of the sensor (up to 20 characters). You can use these wild cards: `%m` (the parent module ID), `%p` (the sensor port number), and `%l` (the parent module location). |
| **Module Name** / **Module Location** | User-defined name and location of the Rack Monitor 250 or the Sensor Pod 150 to which the sensor is connected (up to 20 characters). You can use these wild cards: `%m` (the parent module ID), `%p` (the sensor port number), and `%l` (the parent module location). |
| **Temperature** / **Humidity** / **Voltage** | The current sensor reading. (Temperature/Humidity/Voltage sensors only.) |
| **State** | The current sensor state. (Discrete sensors only.) |
| **Alarm Generation** | When **Alarm Generation** is disabled, the system continues to monitor the state of the sensor, but does not generate alarms. Alarms are not recorded in the event log when **Alarm Generation** is disabled. |
| **Alarm Status** | The current alarm status: **Critical** (immediate attention required), **Warning** (attention required), **Normal**, **Informational**, or **Inactive**. By default, all information is sorted by status. To sort by another column heading, click its name. |
| **Temperature / Humidity Alarms** | Select **Threshold Settings** to set the following thresholds for temperature and humidity:<br>• **Maximum:** The maximum allowable value. If the temperature or humidity rises above this value, a critical alarm is generated.<br>• **High:** If the temperature or humidity rises above this value, a warning alarm is generated.<br>• **Low:** If the temperature or humidity falls below this value, a warning alarm is generated.<br>• **Minimum:** The minimum allowable value. If the temperature or humidity falls below this value, a critical alarm is generated.<br>• **Hysteresis:** This value specifies how much the temperature or humidity must change to clear a threshold violation. **Example:** The maximum temperature threshold is set to 45 °C, and hysteresis is set to 3. The temperature rises above 45 °C, so a critical alarm is generated. The temperature must fall below 42 °C (45–3) to clear the critical alarm. |
| **Voltage Alarms** | Select **Threshold Settings** to set the following thresholds for voltage:<br>• **Maximum:** If the voltage rises above this value, a critical alarm is generated.<br>• **Minimum:** If the voltage falls below this value, a critical alarm is generated. |
| **Temperature Rate of Change Alarms** | Select **Rate of Change Settings** to configure the acceptable short-term and long-term changes in temperature. When the rate of change is exceeded, the appliance generates a critical alarm. Short-term changes are measured over minutes, while long-term changes are measured over hours.<br>• **S.T. Increase:** Short-term temperature increase<br>• **L.T. Increase:** Long-term temperature increase<br>• **S.T. Decrease:** Short-term temperature decrease<br>• **L.T. Decrease:** Long-term temperature decrease<br>• **Reset Rate Alarms:** Clear all existing rate of change alarms. |
| Discrete sensor settings | Discrete sensors detect a single condition instead of a measurable range. For each discrete sensor, you can select the **Normal State**. The alternate state will generate an alarm. You can then select the **Severity** of the alarm generated when the sensor is not in its normal state.<br>Discrete sensors include Dry Contact Inputs, Smoke sensors, Vibration sensors, Fluid detectors, and Door sensors. |

# Manage Rack Access

| NOTICE |
| --- |
| The Mifare Classic card format is vulnerable to cloning. If you use this format, maintain the physical security of your access cards. Consider updating to the MIFARE Plus format. |

The Rack Monitor 250 can support up to 200 registered cardholders. You may be able to configure more than 200 cardholders by using a RADIUS server, LDAP server, or TACACS+ server for authentication.

Both rack handles connected to the appliance, and both rack handles connected to a Rack Access Pod 175, must be the same model: either two 125 kHZ handles (NBPD0125) or two 13.56 MHz handles (NBPD1356). The proximity card type must be the same for both handles.

The following Rack Access Card types are supported:

| **Handle type** | **125 kHZ** | **13.56 MHz** |
| --- | --- | --- |
| **Supported card types** | • H10301 26-bit<br>• H10302 37-bit<br>• H10304 37-bit with facility code<br>• CORP1K35 (Corporate 1000 35 bit)<br>• CORP1K48 (Corporate 1000 48 bit) | • MIFARE Classic 4-byte UID<br>• MIFARE Classic 7-byte UID<br>• MIFARE DESFIRE<br>• MIFARE PLUS<br>• iClass 8-byte |

# Register a New User/Proximity Card

You must have access to the Web UI and physical access to the rack access handles to complete this process.

Lock Properties settings apply to the rack access devices connected directly to the appliance and to all connected Rack Access Pods.

1. In the Web UI, go to **Configuration > Device > Rack Access > Lock Properties**.
2. Select **Enable** to enable the card reader.

   You can select the card type from the drop-down list. Otherwise, the appliance will automatically recognize the card type when **Automatic Card Format Recognition**is set to On.

   Specify the **Auto-Relock** time. If desired, configure the **Door Open Alarm** for Internal Door 1 only, Internal Door 2 only, External POD 1 - 12 Door 1 only, External POD 1 -12 Door 2 only, or all doors, and then click **Apply**..
3. Hold the unregistered proximity card in front of the proximity reader on the handle until you hear a beep.
4. In the Web UI, Go to **Configuration > Device > User Access > Unregistered Users**.
5. Click the card ID number to specify the following setting for the rack access card:

| Setting | Description |
|---|---|
| **Name** | The name for the card user (up to 20 characters). |
| **Contact** | The contact information for the card user (up to 20 characters). |
| **Card ID** | The identification number of the proximity card assigned to the user. This option is not configurable. |
| **Account Access** | Select **Account Access** to activate the proximity card. Clear the check box to disable access permissions for the proximity card. |
| **Door Access** | Select the doors the proximity card is able to open. |
| **Granted Access Schedule** | Select the days and configure the times during which the proximity card is permitted to unlock the doors. Use 24-hour clock values (00:00 to 23:59). By default, all hours are permitted. |

Click **Register User** to save the user configuration, or click **Cancel** to discard the changes.

Once a user is registered, you can click **Delete User** to erase the configured information and remove the card from the list of registered users. If the deleted card is held in front of a rack access handle, the card number appears in the list of unregistered users.

To modify any of these settings for a registered user, go to **Configuration > Device > User Access > Registered Users**.

To specify how rack access users are authenticated, go to **Configuration > Device > Rack Access > RADIUS**

# Update A Registered User Account

**Path: Configuration > Device > Rack Access > Registered Users**

Select a registered user's name to view the card ID number and to edit name, contact information, and access permissions.

| Setting | Description |
|---|---|
| **Name** | The name of the user (up to 20 characters). |
| **Contact** | The contact information for the user (up to 20 characters). |

| Setting | Description |
|---|---|
| **Door Access** | The doors the access card is configured to unlock: Internal Door 1 only, Internal Door 2 only, External POD 1 - 12 Door 1 only, External POD 1 -12 Door 2 only, or all doors.<br>Configuration is limited to one door or all doors. It is not possible to configure user access for individual rack access pods.; |
| **Time Scheduled** | **Granted**: The user's access schedule is configured.<br>**Not Configured** : The user's access schedule is not configured.<br>Until the schedule is configured, this card cannot unlock enclosure doors. |

# Configure Rack Access User Authentication

By default, authentication happens at the NetBotz appliance only.

| Setting | | Description |
|---|---|---|
| **Lock User Authentication Method** | | |
| | **Local NetBotz appliance only** | RADIUS is disabled. Rack access is controlled by the local authentication configured in the Registered Users option. |
| | **RADIUS, then Local NetBotz appliance** | RADIUS is enabled, and local rack access authentication is enabled. Authentication is requested from the RADIUS server first; local rack access authentication is used only if the RADIUS server fails to respond. |
| | **RADIUS Only** | RADIUS is enabled. Local rack access authentication is disabled. If the RADIUS server fails to authenticate the user, access is denied. |
| **Radius Server Settings**<br>**NOTE:** The message **No RADIUS servers have been configured** indicates you must add a properly configured RADIUS server before RADIUS authentication can operate. See Configure a RADIUS Server, page 68 for configuration instructions. | | |
| | **RADIUS New password/ Confirm password** | Set or disable the RADIUS password for Rack Access authenticationConfigure a RADIUS Server, page 68. The password (1 - 64 characters) is enabled by default. The default RADIUS password is the serial number of the NetBotz appliance, displayed under **About > Network**. |

# Lock/Unlock Rack Access Handles

**Path: Control > Lock Control**

Lock and unlock the rack access handle connected to the Door Handle 1 and Door Handle 2 ports on the appliance or on connected Rack Access Pod 175 Pods.
This page is only available when rack access handles are connected to the Rack Monitor 250 or Rack Access Pod 175.
Lock Control settings apply to the rack access devices connected directly to the appliance and to all connected Rack Access Pods.

# Schedule an Automatic Unlocking Event

**Path: Configuration > Device > Rack Access > Schedule**

Use the following settings to schedule a date and time to automatically unlock the doors.
One-time schedule settings apply to the rack access devices connected directly to the appliance and to all connected Rack Access Pods.

| Setting | Description |
|---|---|
| **One-time Schedule** | Enable or disable the scheduled unlock. |
| **Date** | Specify the date for the unlocking event (mm/dd/yy). |
| **Time** | Specify the time at which the doors will unlock. Use the 24-hour clock. |
| **Unlock Doors** | Unlock Internal Door 1 only, Internal Door 2 only, External POD 1 - 12 Door 1 only, External POD 1 -12 Door 2 only, or all doors. |
| **Remain Unlocked for** | Specify how long the doors will remain unlocked. |

Click **Apply** to save your changes, or click **Cancel** to discard them.

# Manage the Wireless Sensor Network

**Path: Configuration > Device > Wireless Sensor Network**

The Wireless Network Configuration Page allows you to view the status, address, firmware version, and identification information for the coordinator and for each sensor in the commission list. You can use this page to add or remove sensors, or to enable or disable the entire wireless sensor network.

When a sensor is added to the wireless sensor network, it appears in the **Wireless Sensor Commission List**. Sensors remain in the commission list even when disconnected. Alarms for each sensor remain in the data log until you remove the sensors from the commission list.

## Add Sensors to the Commission List

**NOTE:** Ensure wireless sensors are within range of the coordinator or a connected router. Each wireless device has a maximum line-of-sight range of 30.5 m (100 ft). In a data center environment where obstructions are common, a range of 15 m (50 ft) is typical.

You can add up to 47 wireless sensors to the commission list.

To add sensors automatically, click **Enable Auto Join**. The Rack Monitor 250 will detect and add all wireless sensors that are in range and that are not already part of another network.

Wireless sensors appear in the Commission list as they join the network. Auto Join runs for five hours, or until you end the process manually.

To add a sensor manually, click **Add New Sensor**, update the sensor settings, then click **Apply**. You must enter the extended address (MAC) for each sensor.

## Remove Sensors from the Commission List

Click the sensor name to open the sensor configuration page. Then click **Remove**.

## Disable or Enable the Wireless Sensor Network

1. On the wireless network configuration page (**Configuration > Device > Wireless Sensor Network**), click **Disable Coordinator** or **Enable Coordinator**.
2. Go to **Control > Network > Reset/Reboot**.
3. Select **Reboot Network Management Interface**, then click **Apply**.

# View Wireless Sensors

The **Wireless Sensor Information** page allows you to view all connected wireless temperature and temperature/humidity sensors.

You can reach the **Wireless Sensor Information** page in several ways:

- From the **Home** page, click **More >** under the **Wireless Sensors** status area.
- Go to **Status > Wireless Sensor Network**.

Near the top right of the page, a temperature icon shows whether the current temperature is measured in Fahrenheit or Celsius. You can click this icon to toggle the temperature setting.



| Setting | Description |
|---|---|
| **Status** | The current alarm status: **Critical** (immediate attention required), **Warning** (attention required), **Normal**, **Informational**, or **Inactive**. By default, all information is sorted by status. To sort by another column heading, click its name. |
| **Name** | User-defined name of the sensor (up to 20 characters). Click a sensor's name to configure its settings. |
| **Extended Address** | The extended MAC address of each sensor. |
| **Location** | User-defined location of each sensor (up to 20 characters). |
| **Type** | The type of sensor. |
| **Temperature** | The temperature reading from each sensor, if available. |
| **Humidity** | The humidity reading from each sensor, if available. |
| **Signal** | The Received Signal Strength Indicator (RSSI). The strength of the wireless signal between each sensor and the Router or Coordinator to which it sends data. A reading above 30% is ideal. |
| **Battery** | The battery voltage for each sensor, if available. |

# Configure Wireless Sensors

The **Wireless Sensor Configuration** page allows you to change the settings of a specific wireless sensor, or to remove the sensor from the commission list.

You can reach the **Wireless Sensor Configuration** page in several ways:

- Click **More >** under any status area for the desired sensor type. Status areas are visible from the **Home** page, and from **Status > Alarm Status**.
- Go to **Status > Wireless Sensor Network**. Select the name of the sensor you want to configure.
- Go to **Configuration > Device > Wireless Sensor Network**. Select the name of the sensor you want to configure.

Near the top right of the page, a temperature icon shows whether the current temperature is measured in Fahrenheit or Celsius. You can click this icon to toggle the temperature setting.



At the bottom of the page are three options: **Apply**, **Cancel**, and **Remove** . Click **Apply** to save your changes. Click **Cancel** to discard your changes. Click **Remove** to remove the sensor from the commission list and remove that sensor's data from the data log.

You can configure the following settings from the wireless sensor configuration pages. Available settings vary by sensor type.

| Setting | Description |
|---|---|
| **Name** / **Location** | User-defined name and location of the sensor (up to 20 characters). |
| **Extended Address** | The extended MAC address of the sensor. |
| **Alarm Generation** | When **Alarm Generation** is disabled, the system continues to monitor the state of the sensor, but does not generate alarms. Alarms are not recorded in the event log when **Alarm Generation** is disabled. |
| **Temperature / Humidity Thresholds** | • **Maximum:** The maximum allowable value. If the temperature or humidity rises above this value, a critical alarm is generated.<br>• **High:** If the temperature or humidity rises above this value, a warning alarm is generated.<br>• **Low:** If the temperature or humidity falls below this value, a warning alarm is generated.<br>• **Minimum:** The minimum allowable value. If the temperature or humidity falls below this value, a critical alarm is generated. |
| **Battery / Signal Thresholds** | • **Low:** If the battery voltage or signal strength drops below its low threshold for the sensor, an alarm occurs.<br>• **Minimum:** If the battery voltage or signal strength drops below its minimum threshold for the sensor, an alarm occurs. |

# Update the Wireless Sensor Network

Firmware updates for the wireless sensor network are included with updates for your appliance. When you update the firmware on your appliance, any new firmware for wireless devices appears in the Target field. Update the firmware on the wireless devices when the Target firmware version does not match the Current firmware version.

On the **Wireless Network Configuration** page:

The **Update** button is activated when the **Target** firmware version is newer than the **Current** firmware version.

Click **Update** to begin the firmware update for the sensors, coordinator, and routers. Allow about 20 minutes per wireless sensor for the update to complete.

**NOTE:** The sensors are updated first and automatically reboot after the firmware is downloaded. Then the coordinator and the routers are updated.

The **Apply** button is activated when all the sensors are updated, and the firmware on the coordinator and routers is staged.

Click **Apply** to reboot the coordinator and routers.

**NOTE:** The firmware update can be interrupted. If the update does not complete, reboot the NetBotz appliance and repeat the update process.

# Manage Output Devices

The outputs consist of the Beacon port, Output Relay port, and Switched Outlet. Devices connected to these outputs are controlled by the output settings.

The output configuration pages allow you to

- change the output settings
- control the outputs manually
- set up alarm mapping for the outputs

You can reach the output configuration pages in several ways:

- Click **More >** under any status area for the desired output. Status areas are visible from the **Home** page, and from **Status > Alarm Status**.
- Go to **Status > Outputs >** *output type*.
- Go to **Control > Outputs >** *output type*.
- Go to **Configuration > Device > Outputs >** *output type*.

The following information is shown for all outputs:

| Setting | Description |
|---|---|
| **Module Name** / **Module Location** | User-defined name and location of the module on which the output is located (up to 20 characters).<br>**NOTE:** Since the outputs are built into the NetBotz appliance, the NetBotz appliance is always the parent module for outputs. |
| **Alarm Status** | The current alarm status: **Critical** (immediate attention required), **Warning** (attention required), **Normal**, **Informational**, or **Inactive**. By default, all information is sorted by status. To sort by another column heading, click its name. |
| **State** | The current state of the output. |

You can configure the following settings for each output:

| Setting | Description |
|---|---|
| **Name** / **Location** | User-defined name and location of the output (up to 20 characters). |
| **Normal State** | Set the normal state of the output. The normal state for the beacon is always Off and cannot be configured. |
| **Control** | Change the current state of the output. |
| **Alarm Mapping** | Outputs can be activated by alarm states of sensors on the NetBotz module. Select one or more alarms that will change the state of the output. Available alarms vary by output. You can select the alarm description to view and edit which sensors control the output. Any selected sensor, in its abnormal state, activates the output. |

# Manage Active Alarms

You can reach the list of active alarms in several ways:

- Go to the Home page.
- Go to **Status > Alarm Status**

A single status area appears for each sensor type. If more than one of each sensor is connected, you can select **More** to view all attached sensors. If only one sensor is attached, you can select **More** to view and edit the sensor settings.

There is only one of each output device (Beacon, Output Relay, and Switched Outlet). You can select the name of the output device to edit the output settings.

If Rack Access handles are connected to the Rack Monitor 250, the **Rack Access** status area shows the status of the Door 1/Door 2. You can select **Lock Control** to lock or unlock the doors.

By default, alarms only appear in the Web UI. You can configure additional actions for active alarms:

- Configure an attached beacon to turn on when an alarm is activated. See Manage Output Devices, page 48 for instructions.
- Configure the appliance to send notifications when an alarm is activated. See for options and configuration instructions.

# 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 Using the Logs, page 86 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 82.

# 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 86
   - Recipients, page 53
   - Configure Trap Receivers, page 54

# 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**<br>or<br>**Until condition clears** | During an active event, the notification repeats for this number of times.<br><br>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** | The contents of the From field in e-mail messages sent by the Rack Monitor 250.<br>• Use the format *user@ [IP_address]* if an IP address is specified as Local SMTP Server.<br>• Use the format *user@domain* if DNS is configured and the DNS name is specified as Local SMTP Server.<br>**NOTE:** The local SMTP server may require that you use a valid user account on the server for this setting. Check the server documentation. |
| **SMTP Server** | The IPv4/ IPv6 address or DNS name of the local SMTP server.<br>**NOTE:** This definition is required only when the SMTP server is set to **Local**. |
| **Port** | The SMTP port number, with a default of 25. Supported ports include 25, 465, 587, 2525, and 5000 to 32768. |
| **Authentication** | Select **Enable** if the SMTP server requires authentication.<br>**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. |
| **Use SSL/TLS** | Select when encryption is used.<br>• **Never:** The SMTP server does neither requires nor supports encryption.<br>• **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.<br>• **Always:** The SMTP server requires the STARTTLS command to be sent on connection to it.<br>• **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 Monitor 250 for encrypted e-mails to be sent. |
| **File Name** | This field is dependent on the root CA certificates installed on the Rack Monitor 250 and whether or not a root CA certificate is required. |

# 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** | 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.<br><br>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. |
| **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** | Select one of the following methods for routing e-mail:<br>• **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.<br>• **Recipient:** This is the SMTP server of the recipient. The Rack Monitor 250 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.<br>• **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:** | The contents of the From field in e-mail messages sent by the Rack Monitor 250:<br>• In the format user@ [IP_address] (if an IP address is specified as Local SMTP Server)<br>• In the format user@domain (if DNS is configured and the DNS name is specified as Local SMTP Server) in the e-mail messages.<br>**NOTE:** The local SMTP server may require that you use a valid user account on the server for this setting. See the server documentation. |
| **SMTP Server:** | The IPv4/ IPv6 address or DNS name of the local SMTP server.<br><br>**NOTE:** This definition is required only when the SMTP server is set to **Local**. |
| **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** | Select when encryption is used.<br>• **Never:** The SMTP server does not require nor support encryption.<br>• **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.<br>• **Always:** The SMTP server requires the STARTTLS command to be sent on connection to it.<br>• **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 Monitor 250 for encrypted e-mails to be sent. |
| **File Name** | This field is dependent on the root CA certificates installed on the Rack Monitor 250 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 Monitor 250 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 Monitor 250 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.

# Configure Settings for Your Appliance and Web UI

## General Configuration

This menu contains miscellaneous configuration items including device identification, date and time, exporting and importing your Rack Monitor 250 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 Monitor 250 and Data Center Expert.

These fields are used by the **sysName**, **sysContact**, and **sysLocation** object identifiers (OIDs) in the SNMP agent of the Rack Monitor 250. 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 Monitor 250. 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 Monitor 250.
- 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 Monitor 250. By default, any Rack Monitor 250 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 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 to configure another. Retrieve the configuration file (*config.ini*) from the configured , customize that file (e.g., change the IP address), and upload the customized file to the new . The file name can be up to 64 characters, and must have the .ini suffix.

| | |
|---|---|
| **Status** | Reports the progress of the upload.<br>• **No configuration file uploaded:** The Rack Monitor 250 has not been configured with a *config.ini* file.<br>• **Configuration file successfully uploaded:** The Rack Monitor 250 has been configured with a *config.ini* file. You may need to refresh the page to see this message.<br>**NOTE:** The upload succeeds even if the file contains errors, but a system event reports the errors in the Event Log. |
| **Upload** | Browse to the customized file and upload it so that the current Rack Monitor 250 can use it to set its own configuration. |
| **Download** | Allows the download of the *config.ini* file directly through the Web browser to your computer. |

Instead of uploading the file to one , you can export the file to multiple Rack Monitor 250 units by using an FTP or SCP script.

**NOTE:** To retrieve and customize the file of a configured Rack Monitor 250, see How to Export Configuration Settings, page 155.

# 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.

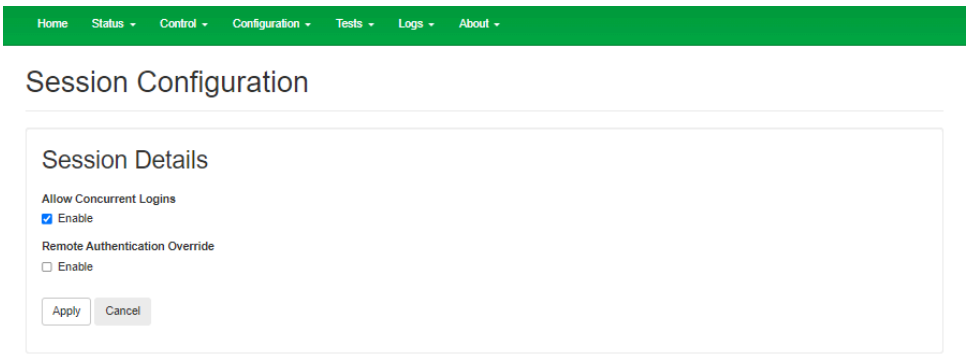
By default, these links access the following Web pages:

- Link 1: The home page of APC website
- Link 2: APC Frequently Asked Questions (FAQ) page
- Link 3: Additional information on Security and Environmental Monitoring equipment

# Manage Security Settings

## Manage Settings for User Sessions

**Path: Configuration > Security > Session Management**

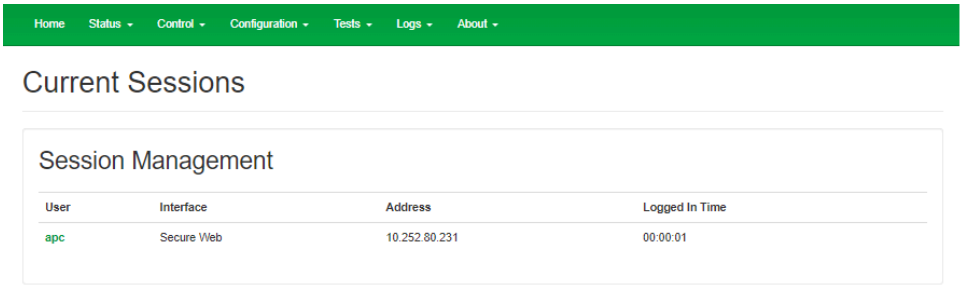



**Allow Concurrent Logins:** Select **Enable** to allow two or more users to log on at the same time. Each user has equal access and each interface (HTTP, FTP, telnet, serial connection, etc.) counts as a logged-in user.

**Remote Authentication Override:** The Rack Monitor 250 supports RADIUS storage of passwords on a server. However, if you enable this override, the Rack Monitor 250 will allow a local user to log on using the password stored locally on the Rack Monitor 250. For more information, see Manage Local User Settings, page 60 and Manage Remote User Settings, page 63.

## Manage User Sessions

**Path: Control > Security > Session Management**




The **Session Management** menu displays all active users currently connected to the Rack Monitor 250. 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.

# Enable Ping Response

**Path: Configuration > Security > Ping Response**

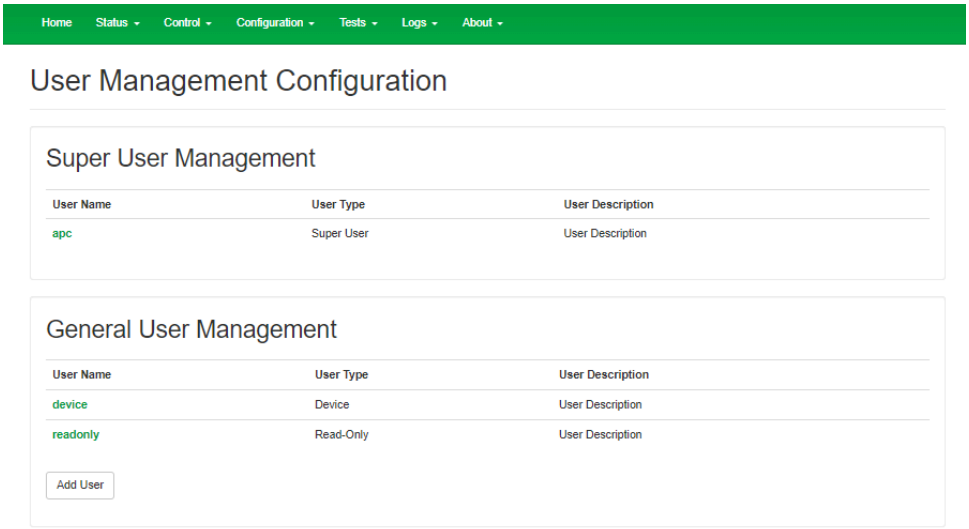
**IPv4 Ping Response:** Select **Enable** to allow the Rack Monitor 250 to respond to network pings. Clear the check box to disable a Rack Monitor 250 response.

If the ping response is enabled and the Rack Monitor 250 does not respond, see “Unable to ping the Rack Monitor 250” under Access Problems, page 165.

This setting does not apply to IPv6.

# Manage Local User Settings

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




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 Monitor 250.
- **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 Monitor 250 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 59).
- **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.<br>**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 Monitor 250 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 Monitor 250.
- **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 Monitor 250 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:**

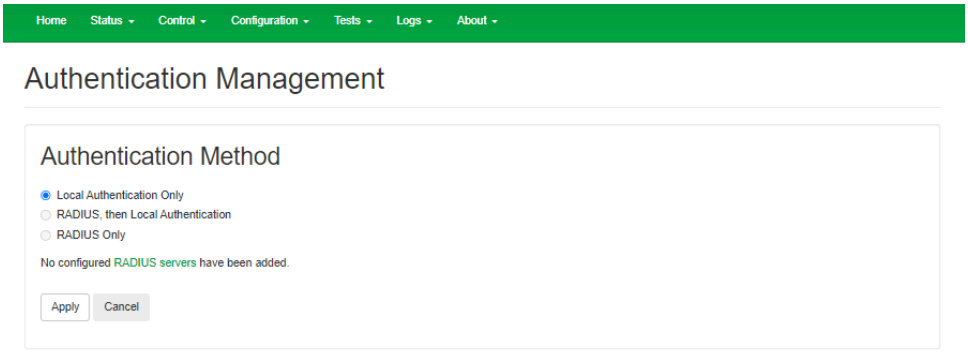
| Option | Description |
|---|---|
| **Event Log Color Coding** | Mark the check box to enable color-coding of alarm text recorded in the Event Log. System event entries and configuration change entries do not change color.<br>**Red:** Alarm Severity = Critical. A critical alarm exists, which requires 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 Monitor 250 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 Monitor 250 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 Monitor 250 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.

# ldap

**Access:** Super User, Administrator, Network-Only User

**Description:** View and configure LDAP settings. You can set up the device to use an LDAP server to authenticate remote users. Two common examples are Microsoft Active Directory and OpenLDAP. Authentication is always performed using a simple bind request over a TLS connection. Ensure that the LDAP server's CA certificate is installed in order for the TLS connection to the LDAP server to complete.

| Option | Argument | Description |
|---|---|---|
| -s | <Search User URI> | An LDAP URI representing the location of a user object to initially bind to. This user object must have permission to search the LDAP database for users. During a user login attempt, the LDAP server in this URI is connected to and a bind to the DN is performed with the password provided in -p (Search User Password). If this bind is successful, the user attempting to login is then searched for.<br><br>This LDAP URI must include a scheme of either "ldap" or “ldaps”. When “ldaps” is used, then the TLS connection is implicit and the TCP connection defaults to using port 636. When “ldap” is used, then the TLS connection is initiated by sending a StartTLS request and the TCP connection defaults to using port 389. Use of “ldaps” is non-standard and discouraged.<br><br>This LDAP URI may include the address of the LDAP server and optionally the port number. The DN of the search user object follows. If the search user DN ends with DC components, then a DNS lookup of the SRV record for the LDAP service at this domain is performed. If the SRV record is found, then it is used instead of the host specified in the URI. If the SRV record is not found, then the host specified in the URI is used. The host component of the URI may be omitted if the SRV record for LDAP is known to exist.<br><br>If the DN is omitted, then the host component must be present, and an anonymous bind is performed.<br><br>Examples:<br>• **ldap://ldap.domain.com/ CN=searchuser,OU=users,DC=domain,DC= com**<br>If DNS is available, a DNS lookup of the SRV record for the LDAP service at domain.com is performed. If it is found, then it is connected to. If it is not found, then "ldap.domain.com" at port 389 is connected to. TLS is then established after sending a StartTLS request, and then a bind to the object “CN=searchuser,OU=users,DC=domain,DC=com” with the password specified in –p (Search User Password) is performed. From here a search for the user logging in is performed.<br>• **ldap:/// CN=searchuser,OU=users,DC=domain,DC= com**<br>If DNS is available, a DNS lookup of the SRV record for the LDAP service at domain.com is performed. If it is found, then it is connected to. If it is not found, then no connection is made because the host component of the URI is omitted and LDAP authentication cannot proceed. If the connection is successful, then StartTLS, bind, and search are performed as described above.<br>• **ldaps://ldap.domain.com**“ldap.domain.com” at port 636 is connected to and a TLS handshake is immediately performed without sending a StartTLS request. If this succeeds, then an anonymous bind is performed. From here a search for the user logging in is performed.<br>• **ldap://ldap.domain.com:42/ CN=searchuser,OU=users,DC=domain,DC= com**<br>This is the same as the first example except that if the SRV record is not found then “ldap.domain. com” at port 42 is connected to.<br>. |
| -p | <Search User Password> | The password to use in the initial bind request to the search user as described above. If left blank, then either an anonymous or unauthenticated bind is performed depending on whether or not a search user DN is provided. |
| -t | <2 — 60> | The timeout in seconds to use when connecting to and communicating with the LDAP server. The initial TCP connection must complete within this amount of time. If it does, then each LDAP response from the server must |

| Option | Argument | Description |
|---|---|---|
| | | be received within this amount of time following each LDAP request. Because a single LDAP authentication can consist of multiple requests (and even to multiple servers if referrals are chased), the overall authentication time may end up being much longer than the timeout value specified here. |
| -u | <Users Base DN> | This is the DN of the base object entry under which all users who login must exist. |
| -g | <Groups Base DN> | This is the DN of the base object entry under which the user groups specified in the following settings must exist. |
| -g | <Groups Base DN> | This is the DN of the base object entry under which the user groups specified in the following settings must exist. |
| -ag | <Admins Group Name> | This is the common name (CN) of the LDAP group to which NMC Administrators are members of. If the user logging in is a member of this group, then the user is granted Administrator access. |
| -dg | <Device Users Group Name> | This is the common name (CN) of the LDAP group to which NMC Device Users are members of. If the user logging in is a member of this group, then the user is granted Device User access. |
| -ng | <Network Users Group Name> | This is the common name (CN) of the LDAP group to which NMC Network Users are members of. If the user logging in is a member of this group, then the user is granted Network User access. |
| -rg | <Read Only Users Group Name> | This is the common name (CN) of the LDAP group to which NMC Read Only Users are members of. If the user logging in is a member of this group, then the user is granted Read Only User access. |
| -ad | <enable \| disable> | If this is enabled, then LDAP directories containing users of the “User” class and groups of the “Group” class following the standard Active Directory schema will be supported. |
| -posix | <enable \| disable> | If this is enabled, then LDAP directories containing users of the “posixAccount” class and groups of the “posixGroup” class following the schema defined in RFC 2307 will be supported. |
| -4519 | <enable \| disable> | If this is enabled, then LDAP directories containing users of the “uidObject” class and groups of either the “groupOfNames” class or the “groupOfUniqueNames” class following the schema defined in RFC 4519 will be supported. |
| -2798 | <enable \| disable> | If this is enabled, then LDAP directories containing users of the “inetOrgPerson” class as defined in RFC 2798 will be supported. |
| -cuser | <enable \| disable> | If this is enabled, then LDAP directories containing users of classes that do not conform to any of the supported classes above can be supported. When this is enabled, the settings –ucn (Custom User Class Name) and –ucua (Custom User Username Attr) must be provided, and – ucga (Custom User Group Number Attr) may optionally be provided. |
| -cgroup | <enable \| disable> | If this is enabled, then LDAP directories containing groups of classes that do not conform to any of the supported classes above can be supported. When this is enabled, the settings –gcn (Custom Group Class Name) and – gcma (Custom Group Member Attr) must be provided, and –gcga (Custom Group Group Number Attr) may optionally be provided. -gcmt (Custom Group Member Type) must also be set correctly. |
| -ucn | <Custom User Class Name> | This is the name of the object class that user entries belong to. It is only used when –cuser (Custom User Class) is enabled. |
| -ucua | <Custom User Username Attr> | This is the name of the attribute that contains a user's username for the object class specified by –ucn (Custom User Class Name). It is only used when –cuser (Custom User Class) is enabled. |

| Option | Argument | Description |
|---|---|---|
| -ucga | <Custom User Group Number Attr> | This is the name of the attribute that contains the group number for a user's primary group for the object class specified by –ucn (Custom User Class Name). This is optional, and only used when –cuser (Custom User Class) is enabled. It is used the same way as the "gidNumber" attribute in the "posixAccount" class. |
| -gcn | <Custom Group Class Name> | This is the name of the object class that group entries belong to. It is only used when –cgroup (Custom Group Class) is enabled. |
| -gcma | <Custom Group Member Attr> | This is the name of the attribute that contains the members of the group for the object class specified by -gcn (Custom Group Class Name). It is only used when - cgroup (Custom Group Class) is enabled. When -gcmt (Custom Group Member Type) is set to DN, then the values in this attribute are DNs. When it is set to username, then the values in this attribute are user names. |
| -gcga | <Custom Group Group Number Attr> | This is the name of the attribute that contains the group number of the group for the object class specified by –gcn (Custom Group Class Name). This is optional, and only used when –cgroup (Custom Group Class) is enabled. It is used the same way as the "gidNumber" attribute in the "posixGroup" class. |
| -gcmt | <DN \| user name> | This specifies how members of the group for the object class specified by –gcn (Custom Group Class Name) are specified. It can be set to either DN or username. |

**Example 1:** To view the existing LDAP settings for the NMC, type:

```
ldap
```

**Example 2:**To configure LDAP to connect to an LDAP server using only an Active Directory schema at ldap.company.com (or to use the ldap SRV record at company.com if available) with a timeout of five seconds, and bind with an initial user with search privileges at DN cn=admin, dc=company, dc=com with password "password", with NMC administrators in the nmc-admins group, NMC read-only users in the nmc-ro-users group, and network only and device only users disabled, type:

```
ldap -s ldap://ldap.company.com/cn=admin,dc=company,dc=com
-p password -t 5 -u ou=users,dc=company,dc=com -g ou=groups,
dc=company,dc=com -ag nmc-admins -rg nmcro-users -dg "" -ng
"" -ad enable -posix disable -4519 disable -2798 disable
-cuser disable -cgroup disable
```

# 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 Monitor 250 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 Monitor 250 supports ports 1812, and 5000 to 32768. |
| **Secret** | The shared secret between the RADIUS server and the Rack Monitor 250. |
| **Reply Timeout** | The time in seconds that the Rack Monitor 250 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 Monitor 250. 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 Monitor 250 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.

# TACACS+ screen (v3.0.x and higher)

**Path: Configuration > Security > User Authentication > TACACS+**

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

- List the TACACS+ servers (a maximum of two) available to the NMC and the time-out period for each.
- Configure the authentication parameters for a new or existing TACACS+ server by clicking on a **TACACS+**link.

| TACACS+ Setting | Description |
|---|---|
| TACACS+ Server | The server name or IP address of the primary or secondary TACACS+ server |
| Port | The port number of the primary or secondary TACACS+ server<br>**NOTE**: TACACS+ servers use port 49 by default to authenticate users. The NMC supports ports 1 to 65535. |
| Secret | The shared secret between the TACACS+ server and the NMC |
| Reply Timeout | The time in seconds that the NMC waits for a response from the TACACS+ server |
| Test Settings | Enter the Administrator user name and password in order to test the TACACS+ server path that you have configured. |
| Skip Test and Apply | Do not test the TACACS+ server path. |

There are two global TACACS+ options applicable to all servers:

| TACACS+ Setting | Description |
|---|---|
| Read-Only User Privilege Level | Specify a value between 0 and 15. If an authorized user's privilege level (priv-lvl authorization argument) is greater than or equal to the specified value, and less than the Administrator Privilege Level, then the user will be granted read-only access.<br>This value must be less than the Administrator Privilege Level. |
| Administra-tor Privilege level | Specify a value between 0 and 15. If an authorized user's privilege level (priv-lvl authorization argument) is greater than or equal to this then the user will be granted administrator access.<br>This value must be greater than the Read-Only User Privilege Level. |

# Configure a TACACS+ Server

**Path: Configuration > Security > User Authentication > TACACS+**

Use this option to do the following:

- List the TACACS+ servers (a maximum of two) available to the Rack Monitor 250 and the Reply Timeout period for each.
- Select a server and configure the parameters for authentication by a new TACACS+ server.
- Select a listed TACACS+ server to display and modify its parameters.

**TACS+ Servers**

You can configure a maximum of two TACACS+ servers to authenticate remote users. The first server in the list is the primary server and will always be contacted first. If the connection times out before the specified timeout value, the secondary server will be contacted. To modify a server, click the link in the list.

**TACS+ Configuration**

Two settings that apply to both servers determine an authorized user's access level:

- **Read-Only User Privilege Level**: Specify a value between 0 and 15. If an authorized user's privilege level (priv-lvl authorization argument) is greater than or equal to this, and less than the Administrator Privilege Level, then the user will be granted read only access. This value must be less than the Administrator Privilege Level.
- **Administrator Privilege Level**: Specify a value between 0 and 15. If an authorized user's privilege level (priv-lvl authorization argument) is greater than or equal to this then the user will be granted administrator access. This value must be greater than the Read-Only User Privilege Level.

**TACACS+ Server Configuration**

Configure the following settings for each TACACS+ server:

- **TACACS+ Server**: The name or IP address of the TACACS+ server.
- **Port**: The port (49 by default) that the TACACS+ server listens on, 1–6553.
- **Secret**: The secret shared by the TACACS+ server and the device.
- **Reply Timeout**: The time in seconds that the device waits for a response from the TACACS+ server.
- **Test Settings**: Enter the username and password of any account on the server to test the settings before applying them.
- **Skip Test and Apply**: Apply the settings without performing a test authentication of the username and password.

# 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 71 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.<br>**subnet:** In the **IP/any** field, you will enter a subnet address.<br>**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:<br>- **any:** The rule applies regardless of the IP address.<br>- **anyipv4:** The rule applies for any IPv4 address.<br>- **anyipv6:** The rule applies for any IPv6 address. |
| **Port** | Specify a port the rule will apply to:<br>- **None:** The rule will apply to any port.<br>- **Common Configured ports:** Select a standard port.<br>- **Other:** Specify a non-standard port number. |
| **Protocol** | Specify which protocol the rule applies to:<br>- **any:** any protocol.<br>- **tcp:** used for more reliable information transfer between applications.<br>- **udp:** alternative to TCP using for faster, lower bandwidth information. transfer. Though it has fewer delays, UDP is less reliable than TCP.<br>- **icmp:** used to report errors for troubleshooting.<br>- **icmpv6:** used to report errors for troubleshooting on applications using IPv6. |
| **Action** | **allow:** Allow the packet that matches this rule.<br>**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.<br>**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).<br>**NOTE:** By default, the supplicant identifier is set to “NMC-Supplicantxx: 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.<br>**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. |

# View Network Status

**Path: Status > Network**

This page allows you to view the following information about your Network Configuration:

| Setting | Description |
|---|---|
| **Current IPv4 Settings** | • **System IP:** The IP address of the unit.<br>• **Subnet Mask:** The IP address of the sub-network.<br>• **Default Gateway:** The IP address of the router used to connect to the network.<br>• **MAC Address:** The MAC address of the unit.<br>• **Mode:** How the IPv4 settings are assigned: **Manual**, **DHCP**, or **BOOTP**.<br>• **DHCP Server:** The IP address of the DHCP server. This is only displayed if Mode is DHCP.<br>• **Lease Acquired:** The date/time that the IP address was accepted from the DHCP server.<br>• **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.<br>• **IP Address:** The IP address of the unit.<br>• **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.<br>• **Active Secondary DNS Server:** The IP address of the secondary DNS server.<br>• **Active Host Name:** The host name of the active DNS server.<br>• **Active Domain Name (IPv4/IPv6):** The IPv4/IPv6 domain name that is currently in use.<br>• **Active Domain Name (IPv6):** The IPv6 domain name that is currently in use. |
| **Port 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). |

# Reset the Network Interface

**Path: Control > Network > Reset/Reboot**

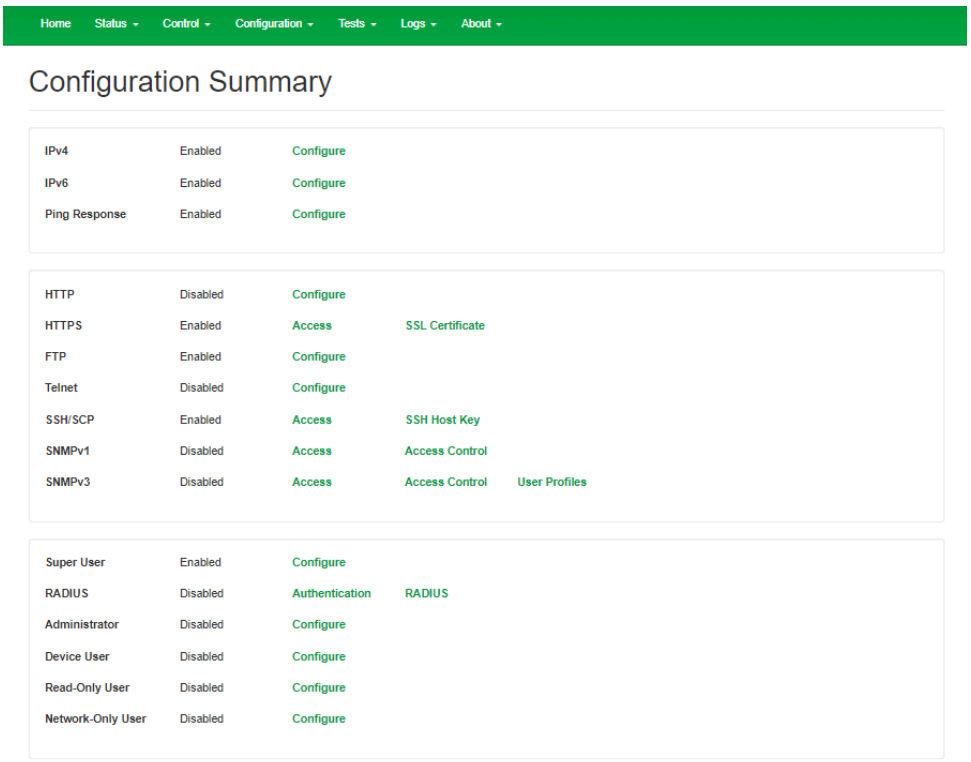
This menu gives you the option to reset and reboot various components of the network interface.

| Setting | Description |
|---|---|
| **Reboot Management Interface** | This option only restarts the Network Management Interface; it does not affect the ON/Off status of the Rack Monitor 250. |
| **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 be required to change your user name and password.<br><br>Select **Exclude TCP/IP** 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 more of the following settings:<br>• **TCP/IP:** Resets only the setting that determines how the Rack Monitor 250 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**.<br>• **Event Configuration:** Resets events to their default configuration. Any specially configured event or group will also revert to the default value.<br>• **Lost Communication Alarms:** Clears lost communication alarms if, for example, you intentionally disconnected a sensor.<br>• **Temperature Rate of Change Alarms:** Clears temperature rate of change alarms to acknowledge a rate of change.<br>• **Module Configuration:** Resets the module to its default configuration.<br>• **User Configurations:** Resets all users to their default configuration.<br>Resetting may take up to a minute. |

# Configure Network Settings

## Protocol Configuration Summary

**Path: Configuration > Network > Summary**




You can use this page to view all protocols enabled or disabled on your Rack Monitor 250. 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 Monitor 250. 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** | A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Rack Monitor 250 requests network assignment from any BOOTP server:<br>• If the Rack Monitor 250 receives a valid response, it starts the network services.<br>• If the Rack Monitor 250 finds a BOOTP server, but a request to that server fails or times out, the Rack Monitor 250 stops requesting network settings until it is restarted.<br>• By default, if previously configured network settings exist, and the Rack Monitor 250 receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible.<br>Click **Next>>** to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail:<br>• **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.<br>• **If retries fail:** Select **Use prior settings** (the default) or **Stop BOOTP** request. |
| **DHCP** | The default setting. At 32-second intervals, the Rack Monitor 250 requests network assignment from any DHCP server.<br>• If the Rack Monitor 250 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.<br>• If the Rack Monitor 250 finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted.1<br>**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 Monitor 250. |
| **NOTE:** The default values for these three settings on configuration pages generally do not need to be changed:<br>• **Vendor Class:** APC<br>• **Client ID:** The MAC address of the Rack Monitor 250, which uniquely identifies it on the local area network (LAN)<br>• **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 Monitor 250 needs to operate on a network, and other information that affects the operation of the Rack Monitor 250.

**Vendor Specific Information (option 43)**

The Rack Monitor 250 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 Monitor 250 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 Monitor 250 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 Monitor 250.
- **Subnet Mask** (option 1): The Subnet Mask value that the Rack Monitor 250 needs to operate on the network.
- **Router**, i.e., Default Gateway (option 3): The default gateway address that the Rack Monitor 250 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 Monitor 250.
- **Renewal Time**, T1 (option 58): The time that the Rack Monitor 250 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 Monitor 250 must wait after an IP address lease is assigned before it can seek to rebind that lease.

## Other options

The Rack Monitor 250 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 Monitor 250 can use.
- **Time Offset** (option 2): The offset of the Rack Monitor 250 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 Monitor 250 can use.
- **Host Name** (option 12): The host name that the Rack Monitor 250 will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the Rack Monitor 250 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 Monitor 250 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 Monitor 250 to send e-mail, you must at least define the IP address of the primary DNS server.
  - The Rack Monitor 250 waits up to 15 seconds for a response from the primary DNS server or secondary DNS server (if specified). If the Rack Monitor 250 does not receive a response within that time, e-mail cannot be sent. Use DNS servers on the same segment as the Rack Monitor 250 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 Monitor 250 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, *`my_server.my_domain`* |
| **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 Monitor 250 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 *Security Handbook*, available at wwww.se.comwww.apc.com. HTTPS is enabled by default. |
| **HTTP Port:** | The TCP/IP port (80 by default) used to communicate by HTTP with the Rack Monitor 250. |
| **HTTPS Port** | The TCP/IP port (443 by default) used to communicate by HTTPS with the Rack Monitor 250.<br><br>**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:<br><br>`http://152.214.12.114:5000`<br><br>`https://152.214.12.114:5000` |
| **Minimum Protocol** | Select minimum HTTPS security protocol from the drop-down list. |
| **Require Authenti-cation 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.<br><br>For more information, see FAQ article FA235784: *Network Management Card 2 (NMC2) "Require Authentication Cookie"*. |
| **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 Monitor 250. |

**NOTE:** To find an FAQ article, go to www.se.com, and select you location. Then select **Support > Documentation & Software Downloads** and enter the article number or title of the FAQ 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** | • **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 Monitor 250.<br>• **Generating:** The Rack Monitor 250 is generating a certificate because no valid certificate was found.<br>• **Loading:** A certificate is being activated on the Rack Monitor 250.<br>• **Valid certificate:** A valid certificate was installed or was generated by the Rack Monitor 250. Select this link to view the contents of the certificate.<br>**NOTE:** If you install an invalid certificate, or if no certificate is loaded when you enable SSL/TLS, the Rack Monitor 250 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. |
| **Certificate Action:** | • **Add or Replace:** Enter or browse to the certificate file created with the Security Wizard. See "Creating and Installing Digital Certificates" in the *Security Handbook*, available at www.apc.com, to choose a method for using digital certificates created by the Security Wizard or generated by the Rack Monitor 250.<br>**NOTE:** All private keys are encrypted by the firmware before storage on the device. The encryption key is unique for each device.<br>• **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 Monitor 250. 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 Monitor 250. 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 Monitor 250 is creating a host key because no valid host key was found.
- **Loading:** A host key is being activated on the Rack Monitor 250.
- **Valid:** One of the following valid host keys is in the /**ssh** directory (the required location on the Rack Monitor 250):
  - A 1024-bit or 2048-bit host key created by the Security Wizard
  - A 2048-bit RSA host key generated by the Rack Monitor 250

**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 Monitor 250 takes up to one minute to create a host key, and the SSH server is not accessible during that time.

  **NOTE:** All private keys are encrypted by the firmware before storage on the device. The encryption key is unique for each device.
- **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 Monitor 250 on the public network, you must have the same version of SNMP (1 or 3) enabled on both the Rack Monitor 250 interface and the Data Center Expert interface. Read access will allow the Data Center Expert to receive traps from the Rack Monitor 250, 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.

## 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:<br>- 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment.<br>- 149.225.**255.255**: Access only by an NMS on the 149.225 segment.<br>- 149.**255.255.255**: Access only by an NMS on the 149 segment.<br>- 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.<br>- **Read:** GETs only, at any time<br>- **Write:** GETs at any time, and SETs when no user is logged onto the Web UI or CLI.<br>- **Write+:** GETs and SETs at any time.<br>- **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 (`hidden` `crypt.phrase`, 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:<br>- 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment.<br>- 149.225.**255.255**: Access only by an NMS on the 149.225 segment.<br>- 149.**255.255.255**: Access only by an NMS on the 149 segment.<br>- 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 Monitor 250 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`.

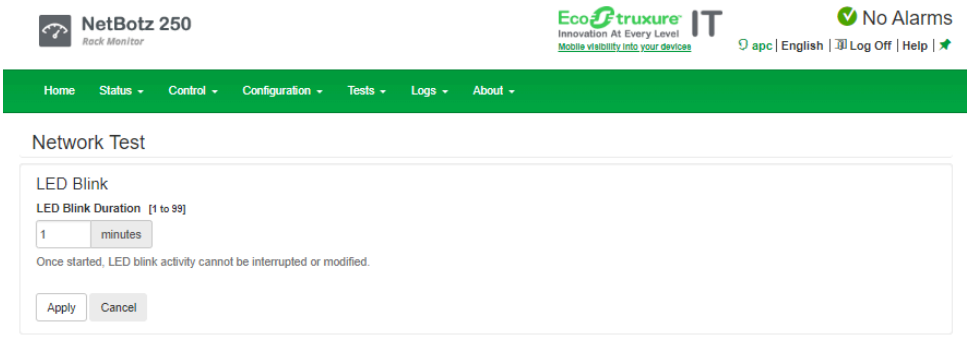
**NOTE:** FTP transfers files without encryption. For higher security, transfer files with Secure CoPy (SCP). Secure SHell (*SSH*) is enabled by default, and enables SCP automatically. However, SCP will not allow a file transfer until the Super User default password (**apc**) is changed. At any time that you want a Rack Monitor 250 to be accessible for management by Data Center Expert, FTP server access must be enabled in the Rack Monitor 250 interface.

**NOTE:** You can use FTP or SCP to configure and update the Rack Monitor 250 with Data Center Expert or EcoStruxure IT as long as the same protocol is enabled on both the Rack Monitor 250 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.

# Set the LED Light to Blink

**Path: Tests > Network > LED Blink**




If you are having trouble finding your Rack Monitor 250, 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.

# Factory Information

**Path: About > Network**

The hardware and software information is useful to APC Customer Support for troubleshooting problems with the appliance. The serial number and MAC address are also available on the appliance.

**Management Uptime** is the length of time the network management interface has been running continuously.

# 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.

# Using the 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 Monitor 250.

**Port:** The port that the Rack Monitor 250 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 Monitor 250 (User, by default).

> **NOTE: User** best defines the Syslog messages sent by the Rack Monitor 250. 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 Monitor 250 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 Monitor 250.
- The Header: a time stamp and the IP address of the Rack Monitor 250.
- 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.`

# View and Configure the Event Log

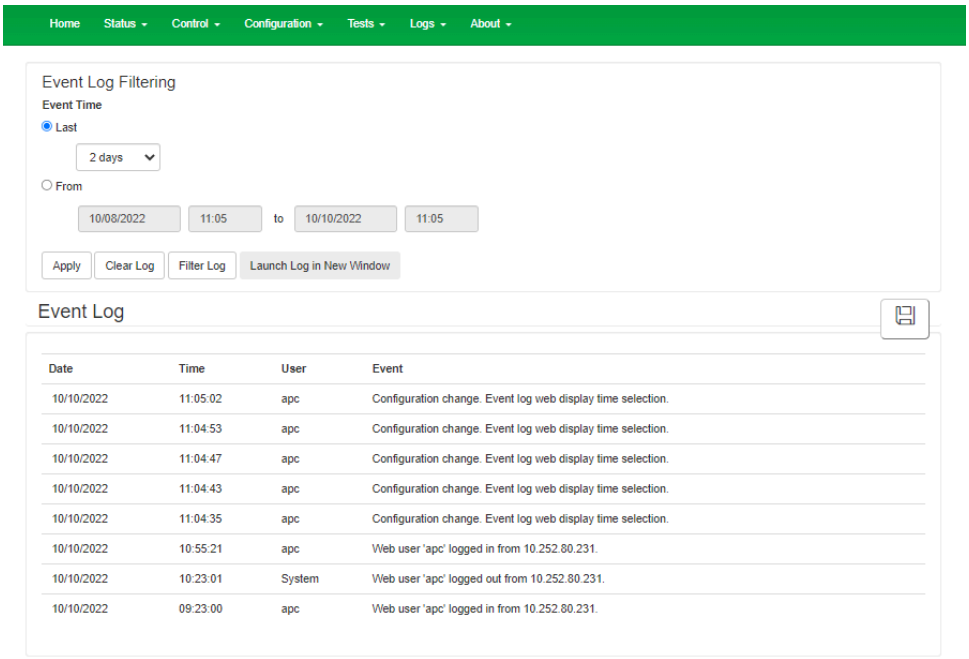
By default, the Event Log displays all events recorded during the last two days, starting with the latest events.

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**




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 92.

**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 Monitor 250 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 Monitor 250 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 .

# 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.

# View and Configure the Data Log

Use the Data Log to display measurements about the Rack Monitor 250, the power input to the Rack Monitor 250, and the ambient temperature of the Rack Monitor 250.

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**.

## 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 Monitor 250 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 *mmddyyyy_ <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 (25-30,000).

**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 70.

# Use FTP or SCP to Retrieve Log Files

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

- The file reports all 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 Monitor 250
  - The unique **Event Code** for each recorded event (*event.txt* file only)

    **NOTE:** The Rack Monitor 250 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 *Network Management Card 3 Security Handbook*(SPD_CCON-BDYD7K_EN) on www.se.com/ww/en/download for information on available security protocols and methods to set up the type of security you need. You must select a location to view and download user manuals from the website.

## 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 Monitor 250, 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 **Configureation > 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.

# Command Line Interface

You can use the Command Line Interface (CLI) to configure, manage, and monitor the status of the Rack Monitor 250. Additionally, the CLI enables you to create scripts for automated operation. You can configure all parameters of a Rack Monitor 250 (including those for which there are not specific CLI commands) by using the CLI to transfer an INI file to the Rack Monitor 250. 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 Monitor 250.

## Local Access to the CLI

For local access, use a computer that connects to the Rack Monitor 250 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 Monitor 250 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 Monitor 250.
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 21 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 Monitor 250 (for example, `telnet 139.225.6.133`, when the Rack Monitor 250 uses the default Telnet port of 23), and press ENTER.

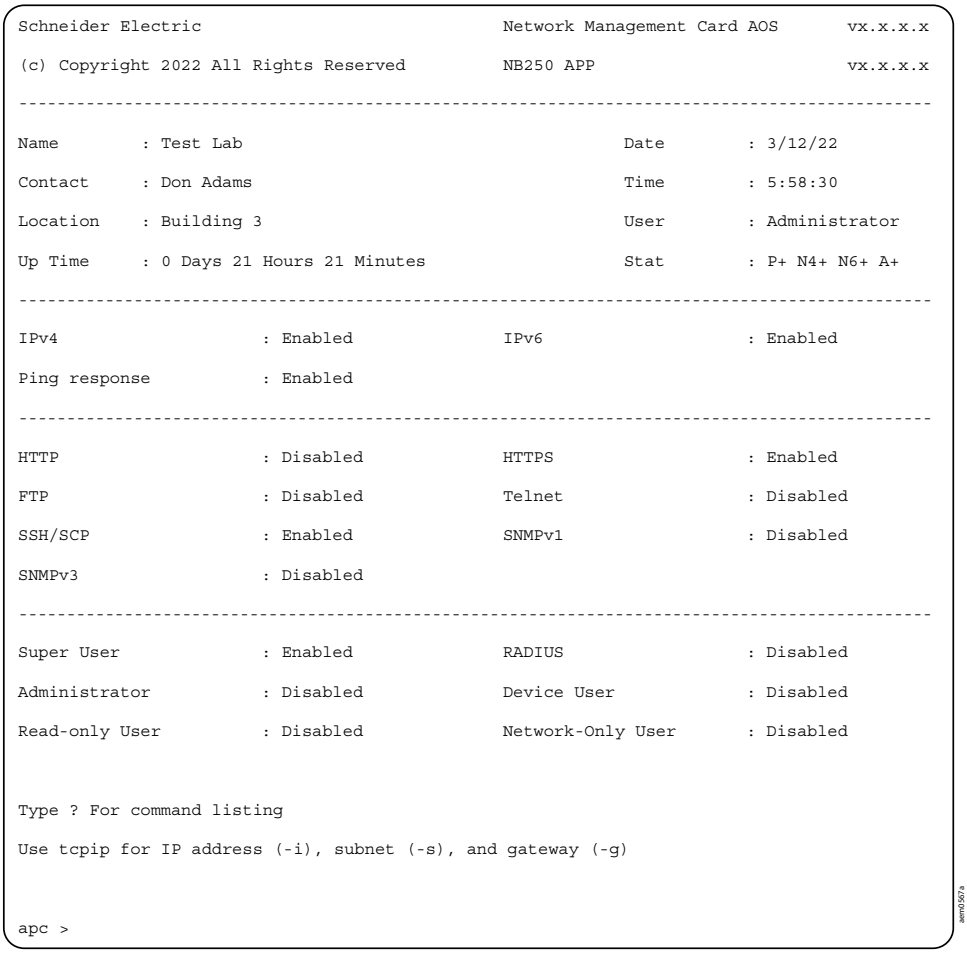
   If the Rack Monitor 250 uses a non-default port number (from 5000 to 32768), you must include a colon or a space, depending on your Telnet client, between the IP address (or DNS name) and the port number. (These are commands for general use; some clients do not allow you to specify the port as an argument 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 30.

## 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 Monitor 250.




- 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 NB250).

  Network Management Card AOS vx.x.x.x

  NB250 APP vx.x.x.x

- Three fields identify the system name, contact person, and location of the Rack Monitor 250.

  Name Test Lab

  Contact Don Adams

  Location : Building 3

- An Up Time field reports how long the Rack Monitor 250 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:                           3/12/22
Time:                           5:58:30
```

- 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 Monitor 250 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 Monitor 250 failed to connect to the network. |
| `N!` | `N6!` | `N4! N6!` | Another device is using the Rack Monitor 250 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 Monitor 250. 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.<br>For example: `-dp <device password>` |
| [ ] | 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:**

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 | Notes |
|---|---|---|
| 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 | Either the data is not available, or the provided data cannot be read. |
| E107 | Serial Communications Lost | — |
| E108 | EAPoL disabled due to invalid/encrypted certificate | — |
| E200 | The provided arguments were invalid. To view 'command' help, type 'command ?'. | — |
| E201 | The provided value does not match expectations for length or range. | Numeric values cannot be written to the device if they are outside of a specific range, and strings cannot be written if they are too long or too short. |
| E202 | The current user does not have 'write' privileges. | — |
| E203 | The target item is not configurable. | — |
| E204 | The requested operation cannot be completed with the device(s) specified. | — |
| E205 | System error: The requested operation could not be completed. | A system error occurred while acting on user input. |
| E206 | System error: Buffer allocation failed. | A system error occurred before the user's input could be interpreted. |

# 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

## ?

**Access:** Super User, Administrator, Device User, Read-Only User, Network-Only User

**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.

| Argument | Description |
|---|---|
| <command> | View help text for a specific 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      ldap         ledblink
logzip       netstat    ntp          ping         portspeed    prompt
pwd          quit       radius       reboot       resetToDef   session
smtp         snmp       snmptrap     snmpv3       ssh          ssl
system       tacacs+    tcpip        tcpip6       user         userauth
userdflt     web        whoami       wifi         xferINI      xferstatus
```

**Error Message:** E000, E102

# about

**Access:** Super User, Administrator, Device User, Read-Only User, Network-Only User

**Description:** View hardware and firmware information. This information is useful in troubleshooting and enables you to determine if updated firmware is available at the website.

**Parameters:** None

**Example:**

```
apc> about
     E000: Success
     Hardware
     Factory
     --------------
     --
     Model Number:      nnnnnnnnnn
     Serial Number:     nnnnnnnnnn
     Hardware           nnnn
     Revision:
     Manufacture        mm/dd/yyyy
     Date:
     MAC Address:       00 05 A2 18 00 01
     Management         0 Days 1 Hour 42 Minutes
     Uptime:
```

**Error Message:** `E000`

# alarmcount

**Access:** Super User, Administrator, Device User, Read-Only User, Network-Only User

**Description:** Displays alarms present in the system.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-p` | `all` | View the number of active alarms reported by the Rack Monitor 250. 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. |
| | `informational` | View the number of active informational alarms. |

**Example:** To view all active warning alarms, type

```
apc> alarmcount -p warning
E000: Success
WarningAlarmCount: 0
```

**Error Message:** `E000, E102`

# boot

**Access:** Super User, Administrator, Network-Only User

**Description:** Define how the Rack Monitor 250 will obtain its network settings, including the IP address, subnet mask, and default gateway. Then configure the BOOTP or DHCP server settings.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-b <boot mode>` | `dhcp \| bootp \| manual` | Define how the TCP/IP settings will be configured when the Rack Monitor 250 turns on, resets, or restarts. |
| `-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. |
| The default values for these three settings generally do not need to be changed. | | |
| `-v` | `[<vendor class>]` | APC. |
| `-i` | `[<client id>]` | The MAC address of the Rack Monitor 250, which uniquely identifies it on the network. |
| `-u` | `[<user class>]` | The name of the application firmware module. |

**Example:** To use a DHCP server to obtain network settings:

1. Type `boot -b dhcp`
2. Enable the requirement that the DHCP server provide the APC cookie:

```
apc> boot -c enable
E000: Success
```

**Error Message:** `E000, E102`

# bye

**Access:** Super User, Administrator, Device User , Read-Only User, Network-only User

**Description:** Exit the CLI session. This works the same as the `exit` or `quit` commands.

**Parameters:** None.

**Example:**

```
apc> bye
Connection Closed - Bye
```

**Error Message:** None.

# cd

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

**Description:** Navigate to a folder in the directory structure of the Rack Monitor 250. The working directory is set back to the root directory '/' when the you log out of the CLI.

**Parameters:** `<directory name>`

**Example 1:** To change to the ssh folder and confirm that an SSH security certificate was uploaded to the Rack Monitor 250,

1. Type `cd ssh` and press ENTER.
2. Type `dir` and press ENTER to list the files stored in the SSH folder.

**Example 2:** To return to the previous directory folder, type `cd . .`

**Error Message:** `E000, E102`

# clrrst

**Access:** Super User, Administrator

**Description:** Clear the network interface reset reason. See lastrst, page 118 for more information on the 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 Monitor 250 (23 by default). |
| `-ps` | `<SSH port n>` | Define the SSH port used to communicate with the Rack Monitor 250 (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 enable`

**Example 2:** To change the Telnet port to 5000, type
`console -pt 5000`

**Error Message:** `E000, E102`

# date

**Access:** Super User, Administrator

**Definition:** Configure the date and time used by the Rack Monitor 250.

**NOTE:** To configure an NTP server to define the date and time for the Rack Monitor 250, see ntp, page 123.

**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 October 30, 2009, using the format configured in the preceding example, type

```
date -d "2009-10-30"
```

**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. (To delete the eveng log, see eventlog, page 114.)

**Parameters:**

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

**Example:** To delete a file,

1. Navigate to the folder that contains the file. For example, to navigate to the logs folder, type
   `cd logs`
2. To view the files in the logs folder, type
   `dir`
3. To delete a file, type
   `delete <file name>`

**Error Messages:** `E000, E102`

# dir

**Access:** Super User, Administrator, Device User, Read-Only User, Network-Only User

**Description:** View the files and folders stored on the Rack Monitor 250.

**Parameters:** None

**Example:**

```
apc> dir
E000: Success
1024 Jan 2 4:34 apc_hw21_aos_2.5.0.8.bin
6249332 Jan 2 4:34 apc_hw21_nb250_1.1.0.15.bin
45000 Sep 30 1996 config.ini
          0   Apr   23  18:53   db/
          0   Apr   23  18:53   ssl/
          0   Apr   23  18:53   ssh/
          0   Apr   23  18:53   logs/
          0   Apr   23  18:53   sec/
          0   Apr   23  18:53   fwl/
          0   Apr   23  18:53   email/
          0   Apr   23  18:53   eapol/
          0   Apr   23  18:53   tmp/
          0   Apr   23  18:53   upsfw/
```

**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. When this setting is enabled, configuration data from other sources (typically DHCP) takes precedence over the manual configuration set here. |
| -y | <enable \| disable> | System-hostname sync |
| -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. |

**Example:**

```
apc > dns -OM
E000: Success
Override Manual DNS Settings: enabled
```

**Error Message:** E000, E102

# eapol

**Access:** Super User, Administrator

**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
```

**Example 2:** To enable EAPoL:

```
apc>eapol -S enable
E000: Success
Reboot required for change to take effect.
```

# email

**Access:** Super User, Administrator

**Description:** Configure parameters for email, which the Rack Monitor 250 uses to send event notifications.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-g[n]` | `<enable \| disable>` | Enables (default) or disables sending email to the recipient. |
| `-t[n]` | `<To Address>` | The user and domain names of the recipient. To use email for paging, use the email address for the recipient's pager gateway account (for example, myacct100@skytel.com). The pager gateway will generate the page. |
| `-o[n]` | `<long \| short> (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. |
| `-l[n]` | `<Language Code>` | The language which the email notification will be sent in. Only English is available at this time. |
| `-r [n]` | `<Local \| recipient \| custom> (Route)` | Set the SMTP Server options:<br><br>`Local` (recommended): Choose this option if your SMTP server is located on your internal network, or is set up for your e-mail domain. Choose this setting to limit delays and network outages. If you choose this setting, you must also enable forwarding at the SMTP server of the device, and set up a special external e-mail account to receive the forwarded e-mail. **NOTE:** Check with your SMTP server administrator before making these changes.<br><br>`Recipient`: This setting sends email directly to the recipient's SMTP server, which is determined by an MX record lookup of the domain of the To: Address. The device tries only once to send the e-mail. A network outage or a busy remote SMTP server can cause a time-out and cause the e-mail to be lost. This setting requires no additional administrative tasks on the SMTP server. **NOTE:** When using this setting, the "From Address" will match the "To Address", authentication and encryption (TLS) will be disabled, and port 25 will be used.<br><br>`Custom`: This setting allows each email recipient to have its own server settings. These settings are independent of the settings given by the `smtp` command. |
| `Custom Route Option` | | |
| `-f[n]` | `<From Address>` | The contents of the From field in email messages sent by the Rack Monitor 250 in the format *user@ [IP_address]* if an IP address is specified as Local SMTP Server), or in the format *user@domain* if DNS is configured and the DNS name is specified as Local SMTP Server in the email messages.<br><br>The local SMTP server may require that you use a valid user account on the server for this setting. See the server documentation. |
| `-s{n}` | `<SMTP Server>` | The IPv4/ IPv6 address or DNS name of the local SMTP server. This definition is required only when the `-r` option is set to `Local`. |
| `-p[n]` | `<Port>` | The SMTP port number, with a default of 25. Common ports are 25 for unencrypted e-mail, and 465 and 587 for SSL/TLS encrypted e-mail. You can change the port setting to any port from 1 to 65535. |
| `-a[n]` | `<enable \| disable> (Authentication)` | Enable this if the SMTP server requires authentication. |
| `-u[n]` | `<User Name>` | If the SMTP server requires authentication, type the user name and password here. This performs a simple authentication, not SSL/TLS. |
| `-w[n]` | `<Password>` | |
| `-e[n]` | `<none \| ifsupported \| always \| implicit>` | Specify when encryption is used.<br><br>`none`: The SMTP server does not require or support encryption.<br><br>`ifsupported`: 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. This is typically used with port 25.<br><br>`always`: The SMTP server requires the STARTTLS command to be sent on connection to the server. This is typically used with port 587.<br><br>`implicit`: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server. This is typically used with port 465. |

| Option | Argument | Description |
|---|---|---|
| -c[n] | <enable \| disable > | Require CA Root Certificate: This should 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 CA certificate for the SMTP server must be installed to the Rack Monitor 250's certificate store using the certificate loader in order for a TLS connection with the SMTP server to succeed. |
| -i[n] | <Certificate File Name> | This field is dependent on the root CA certificates installed on the Rack PDU and whether or not a root CA certificate is required. |
| n = Email Recipient Number (1,2,3 or 4) | | |

**Example:** To enable email to be sent to email recipient 1 with email address recipient1@apc.com, using the local SMTP server:

```
apc> email -g1 enable -r1 local -t1 recipient1@apc.com
E000: Success
```

**Error Message:** E000, E102

# eventlog

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

**Description:** View the date and time you retrieved the Event Log, the status of the Rack Monitor 250, and the status of sensors connected to the Rack Monitor 250. 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: 2/9/2024 Time: 13:22:26

  ----------------------------------

  Metered NetBotz 250: Communication Established

  Date         Time         User       Event

  ------------------------------------------------------------------

  2/9/2024     13:17:22     System     Set Time.

  2/9/2024     13:16:57     System     Configuration change. Date format
                                       preference.
  2/9/2024     13:16:49     System     Set Date.

  2/9/2024     13:16:35     System     Configuration change. Date format
                                       preference.
  2/9/2024     13:16:08     System     Set Date.

  2/9/2024     13:15:30     System     Set Time.

  2/9/2024     13:15:00     System     Set Time.

  2/9/2024     13:13:58     System     Set Date.

  2/9/2024     13:12:22     System     Set Date.

  2/9/2024     13:12:08     System     Set Date.

  2/9/2024     13:11:41     System     Set Date.

<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

**Error Message:** E000, E100

# exit

**Access:** Super User, Administrator, Device User , Read-Only User, Network-only User

**Description:** Exit the CLI session. This works the same as the `bye` or `quit` commands.

**Parameters:** None.

**Example:**

```
apc> exit
Bye
```

**Error Message:** None.

# firewall

**Access:** Super User, Administrator

**Description:** Enable, disable, or configure the internal Rack Monitor 250 firewall feature.

**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` | | Shows active file errors. |
| `-te` | | Shows test file errors. |
| `-c` | | Cancel a firewall test. |
| `-r` | | Shows active firewall rules. |
| `-l` | | Shows firewall activity log. |
| `-Y` | | Skip firewall test prompt. |

**Example:** To enable the firewall policy file *example.fwl*, type

```
apc> firewall -f example.fwl
E000: Success
```

**Error Message:** `E000, E102`

# format

**Access:** Super User, Administrator

**Description:** Reformat the file system of the Rack Monitor 250 and erase all security certificates, encryption keys, configuration settings, and the event and data logs. Be careful with this command.

**NOTE:** You must confirm by entering “YES” when prompted.

**NOTE:** To reset the Rack Monitor 250 to its default configuration, use the `resetToDef` command instead.

**Parameters:**

| Option | Definition |
|---|---|
| -f | This will delete all configuration data, event and data logs, certificates and keys. Network settings will NOT be preserved. |
| -p | This will delete all configuration data, event and data logs, certificates and keys. Network settings WILL be preserved. |

**Example:**

```
apc> format -p

Format FLASH file system

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

All network configuration settings WILL be preserved.

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

**Error Message:** None

# ftp

**Access:** Super User, Administrator

**Description:** Enable or disable access to the FTP server. Optionally, change the port setting to the number of any unused port from 5001 to 32768 for added security.

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

**NOTE:** FTP is disabled by default, and Secure CoPy (SCP) is automatically enabled when the Super User password is set via SSH.

**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 Monitor 250 (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
```

**Error Message:** `E000, E102`

# help

**Access:** Super User, Administrator, Device User, Read-Only User, Network-Only User

**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 `help`.

**Parameters:** `[<command>]`

**Example 1:** To view a list of commands available to someone logged on as a Device User, log on to the CLI as the Device User, then type

```
help
```

**Example 2:** To view a list of options that are accepted by the `alarmcount` command, type

```
apc> alarmcount help
Usage: alarmcount -- Display Alarms
         alarmcount [-p <all | warning | critical |
         informational>]
```

# 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 last network interface reset reason. Use the output of this command to troubleshoot network interface issues with the guidance of technical support.

| Option | Description |
|---|---|
| `02 NMI Reset` | The network interface was reset via the Reset button on the Rack Monitor 250 front display. |
| `09 Coldstart Reset` | The network interface was reset by removing power from the hardware. |
| `12 WDT Reset` | The network interface was reset via a firmware command. |

**Parameters:** None

**Example:**

```
apc> lastrst
09 Coldstart Reset
E000: Success
```

**Error Message:** `E000, E102`

## ldap

**Access:** Super User, Administrator, Network-Only User

**Description:** View and configure LDAP settings. You can set up the device to use an LDAP server to authenticate remote users. Two common examples are Microsoft Active Directory and OpenLDAP. Authentication is always performed using a simple bind request over a TLS connection. Ensure that the LDAP server's CA certificate is installed in order for the TLS connection to the LDAP server to complete.

| Option | Argument | Description |
|---|---|---|
| -s | <Search User URI> | An LDAP URI representing the location of a user object to initially bind to. This user object must have permission to search the LDAP database for users. During a user login attempt, the LDAP server in this URI is connected to and a bind to the DN is performed with the password provided in -p (Search User Password). If this bind is successful, the user attempting to login is then searched for.<br><br>This LDAP URI must include a scheme of either "ldap" or “ldaps”. When “ldaps” is used, then the TLS connection is implicit and the TCP connection defaults to using port 636. When “ldap” is used, then the TLS connection is initiated by sending a StartTLS request and the TCP connection defaults to using port 389. Use of “ldaps” is non-standard and discouraged.<br><br>This LDAP URI may include the address of the LDAP server and optionally the port number. The DN of the search user object follows. If the search user DN ends with DC components, then a DNS lookup of the SRV record for the LDAP service at this domain is performed. If the SRV record is found, then it is used instead of the host specified in the URI. If the SRV record is not found, then the host specified in the URI is used. The host component of the URI may be omitted if the SRV record for LDAP is known to exist.<br><br>If the DN is omitted, then the host component must be present, and an anonymous bind is performed.<br><br>Examples:<br>• **ldap://ldap.domain.com/ CN=searchuser,OU=users,DC=domain,DC= com**<br>If DNS is available, a DNS lookup of the SRV record for the LDAP service at domain.com is performed. If it is found, then it is connected to. If it is not found, then "ldap.domain.com" at port 389 is connected to. TLS is then established after sending a StartTLS request, and then a bind to the object “CN=searchuser,OU=users,DC=domain,DC=com” with the password specified in –p (Search User Password) is performed. From here a search for the user logging in is performed.<br>• **ldap:/// CN=searchuser,OU=users,DC=domain,DC= com**<br>If DNS is available, a DNS lookup of the SRV record for the LDAP service at domain.com is performed. If it is found, then it is connected to. If it is not found, then no connection is made because the host component of the URI is omitted and LDAP authentication cannot proceed. If the connection is successful, then StartTLS, bind, and search are performed as described above.<br>• **ldaps://ldap.domain.com**“ldap.domain.com” at port 636 is connected to and a TLS handshake is immediately performed without sending a StartTLS request. If this succeeds, then an anonymous bind is performed. From here a search for the user logging in is performed.<br>• **ldap://ldap.domain.com:42/ CN=searchuser,OU=users,DC=domain,DC= com**<br>This is the same as the first example except that if the SRV record is not found then “ldap.domain. com” at port 42 is connected to.<br>. |
| -p | <Search User Password> | The password to use in the initial bind request to the search user as described above. If left blank, then either an anonymous or unauthenticated bind is performed depending on whether or not a search user DN is provided. |
| -t | <2 — 60> | The timeout in seconds to use when connecting to and communicating with the LDAP server. The initial TCP connection must complete within this amount of time. If it does, then each LDAP response from the server must |

| Option | Argument | Description |
|---|---|---|
| | | be received within this amount of time following each LDAP request. Because a single LDAP authentication can consist of multiple requests (and even to multiple servers if referrals are chased), the overall authentication time may end up being much longer than the timeout value specified here. |
| -u | <Users Base DN> | This is the DN of the base object entry under which all users who login must exist. |
| -g | <Groups Base DN> | This is the DN of the base object entry under which the user groups specified in the following settings must exist. |
| -g | <Groups Base DN> | This is the DN of the base object entry under which the user groups specified in the following settings must exist. |
| -ag | <Admins Group Name> | This is the common name (CN) of the LDAP group to which NMC Administrators are members of. If the user logging in is a member of this group, then the user is granted Administrator access. |
| -dg | <Device Users Group Name> | This is the common name (CN) of the LDAP group to which NMC Device Users are members of. If the user logging in is a member of this group, then the user is granted Device User access. |
| -ng | <Network Users Group Name> | This is the common name (CN) of the LDAP group to which NMC Network Users are members of. If the user logging in is a member of this group, then the user is granted Network User access. |
| -rg | <Read Only Users Group Name> | This is the common name (CN) of the LDAP group to which NMC Read Only Users are members of. If the user logging in is a member of this group, then the user is granted Read Only User access. |
| -ad | <enable \| disable> | If this is enabled, then LDAP directories containing users of the “User” class and groups of the “Group” class following the standard Active Directory schema will be supported. |
| -posix | <enable \| disable> | If this is enabled, then LDAP directories containing users of the “posixAccount” class and groups of the “posixGroup” class following the schema defined in RFC 2307 will be supported. |
| -4519 | <enable \| disable> | If this is enabled, then LDAP directories containing users of the “uidObject” class and groups of either the “groupOfNames” class or the “groupOfUniqueNames” class following the schema defined in RFC 4519 will be supported. |
| -2798 | <enable \| disable> | If this is enabled, then LDAP directories containing users of the “inetOrgPerson” class as defined in RFC 2798 will be supported. |
| -cuser | <enable \| disable> | If this is enabled, then LDAP directories containing users of classes that do not conform to any of the supported classes above can be supported. When this is enabled, the settings –ucn (Custom User Class Name) and –ucua (Custom User Username Attr) must be provided, and – ucga (Custom User Group Number Attr) may optionally be provided. |
| -cgroup | <enable \| disable> | If this is enabled, then LDAP directories containing groups of classes that do not conform to any of the supported classes above can be supported. When this is enabled, the settings –gcn (Custom Group Class Name) and – gcma (Custom Group Member Attr) must be provided, and –gcga (Custom Group Group Number Attr) may optionally be provided. -gcmt (Custom Group Member Type) must also be set correctly. |
| -ucn | <Custom User Class Name> | This is the name of the object class that user entries belong to. It is only used when –cuser (Custom User Class) is enabled. |
| -ucua | <Custom User Username Attr> | This is the name of the attribute that contains a user's username for the object class specified by –ucn (Custom User Class Name). It is only used when –cuser (Custom User Class) is enabled. |

| Option | Argument | Description |
|---|---|---|
| -ucga | <Custom User Group Number Attr> | This is the name of the attribute that contains the group number for a user's primary group for the object class specified by –ucn (Custom User Class Name). This is optional, and only used when –cuser (Custom User Class) is enabled. It is used the same way as the “gidNumber” attribute in the “posixAccount” class. |
| -gcn | <Custom Group Class Name> | This is the name of the object class that group entries belong to. It is only used when –cgroup (Custom Group Class) is enabled. |
| -gcma | <Custom Group Member Attr> | This is the name of the attribute that contains the members of the group for the object class specified by -gcn (Custom Group Class Name). It is only used when - cgroup (Custom Group Class) is enabled. When -gcmt (Custom Group Member Type) is set to DN, then the values in this attribute are DNs. When it is set to username, then the values in this attribute are user names. |
| -gcga | <Custom Group Group Number Attr> | This is the name of the attribute that contains the group number of the group for the object class specified by –gcn (Custom Group Class Name). This is optional, and only used when –cgroup (Custom Group Class) is enabled. It is used the same way as the “gidNumber” attribute in the “posixGroup” class. |
| -gcmt | <DN \| user name> | This specifies how members of the group for the object class specified by –gcn (Custom Group Class Name) are specified. It can be set to either DN or username. |

**Example 1:** To view the existing LDAP settings for the NMC, type:

```
ldap
```

**Example 2:**To configure LDAP to connect to an LDAP server using only an Active Directory schema at ldap.company.com (or to use the ldap SRV record at company.com if available) with a timeout of five seconds, and bind with an initial user with search privileges at DN cn=admin, dc=company, dc=com with password “password”, with NMC administrators in the nmc-admins group, NMC read-only users in the nmc-ro-users group, and network only and device only users disabled, type:

```
ldap -s ldap://ldap.company.com/cn=admin,dc=company,dc=com
-p password -t 5 -u ou=users,dc=company,dc=com -g ou=groups,
dc=company,dc=com -ag nmc-admins -rg nmcro-users -dg "" -ng
"" -ad enable -posix disable -4519 disable -2798 disable
-cuser disable -cgroup disable
```

# ledblink

**Access:** Super User, Administrator

**Description:** Sets the status LED to blink for the specified amount of time. Use this command to help visually locate the .

**Parameters:**

| Argument | Definition |
|---|---|
| `<time>` | Number of minutes to blink the LED. |

**Example:**

```
apc> ledbllink 1
E000: Success
```

**Error Message:** `E000, E102`

# logzip

**Access:** Super User, Administrator

**Description:** Creates a single, compressed archive of the log files available from the NMC and Rack Monitor 250. These files can be used by technical support to troubleshoot issues.

**Parameters:**

| Option | Argument | Definition |
|---|---|---|
| `-m` | `<email recipient> (1-4)` | The identifying number (1–4) of the email recipient to which the zip file will be sent. Enter the number of one of the four possible email recipients configured. |

**Example:**

```
apc> logzip -m 1
Generating files
/dbg/debug_ZA1023006009.tar
Emailing log files to email recipient - 1
E000: Success
```

**Error Message:** `E000, E102`

# netstat

**Access:** Super User, Administrator

**Description:** View the status of the network and all active IPv4 and IPv6 addresses.

**Parameters:** None

**Example:**

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

**Error Message:** `E000, E10`

# ntp

**Access:** Super User, Administrator

**Description:** View and configure the Network Time Protocol parameters.

**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. |
| `-e` | `enable \| disable` | Enable or disable the use of NTP. |
| `-u` | `<update now>` | Immediately update theRack Monitor 250 time from the NTP 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, Network-Only User

**Description:** Determine whether the device with the IP address or DNS name you specify is connected to the network. Four inquiries are sent to the address.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| n/a | `<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. |
| –t | | Ping until stopped. |

**Example:** To determine whether a device with an IP address of 192.168.1.50 is connected to the network, type

```
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, Network-Only User

**Description:** Define the communication speed of the Ethernet port.

**NOTE:** The Port Speed setting can be changed to 1000 Mbps. However, this change can only be made via the Web UI.

**Parameters:**

| Option | Arguments | Description |
|---|---|---|
| `-s` | `auto \| 10H \| 10F \| 100H \| 100F` | `auto` enables the Ethernet devices to negotiate to transmit at the highest possible speed.<br>`H` = Half Duplex (communication in only one direction at a time)<br>`F` = Full Duplex (communication in both directions simultaneously)<br>`10` = 10 Megabits<br>`100` = 100 Megabits |

**Example:** To configure the TCP/IP port to communicate using 100 Mbps with half-duplex communication, type

```
apc> portspeed -s 100H
E000: Success
Reboot required for change to take effect.
```

**Error Message:** `E000, E102`

# prompt

**Access:** Super User, Administrator, Device User, Network-Only User

**Description:** Configure the command line interface prompt to include or exclude the account type of the currently logged-in user. Any user can change this setting; all user accounts will be updated to use the new setting.

**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: `apc>` |

**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 User, Network-Only User

**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

**Access:** Super User, Administrator, Device User ,, Read-Only User, Network-only User

**Description:** Exit the CLI session. This works the same as the `exit` or `bye` commands.

**Parameters:** None.

**Example:**

```
apc> quit
Bye
```

**Error Message:** None.

# radius

**Access:** Super User, Administrator, Network-Only User

**Description:** View the existing RADIUS settings and configure basic authentication parameters for up to two RADIUS servers. Additional authentication parameters are available in the Web UI.

For detailed information about configuring your RADIUS server, see the Network Management Card 3 Security Handbook.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-a` | `<local \| radiusLocal \| radius>` | Configure RADIUS authentication:<br><br>`local` = RADIUS is disabled. Local authentication is enabled.<br><br>`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.<br><br>`radius` = RADIUS is enabled. Local authentication is disabled. |
| `-p1`<br>`-p2` | `<server IP>` | The server name or IP address of the primary or secondary RADIUS server. |
| `-o1`<br>`-o2` | `<port>` | The port number of the primary or secondary RADIUS server.<br><br>**NOTE:** RADIUS servers use port 1812 by default to authenticate users. The Rack Monitor 250 supports ports 1 to 65535. |
| `-s1`<br>`-s2` | `<server secret>` | The shared secret between the primary or secondary RADIUS server and the Rack Monitor 250. |
| `-t1`<br>`-t2` | `<server timeout>` | The time in seconds that the Rack Monitor 250 waits for a response from the primary or secondary RADIUS server. |

**Example 1:** To view the existing RADIUS settings for the Rack Monitor 250, type `radius` and press ENTER.

**Example 2:** 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, Network-Only User

**Description:** Restart the network management interface of the Rack Monitor 250 only. This does not affect the output power of the Rack Monitor 250.

| 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: YES
Rebooting...
```

**Example 2:**

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

**Error Message:** `E000, E100`

# resetToDef

**Access:** Super User, Administrator

**Description:** Reset all configurable parameters to their defaults. Delete all accounts and clear Event and Data Logs.

> **NOTE:** Certain non-configurable parameters are not reset using `resetToDef`, and can only be erased from the Rack Monitor 250 by formatting the file system using the `format` command.

**Parameters:**

| Option | Arguments | Description |
|---|---|---|
| `-p` | `all \| keepip` | Caution: This resets all configurable parameters to their defaults.<br>`all` = Reset all configuration changes, including event actions, device settings, and TCP/IP settings.<br>`keepip` = Reset all configuration changes, *except* for the TCP/IP settings. |

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

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

**Error Message:** `E000, E100`

# session

**Access:** Super User, Administrator

**Description:** Records who is logged in (user), the interface, the address, time and ID.

**Parameters:**

| Option | Arguments | Description |
|---|---|---|
| -d | [-d <session nID>] (Delete) | Delete the session for the current user with the specified session ID. |
| -m | <enable \| disable> (MultiUser Enable) | Enable to allow two or more users to log on at the same time. Disable to allow only one user to log in at a time. |
| -a | <enable \| disable> (Remote Authentication Override) | The Rack Monitor 250 supports RADIUS storage of passwords on a server. Enable Remote Authentication Override to allow a local user to log on using a username and password for the Rack Monitor 250 that is stored locally on the Rack Monitor 250. |

**Example:**

```
apc> session
User    Interface  Address          Logged In Time      ID
-------------------------------------------------------

apc     Telnet     10.169.118.1-    00:00:03           19
                   00
E000: Success
```

**Error Message:** E000, E102

# smtp

**Access:** Super User, Administrator, Network-Only User

**Description:** Configure the settings for the local e-mail server.

**Parameters:**

| Option | Arguments | Description |
|---|---|---|
| -f | <From Address> | The address from which e-mail will be sent by the Rack Monitor 250. |
| -s | <SMTP Server> | The IPv4/IPv6 address or DNS name of the local SMTP server. |
| -p | <Port> | The SMTP port number, 25 by default. Common ports are 25 for unencrypted e-mail, and 465 and 587 for SSL/TLS encrypted e-mail. You can change the port setting to any port from 1 to 65535. |
| -a | <enable \| disable> | Enable this if your SMTP server requires authentication. |
| -u | <User Name> | If the SMTP server requires authentication, type the user name and password here. |
| -w | <Password> | |
| -e | <none \| ifavail \| always \| implicit> | Encryption options:<br>none: The SMTP server does not require/support encryption.<br>ifavail: The SMTP server advertises support for STARTTLS but does not require the connection to be encrypted. The STARTTLS command is sent after the advertisement is given. This is typically used with port 25.<br>always: The SMTP server requires the STARTTLS command to be sent upon connection to the server. This is typically used with port 587.<br>implicit: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server. This is typically used with port 465. |
| -c | <enable \| disable> | Require CA Root Certificate.<br>This should 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 CA certificate for the SMTP server must be installed to the Rack Monitor 250's certificate store using the certificate loader in order for a TLS connection with the SMTP server to succeed. |
| -i | <certificate file name> | The file name of the certificate. |

**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, Network-Only User

**Description:** Enable or disable and configure SNMPv1.

**NOTE:** SNMPv1 is disabled by default. The Community Name (`-c[n]`) must be set before SNMPv1 communications can be established.

**Parameters:**

| Option | Arguments | Description |
|---|---|---|
| `-S` | `<enable \| disable>` | Enable or disable SNMPv1 |
| `-c [n]` | `<Community>` | Specify a community name or string. |
| `-a [n]` | `<read \| write \| writeplus \| disable>` | Indicate the usage rights. |
| `-n [n]` | `<IP or Domain Name>` | Specify the IPv4/IPv6 address or the domain name of the Network Management Station. |
| `[n]` = the access control number: 1,2,3, or 4. | | |

**Example:** To enable SNMP version1, type

```
apc> snmp -S enable
E000:  Success
Reboot required for change to take effect.
```

**Error Message:** `E000, E102`

# snmpv3

**Access:** Super User, Administrator

**Description:** Enable or disable and configure SNMPv3.

**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>` | Specify a user name, an authentication phrase and encryption phrase. |
| `-a[n]` | `<Auth phrase>` | |
| `-c[n]` | `<Crypt phrase>` | |
| `-ap[n]` | `<sha \| md5 \| none>` | Indicate the type of authentication protocol. |
| `-pp[n]` | `<aes \| des \| none>` | Indicate the privacy (encryption) protocol. |
| `-ac[n]` | `<enable \| disable` | Enable or disable access. |
| `-au[n]` | `<User profile name>` | Give access to a specified user profile. |
| `-n[n]` | `<IP or Domain Name>` | Specify the IPv4/IPv6 address or the hostname for the Network Management Station. |
| `[n]` = Access Control # = 1, 2, 3, through 8 | | |

**Example:** To give access level 2 to user “JMurphy”, type

```
apc> snmpv3 -au2 "JMurphy"
E000: Success

*Reboot required for change to take effect
```

**Error Message:** `E000, E102`

# snmptrap

**Access:** Super User, Administrator, Network-Only User

**Description:** Enable or disable SNMP trap generation

**Parameters:**

| Option | Arguments | Description |
|---|---|---|
| `-c[n]` | `<Community>` | Specify a community name or string. |
| `-r[n]` | `<Receiver NMS IP>` | The IPv4/IPv6 address or host name of the trap receiver. |
| `-l[n]` | `<Language code>` | Specify a language. English (`enUS`) is the only avaiable option at this time. |
| `-t[n]` | `[snmpV1 \| snmpV3]` | Specify the trap type: SNMPv1 or SNMPv3. |
| `-p[n]` | `<Port>` | Specify the SNMP trap port number for this trap receiver (162 by default). The range is 1 to 65535. |
| `-g[n]` | `[enable \| disable]` | Enable or disable trap generation for this trap receiver. Enabled by default. |
| `-a[n]` | `[enable \| disable]` | Enable or disable authentication of traps for this trap receiver, SNMPv1 only. |

| Option | Arguments | Description |
|---|---|---|
| -u[n] | <profile1 \| profile2 \| profile3 \| profile4> | Select the identifier of the user profile for this trap receiver, SNMPv3 only. |
| n = Trap receiver # = 1, 2, 3, 4, 5, or 6 | | |

**Example:** To enable and configure an SNMPv1 trap for Receiver 1, with the Community Name of public, receiver 1 IP address of 10.169.118.100, using the default English language, type

```
apc> snmptrap -c1 public -r1 10.169.118.100 -l1 enUS -t1
snmpV1 -g1 enable
E000: Success
```

**Error Message:** E000, E102

## ssh

**Access:** Super User, Administrator, Network-Only User

**Description:** Show, delete, and generate SSH server keys.

**NOTE:** You must use the ssh key command to use the options below.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| -s | | Display the current SSH server key in use. |
| -f | | Display the current SSH server key's fingerprint. |
| -d | | Delete the current SSH server key in use. |
| -i | <filename>.p15 | Import the SSH server key from a PKCS #15 file. |
| -ecdsa | <256> (bit size) | Generate an Elliptic Curve Digital Signature Algorithm (ECDSA) SSH server key with the specified size in bits. |
| -rsa | <1024 \| 2048 \| 4096>(bit size) | Generate a Rivest–Shamir–Adleman (RSA) SSH server key with the specified size in bits. |

**Example 1:** To delete the SSH server key, type

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

**Example 2:** To import the SSH server key from a .p15 file generated by the NMC Security Wizard CLI Utility, type

```
apc> ssh key -i nmc.p15
E000: Success
```

**Error Messages:** E000, E102

## ssl

**Access:** Super User, Administrator, Network-Only User

**Description:** Configure and manage the Rack Monitor 250's public key and Web UI certificate, and create a Certificate Signing Request (CSR).

**NOTE:** There are three sets of options for this command, indicated below (key, csr, and cert).

### Configure public keys (`key`):

| Option | Argument | Description |
|---|---|---|
| `-s` | | Display the current public key in use. |
| `-d` | | Delete the current public key in use. |
| `-i` | `<filename>.p15` | Import the public key from a PKCS #15 file. |
| `-ecdsa` | `<256 \| 384 \| 521>` | Generate an Elliptic Curve Digital Signature Algorithm (ECDSA) public key with the specified size in bits. |
| `-rsa` | `<1024 \| 2048 \| 4096>` | Generate a Rivest–Shamir–Adleman (RSA) public key with the specified size in bits. |

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

**Example 1:** To generate a new ECDSA-521 public key, type

```
apc> ssl key —ecdsa 521
E000: Success
```

**Example 2:** To import the public key from a .p15 file generated by the NMC Security Wizard CLI Utility, type

```
apc> ssl key -i nmc.p15
E000: Success
```

### Configure Certificate Signing Request (`csr`):

| Option | Argument | Description |
|---|---|---|
| `-s` | `<File Name>` | Show the current CSR. If no file path is specified, the command checks the default location: ssl/nmc.csr. |
| `-q` | `<File Name>` | Create a CSR from an active configuration. If no file path is specified, the CSR is stored at the default location: ssl/nmc.csr |
| `-CN` | `<Common Name>` | Create a custom CSR. The Common Name is the fully qualified domain name (FQDN) of the Rack Monitor 250. For example, its IP address or *.nmc.local. |
| Custom Certificate Signing Request (CSR) options. **NOTE:** The options below are only available for `-CN` | | |
| `-O` | `<organization>` | The name of your organization. |
| `-OU` | `<organization unit>` | The division of your organization handling the certificate. |
| `-C` | `<country>` | The two-letter country code of where your organization is located. |
| `-san` | `<Common Name \| IP Address>` | The Common Name or IP address of the Rack Monitor 250. |

**NOTE:** Created Certificate Signing Requests will be stored in the Rack Monitor 250's ssl directory. See dir, page 109.

**Example 3:** To create a quick CSR from the current configuration, type

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

**Example 4:** To create a minimal CSR, type

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

**Example 5:** To create a custom Certificate Signing Request (CSR), type

```
apc> ssl csr -CN apcXXXXXX.nmc.local -C US -san *.nmc.local
-san 190.0.2.0
E000: Success
```

**Configure the Web UI's certificate (`cert`):**

| Option | Argument | Description |
|---|---|---|
| `-s` | `<File Name>` | Display the specified certificate. **NOTE:** Executing this option without an argument will display the current certificate in use. |
| `-f` | `<File Name>` | Display the specified certificate's fingerprint. **NOTE:** Executing this option without an argument will display the current certificate's fingerprint. |
| `-i` | `<File Name>` | Import a 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 6:** To show the active certificate, type

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

Certificate
-----------
  Serial Number: XXXXxXXXXXXxXXXXx
  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: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
  Thumbprint: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
  Fingerprint:
  xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

**Example 7:** To display nmc.crt located in the ssl directory, type
`ssl cert -s ssl/nmc.crt`

**Example 8:** To import another certificate (*other.crt*), type
`apc> ssl cert -i other.crt`

**Error Messages:** `E000, E102`

# system

**Access:** Super User, Administrator

**Description:** View and set the system name, the contact, the location. Configure system messages, 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, page 96 for more information about system status).(See 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.<br><br>**NOTE:** If you define a value with more than one word, you must enclose the value in quotation marks. These values are also used |
| `-c` | `<system contact>` | |
| `-l` | `<system location>` | |

| | | |
|---|---|---|
| | | by StruxureWare Data Center Expert, or EcoStruxure IT Expert and the Rack Monitor 250's SNMP agent. |
| -m | <system message> | Show a configurable custom message or banner on the logon page of the Web UI, CLI (Serial, Telnet, SSH), FTP or SCP. |
| -s | <enable \| disable> | Allow the host name to be synchronized with the system name so both fields automatically contain the same value.<br><br>This is the same as using "dns -y".<br><br>**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). |

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

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

**Example 2:** To set the system name as Don Adams, type

```
apc> system -n "Don Adams"
E000: Success
```

**Error Message:** E000, E102

# tacacs+

**Access:** Super User, Administrator, Network-Only User

**Description:** View the existing TACACS+ settings and configure basic authentication parameters for up to two TACACS+ servers.

| Option | Argument | Description |
|---|---|---|
| -p1<br>-p2 | <server IP> | The server name or IP address of the primary or secondary TACACS+ server.<br>. |
| -o1<br>-o2 | <port> | The port number of the primary or secondary TACACS + server.<br>**NOTE:** TACACS+ servers use port 49 by default to authenticate users. The NMC supports ports 1 to 65535. |
| -s1<br>-s2 | <server secret> | The shared secret between the primary or secondary TACACS+ server and the NMC. |
| -t1<br>-t2 | <server timeout> | The time in seconds that the NMC waits for a response from the primary or secondary TACACS+ server. |
| -d1<br>-d2 | | Delete the primary or secondary TACACS+ server configuration. |
| -r | <0 — 15> | Read-Only User privilege level. |
| -a | <0 — 15> | Administrator privilege level. |

**Example 1:** To view the existing TACACS+ settings for the NMC, type:

```
tacacs+
```

**Example 2:**To configure a 10 second time out for a secondary TACACS+ server, type:

```
tacacs+ -t2 10
```

# tcpip

**Access:** Super User, Administrator

**Description:** View and manually configure IPV4 TCP/IP settings for the Rack Monitor 250.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| -S | enable \| disable | Enable or disable TCP/IP v4. |
| -l | <IPv4 address> | Type the IP address of the Rack Monitor 250, using the format *xxx.xxx.xxx.xxx* |
| -s | <subnet mask> | Type the subnet mask for the Rack Monitor 250. |
| -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 Monitor 250 will use. |

**Example 1:** To view the network settings of the Rack Monitor 250, type

```
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 manually configure an IP address of `192.168.1.49`, 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 Monitor 250:

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-S` | `enable` \| `disable` | Enable or disable IPv6. |
| `-man` | `enable` \| `disable` | Enable manual addressing for the IPv6 address of the Rack Monitor 250. |
| `-auto` | `enable` \| `disable` | Enable the Rack Monitor 250 to automatically configure the IPv6 address |
| `-i` | `<IPv6 address>` | Set the IPv6 address of the Rack Monitor 250 |
| `-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), or `never`. |

**Example 1:** To view the network settings of the Rack Monitor 250, 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
```

**Example 2:** To manually configure an IPv6 address of 2001:0:0:0:0:FFD3:0:57ab for the, type

```
tcpip -i 2001:0:0:0:0:FFD3:0:57ab
```

**Error Message:** `E000`, `E102`

# user

**Access:** Super User, Administrator

**Description:** Configure the user name, password, and inactivity timeout for each account type.

**NOTE:** You can't edit a user name; you must delete it and then create a new user.

**NOTE:** To change the Super User account settings remotely, you must enter the current password (`-cp`).

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-n` | `<user>` | Indicate the user. |
| `-cp` | `<current password>` | For a Super User, you must specify the current password.<br>**NOTE:** The `-cp` option is only required when changing the Super User's settings remotely. |
| `-pw` | `<user password>` | Specify these options for a user.<br>**NOTE:** The description must be enclosed in quotation marks. |
| `-pe` | `<user permission>` | |
| `-d` | `<user description>` | |
| `-e` | `enable \| disable` | Enable or disable access for the particular user account. |
| `-te` | `enable \| disable` | Enable or disable touch screen access. |
| `-tp` | `<touch screen access pin>` | This option is only available on certain devices. |
| `-tr` | `enable \| disable` | Enable the touch screen remote authorization override. This option is only available on certain devices. If you enable this override, the Rack Monitor 250 will allow a local user to log on using the password for the Rack Monitor 250 that is stored locally on the Rack Monitor 250. |
| `-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. English is the only available language at this time. |
| `-del` | `<user name>` | Delete a user. |
| `-l` | | Display the current user list. |

**Example 1:** To change the log off time to 10 minutes for user "JMurphy", type `user -n "JMurphy" -st 10`

**Example 2:** To change the log off time to 10 minutes for the Super User "apc", type `user -n "apc" –cp <password> –st 10`

**Error Message:** `E000, E102`

# userauth

**Access:** Super User, Administrator, Network-Only User

**Description:** View or configure the user authentication method. Local authentication, as well as the LDAP, RADIUS, and TACACS+ protocols are supported.

| Option | Argument | Description |
|---|---|---|
| `-l` | `first \| last \| off` | Specify if and when the local user database is checked:<br><br>**first:** The local user database is always checked first. If the username is found, then the password is checked and the login either succeeds or is unsuccessful. If the username is not found, then remote authentication is used, if enabled.<br><br>**last:** The local user database is checked after attempting remote authentication, if there is an error contacting the remote authentication server. When remote authentication is off, it behaves the same as first.<br><br>**off:** The local user database is never checked.<br><br>**Note:** Setting this to off is not recommended as it can result in being permanently locked out of the NMC if the remote authentication server goes down or is misconfigured on the NMC. If off is used, it is strongly recommended to enable the Remote Authentication Override setting (session –a) and to set the Serial Remote Authentication Override option (user –sr) for the Super User or an Administrator.<br><br>**Note:** If both Local and Remote User Authentication settings are set to off, then Local User Authentication will automatically be set to first.<br>. |
| `-r` | `off \| radius \| tacacs+ \| ldap` | Specify which, if any, and remote authentication protocol is used:<br><br>**off:** Do not use remote user authentication and always perform local user authentication.<br><br>**radius:** Remote user authentication will use RADIUS.<br><br>**tacacs+:** Remote user authentication will use TACACS +.<br><br>**ldap:** Remote user authentication will use LDAP. |

**Example :** To configure local authentication first, followed by TACACS+ authentication, type:

```
userauth -l first -r tacacs+
```

# userdflt

**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. The description must be enclosed in quotation marks. |
| -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.<br><br>**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:<br>• The password must be 8–64 characters long.<br>• The password must contain at least one lowercase ltter, one uppercase letter, one number, and one symbol ( ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [ \ ] ^ _ ` { \| } ~). |
| -pp | <interval in days> | Required password change interval. |

**Example:** To set the default user's session timeout to 60 minutes, type
```
apc> userdflt -st 60
E000: Success
```
**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.<br>HTTP is disabled by default. |
| -s | enable \| disable | Enable or disable access to the user interface for HTTPS.<br>HTTPS is enabled by default.<br>When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate. |
| -mp | <minimum protocol> | Specify the minimum protocol used by the web interface: SSL v3.0,TLS v1.1, or TLS v1.2. |
| -ph | <http port #> | Specify the TCP/IP port used by HTTP to communicate with the Rack Monitor 250 (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 Monitor 250 (443 by default). The other available range is 5000–32768. |
| -lsp | enable \| disable | Enable or disable access to the Limited Status page in the Web UI. |
| -lsd | enable \| disable | Enable or disable the Limited Status page being used as the default page when accessing the device's IP or hostname in a web browser. |
| -cs | <0 \| 1 \| 2 \| 3 \| 4> | Select the level of security of TLS v1.2 cipher suites between 0 - 4, where 4 is the highest level of security, and 0 is the lowest level of security. The default value is 4.<br><br>**NOTE:** The -cs option is only applied when -mp is set to TLS v1.2.<br><br>When a value between 0 - 4 is entered, the CLI responds with a list of the currently allowed SSL cipher suites. |
| -hs | enable \| disable | Enable/ disable the HTTP Strict Transport Security Header (HSTS) response header. |

**Example 1:** To prevent all access to the Web UI, type
```
apc> web -h disable -s disable
```

**Example 2:** To define the TCP/IP port used by HTTP, type
```
apc> web -ph 80
E000: Success
```

**Error Message:** `E000, E102`

## whoami

**Access:** Super User, Administrator, Device User, Read-Only User, Network-Only User

**Description:** Provides login information on the current user.

**Parameters:** None

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

**Error Message:** `E000, E102`

# 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: Successful
```

See Last Transfer Result Codes, page 163 for descriptions of the transfer result codes.

**Error Message:** `E000`

# Device Command Descriptions

## modbus

**Access:** Super User, Administrator

**Description:** View or configure modbus options.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| -a | enable \| disable | Enable or disable Modbus. |
| -br | 2400 \| 9600 \| 19200 \| 38400 | Specify the baud rate. |
| -pr | even \| odd \| none | Select even or odd or no parity. The number of stop bits is automatically selected: for no parity, 2 stop bits, and for even/odd parity,1 stop bit in Modbus master. |
| -m | 8e1 \| 8o1 \| 8n2 \| 8n1 | Set the parity and stop bits.<br>• 8e1: Even parity, 1 stop bit<br>• 8o1: Odd parity, 1 stop bit<br>• 8n2: No parity, 2 stop bits<br>• 8n1: No parity, 1 stop bit |
| -s | <1-F7> | Specify the Modbus slave address in hexidecimal. |
| -rDef | no argument | Restore default settings. |
| -tE | enable \| disable | Enable or disable Modbus TCP. |
| -tP | no argument | View the Modbus TCP port number. |
| -tTO | <0-64800> | TCP communication in timeout in seconds. 0 = never. |
| -ka | enable \| disable | Modbus TCP keep-alive |

**Example 1:** To enable modbus, enter

```
apc> modbus -a enable
```

**Example 2:** To disable modbus, enter

```
apc> modbus -a disable
E000: Success

apc> modbus
E000: Success

Slave Address = 0x1
Status = DISABLED
Baud Rate = 9600
Parity/Stop bits Mode = EVEN (8, E, 1)
TCP Status = DISABLED
TCP Port Number = 502
TCP Communication Timeout = 30 secs
```

**Error Messages:** E000, E101, E102

# nbabout

**Access:** Super User, Administrator, Device User, Read-only User

**Description:** View or configure information about the Rack Monitor 250. Enter a `<new>` value (where applicable) to configure settings.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-n` | `<name>` | Set a name for the appliance (up to 20 characters). |
| `-l` | `<location>` | Set the location of the appliance (up to 20 characters). |
| `-a` | no argument | View the cumulative alarm status. |
| `-mn` | no argument | View the model number. |
| `-sn` | no argument | View serial number. |
| `-fw` | no argument | View the firmware version of the sensor access controller. |
| `-hw` | no argument | View hardware version. |

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

```
apc> nbabout -n New_Name
Old Name: NetBotz
New Name: New_Name
E000: Success
```

**Error Messages:** `E000, E200, E201, E202, E203, E204`

# nbbeacon

**Access:** Super User, Administrator, Device User, Read-only User

**Description:**View or configure information for the beacon attachment (AP9324).

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-n` | `<name>` | Set a name for the beacon (up to 20 characters). |
| `-l` | `<location>` | Set the location of the beacon (up to 20 characters). |
| `-s` | `Off \| On` | Turn the beacon off or on. |

**Example:**

```
apc> nbbeacon -n New_Name
Old Name: Beacon NB
New Name: New_Name
E000: Success
```

**Error Messages:** `E000, E200, E201, E202, E203, E204`

# nboutlet

**Access:** Super User, Administrator, Device User, Read-only User

**Description:** View information about the switched outlet.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| -n | <name> | Set a name for the outlet (up to 20 characters). |
| -l | <location> | Set the location of the outlet (up to 20 characters). |
| -s | Off \| On | Set the current switched outlet state. |
| -ns | Off \| On | Set the normal switched outlet state. |

**Example:**

```
apc> nboutlet -n New_Name
Old Name: Outlet
New Name: New_Name
E000: Success
```

**Error Messages:** E000, E200, E201, E202, E203, E204

# nbrack

**Access:** Super User, Administrator, Device User, Read-only User

**Description:** View or configure rack access information.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| -c | HID26b \| HID37b \| HID37Fac \| Corp1000 \| Mifare4B \| Mifare7B \| MifareD \| MifareP \| iCLASS8B | Enter the type of rack-access cards used with the appliance. |
| -r | no argument | View the number of registered rack access card users. |
| -rr | [1:200] | View the RFID number associated with a registered user's rack access card. |
| -rn | [1:200 <user name>] | Identify a registered user (1–200) and assign him or her a user name. |
| -rc | [1:200 <contact info>] | Identify a registered user (1–200) and enter his or her contact information. |
| -rs | [1:200 <Disabled \| Enabled \| Delete >] | Identify a registered user (1–200). Disable or enable rack access for that user, or delete the user account. |
| -u | no argument | View the number of unregistered users that have held a rack access card up to a lock configured for rack access. |
| -ur | [1:10] | View the RFID number associated with for an unregistered user's rack access card. |
| -us | [1:10 <Register \| Delete>] | Identify an unregistered user (1–10). Register or delete that user. |
| -cs | disabled \| enabled | View the card reader status, or enable/disable the card readers. |
| -ds | [1:2] | View the state of door sensor 1 or door sensor 2. |
| -ls | [1:2 <locked \| unlocked>] | Set the state (locked or unlocked) of rack handle 1 or rack handle 2. |
| -fw | no argument | View the firmware version of the rack access controller. |

**Example:**

```
apc> nbrack -c HID-37
Old Card : HID-26
New Card : HID-37
E000: Success
```

**Error Messages:** E000, E200, E201, E202, E203, E204

# nbrelay

**Access:** Super User, Administrator, Device User, Read-only User

**Description:** View or configure information about the output relay.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| -n | <name> | Set a name for the relay (up to 20 characters). |
| -l | <location> | Set the location of the relay (up to 20 characters). |
| -s | Closed \| Open | Set the current relay output state. |
| -ns | Closed \| Open | Set the normal relay output state. |

**Example:**

```
apc> nbrelay -n New_Name
Old Name : Relay
New Name : New_Name
E000: Success
```

**Error Messages:** E000, E200, E201, E202, E203, E204

# nbsensor

**Access:** Super User, Administrator, Device User, Read-only User

**Description:** Configure settings for sensors connected to universal sensor ports and Temperature & Humidity sensors cascaded from the A-Link ports. Select each sensor by its number: universal sensor ports are designated as 1–6 (according to the port number), while cascaded sensors are designated as 7–14 (according to the A-Link address).

**NOTE:** You can set a unique A-Link address for each cascaded Temperature & Humidity sensor (see the sensor documentation on www.apc.com for details). The sensor number is the A-Link address plus 6 (for example, a sensor with an A-Link address of 1 would be designated as 7 in the CLI). You can also check the sensor name and type of cascaded sensor to determine which is which.

**Parameters:**

**General**

| Option | Argument | Description |
|---|---|---|
| -n | [1:14 <name>] | Set a name for the sensor (up to 20 characters). |
| -l | [1:14 <location>] | Set the location of the sensor (up to 20 characters). |
| -tp | [1:14] | View the sensor type. |
| -a | [1:14] | View active alarms. |
| -ds | [1-6 <Info \| Warn \| Crit>] | Set the severity of alarms generated by a discrete sensor (informational, warning, or critical). |

**Temperature Sensor Thresholds**

| Option | Argument | Description |
|---|---|---|
| -t | [1:14] | View the current temperature on the selected temperature sensor. |
| -tmx | [1:14 <max temp>] | Set the maximum allowable temperature by sensor. If the temperature rises above this value, a critical alarm is generated. |
| -th | [1:14 <high temp>] | Set the threshold for the high temperature alarm by sensor. If the temperature rises above this value, a warning alarm is generated. |

**Temperature Sensor Thresholds (Continued)**

| Option | Argument | Description |
|---|---|---|
| -tl | [1:14 <low temp>] | Set the threshold for the low temperature alarm by sensor. If the temperature goes below this value, a warning alarm is generated. |
| -tmn | [1:14 <min temp>] | Set the threshold for the minimum allowable temperature by sensor. If the temperature goes below this value, a critical alarm is generated. |
| -thy | [1:14 <hysteresis>] | Set hysteresis for temperature alarms by sensor. This hysteresis value determines the point at which temperature alarms are cleared (the clearing point). The clearing point for a high/ maximum alarm is the alarm threshold minus the hysteresis value. The clearing point for a low/ minimum alarm is the threshold plus the hysteresis value. For example, if you have a low temperature threshold of 26 degrees and a hysteresis value of 5, the clearing point for a low temperature alarm would be 31 degrees (26 plus 5). |

**Long-term rate-of-change thresholds: Set alarms to indicate a change in temperature over several hours.**

| Option | Argument | Description |
|---|---|---|
| -tlim | [1:14 <degree range increase>] | Set the maximum number of degrees the temperature can increase within a specified time before an alarm is generated. |
| -tlit | [1:14 <hours increase>] | View or specify a number of hours. If the temperature increases too much within the time period you specify, an alarm is generated. |
| -tldm | [1:14 <degree range decrease>] | Set the maximum number of degrees the temperature can decrease before an alarm is generated. |
| -tldt | [1:14 <hours decrease>] | Set the number of hours. If the temperature decreases too much within the time period you specify, an alarm is generated. |

**NOTE:** All violations to rate-of-change thresholds result in critical alarms.

**Short-term rate-of-change thresholds: Set alarms to indicate a change in temperature over several minutes.**

| Option | Argument | Description |
|---|---|---|
| -tsim | [1:14 <degree range increase>] | Set the maximum number of degrees the temperature can increase within a specified time before an alarm is generated. |
| -tsit | [1:14 <hours increase>] | View or specify a number of minutes. If the temperature increases too much within the time period you specify, an alarm is generated. |
| -tsdm | [1:14 <degree range decrease>] | Set the maximum number of degrees the temperature can decrease before an alarm is generated. |
| -tsdt | [1:14 <hours decrease>] | Set the number of minutes. If the temperature decreases too much within the time period you specify, an alarm is generated. |

**NOTE:** All violations to rate-of-change thresholds result in critical alarms.

**Humidity Sensor Thresholds**

| Option | Argument | Description |
|---|---|---|
| -h | [1:14] | View the current humidity on the selected humidity sensor. |
| -hmx | [1:14 <max humidity>] | Set the maximum allowable humidity by sensor. If the humidity rises above this value, a critical alarm is generated. |
| -hh | [1:14 <high humidity>] | Set the threshold for the high humidity alarm by sensor. If the humidity rises above this value, a warning alarm is generated. |
| -hl | [1:14 <low humidity>] | Set the threshold for the low humidity alarm by sensor. If the humidity goes below this value, a warning alarm is generated. |

### Humidity Sensor Thresholds (Continued)

| Option | Argument | Description |
|---|---|---|
| -hmn | [1:14 <min humidity>] | Set the threshold for the minimum allowable humidity by sensor. If the humidity goes below this value, a critical alarm is generated. |
| -hhy | [1:14 <hysteresis>] | Set hysteresis for humidity alarms by sensor. This hysteresis value determines the point at which humidity alarms are cleared (the clearing point). The clearing point for a high/maximum alarm is the alarm threshold minus the hysteresis value. The clearing point for a low/minimum alarm is the threshold plus the hysteresis value. For example, if you have a low humidity threshold of 26 degrees and a hysteresis value of 5, the clearing point for a low humidity alarm would be 31 degrees (26 plus 5). |

### Voltage Sensor Thresholds

| Option | Argument | Description |
|---|---|---|
| -v | [1:6] | View the current voltage on the selected voltage sensor. |
| -vmx | [1:6 <max voltage>] | View or configure the maximum allowable voltage. If the voltage rises above this value, a critical alarm is generated. |
| -vmn | [1:6 <min voltage>] | View or configure the minimum allowable voltage. If the voltage falls below this value, a critical alarm is generated. |

### Example:

```
apc> nbsensor -n 4 New_Name

Old Name : Sensor NB:4

New Name : New_Name

E000: Success
```

**Error Messages:** E000, E200, E201, E202, E203, E204

# spabout

**Access:** Super User, Administrator, Device User, Read-only User

**Description:** View or configure sensor pod settings. Identify the senor pod by its reference number (1–12). You can view the reference number on the LED display of your sensor pod.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| -n | [1:12 <name>] | Enter a name for the sensor pod (up to 20 characters). |
| -l | [1:12 <location>] | Enter the location of the sensor pod (up to 20 characters). |
| -a | [1:12] | View the alarm status of all sensor pod sensors. |
| -mn | [1:12] | View the model number. |
| -sn | [1:12] | View the serial number. |
| -fw | [1:12] | View the firmware version. |
| -hw | [1:12] | View the hardware version. |
| -r | [1:12] | View the reference number. |

**Example:**

```
apc> spabout -n 1 New_Name
Old Name : NBPod150
New Name : New_Name
E000: Success
```

**Error Messages:** E000, E200, E201, E202, E203, E204

# spsensor

**Access:** Super User, Administrator, Device User, Read-only User

**Description:** View and configure settings for wired sensors connected to a Sensor Pod 150. Identify the senor pod by its reference number (1–12). (You can view the reference number on the LED display of your sensor pod.) Then identify the sensor by the port to which it is connected (1-6).

**Parameters:**

**General**

| Option | Argument | Description |
|---|---|---|
| -n | [1:12 [1:6 <name>]] | Set a name for the sensor (up to 20 characters). |
| -l | [1:12 [1:6 <location>]] | Set the location of the sensor (up to 20 characters). |
| -tp | [1:12 [1:6]] | View the sensor type. |
| -a | [1:12 [1:6]] | View active alarms. |
| -ds | [1:12 [1:6 <Info \| Warn \| Crit>]] | Set the severity of alarms generated by a discrete sensor (informational, warning, or critical). |

**Temperature Sensor Thresholds**

| Option | Argument | Description |
|---|---|---|
| -t | [1:12 [1:6]] | View the current temperature on the selected temperature sensor. |
| -tmx | [1:12 [1:6 <max temp>]] | Set the maximum allowable temperature by sensor. If the temperature rises above this value, a critical alarm is generated. |

**Temperature Sensor Thresholds (Continued)**

| Option | Argument | Description |
|---|---|---|
| -th | [1:12 [1:6 <high temp>]] | Set the threshold for the high temperature alarm by sensor. If the temperature rises above this value, a warning alarm is generated. |
| -tl | [1:12 [1:6 <low temp>]] | Set the threshold for the low temperature alarm by sensor. If the temperature goes below this value, a warning alarm is generated. |
| -tmn | [1:12 [1:6 <min temp>]] | Set the threshold for the minimum allowable temperature by sensor. If the temperature goes below this value, a critical alarm is generated. |
| -thy | [1:12 [1:6 <hysteresis>]] | Set hysteresis for temperature alarms by sensor. This hysteresis value determines the point at which temperature alarms are cleared (the clearing point). The clearing point for a high/ maximum alarm is the alarm threshold minus the hysteresis value. The clearing point for a low/ minimum alarm is the threshold plus the hysteresis value. For example, if you have a low temperature threshold of 26 degrees and a hysteresis value of 5, the clearing point for a low temperature alarm would be 31 degrees (26 plus 5). |

**Long-term rate-of-change thresholds: Set alarms to indicate a change in temperature over several hours.**

| Option | Argument | Description |
|---|---|---|
| -tlim | [1:12 [1:6 <degree range increase>]] | Set the maximum number of degrees the temperature can increase within a specified time before an alarm is generated. |
| -tlit | [1:12 [1:6 <hours increase>]] | View or specify a number of hours. If the temperature increases too much within the time period you specify, an alarm is generated. |
| -tldm | [1:12 [1:6 <degree range decrease>]] | Set the maximum number of degrees the temperature can decrease before an alarm is generated. |
| -tldt | [1:12 [1:6 <hours decrease>]] | Set the number of hours. If the temperature decreases too much within the time period you specify, an alarm is generated. |

**NOTE:** All violations to rate-of-change thresholds result in critical alarms.

**Short-term rate-of-change thresholds: Set alarms to indicate a change in temperature or humidity over several minutes.**

| Option | Argument | Description |
|---|---|---|
| -tsim | [1:12 [1:6 <degree range increase>]] | Set the maximum number of degrees the temperature can increase within a specified time before an alarm is generated. |
| -tsit | [1:12 [1:6 <hours increase>]] | View or specify a number of minutes. If the temperature increases too much within the time period you specify, an alarm is generated. |
| -tsdm | [1:12 [1:6 <degree range decrease>]] | Set the maximum number of degrees the temperature can decrease before an alarm is generated. |
| -tsdt | [1:12 [1:6 <hours decrease>]] | Set the number of minutes. If the temperature decreases too much within the time period you specify, an alarm is generated. |

**NOTE:** All violations to rate-of-change thresholds result in critical alarms.

**Humidity Sensor Thresholds**

| Option | Argument | Description |
|---|---|---|
| -h | [1:12 [1:6]] | View the current humidity on the selected humidity sensor. |
| -hmx | [1:12 [1:6 <max humidity>]] | Set the maximum allowable humidity by sensor. If the humidity rises above this value, a critical alarm is generated. |
| -hh | [1:12 [1:6 <high humidity>]] | Set the threshold for the high humidity alarm by sensor. If the humidity rises above this value, a warning alarm is generated. |

### Humidity Sensor Thresholds (Continued)

| Option | Argument | Description |
|---|---|---|
| -hl | [1:12 [1:6 <low humidity>]] | Set the threshold for the low humidity alarm by sensor. If the humidity goes below this value, a warning alarm is generated. |
| -hmn | [1:12 [1:6 <min humidity>]] | Set the threshold for the minimum allowable humidity by sensor. If the humidity goes below this value, a critical alarm is generated. |
| -hhy | [1:12 [1:6 <hysteresis>]] | Set hysteresis for humidity alarms by sensor. This hysteresis value determines the point at which humidity alarms are cleared (the clearing point). The clearing point for a high/maximum alarm is the alarm threshold minus the hysteresis value. The clearing point for a low/minimum alarm is the threshold plus the hysteresis value. For example, if you have a low humidity threshold of 26 degrees and a hysteresis value of 5, the clearing point for a low humidity alarm would be 31 degrees (26 plus 5). |

### Voltage Sensor Thresholds

| Option | Argument | Description |
|---|---|---|
| -v | [1:12 [1:6]] | View the current voltage on the selected voltage sensor. |
| -vmx | [1:12 [1:6 <max voltage>]] | View or configure the maximum allowable voltage. If the voltage rises above this value, a critical alarm is generated. |
| -vmh | [1:12 [1:6 <min voltage>]] | View or configure the minimum allowable voltage. If the voltage falls below this value, a critical alarm is generated. |

### Example:

```
apc> spsensor -n 2 New_Name

Old Name : Sensor SP 06:2

New Name : New_Name

E000: Success
```

**Error Messages:** E000, E200, E201, E202, E203, E204

## zw

**Access:** Super User, Administrator

**Description:** View information for all Zigbee wireless sensors, or select a wireless sensor (1–48) to view and edit its settings.

### Parameters:

### General

| Option | Argument | Description |
|---|---|---|
| -c | no argument | View the number of commissioned sensors. |
| -ch | [1:48] | View the wireless channel of the sensor. |
| -n | [1:48 <name>] | View or configure sensor name (up to 20 characters). |
| -l | [1:48 <location>] | View or configure sensor location (up to 20 characters). |
| -sn | [1:48] | View the serial number. |
| -mn | [1:48] | View the model number. |
| -tp | [1:48] | View sensor type. |
| -a | [1:48] | View sensor active alarm severity. |
| -xa | [1:48] | View the extended address. |
| -fw | [1:48] | View the firmware version. |

### General (Continued)

| Option | Argument | Description |
|---|---|---|
| -s | [1:48] | View the Received Signal Strength Indicator (RSSI). |
| -sl | [1:48 <low signal>] | Set the threshold for low signal strength. If the signal strength goes below this value, an alarm is generated. |
| -smn | [1:48 <min signal>] | Set the threshold for the minimum allowable signal strength. If the signal strength goes below this value, an alarm is generated. |
| -b | [1:48] | View the battery voltage. |
| -bl | [1:48 <low threshold>] | Set the low battery threshold. If the battery voltage drops below this threshold, an alarm is generated. |
| -bmn | [1:48 <min voltage>] | Set the threshold for the minimum allowable battery voltage. If the battery voltage goes below this value, an alarm is generated. |
| -wn | <Enabled \| Disabled > | Enable or disable the wireless coordinator and all wireless communication. |

### Temperature Thresholds

| Option | Argument | Description |
|---|---|---|
| -t | [1:48] | View the current temperature on the selected sensor. |
| -tmx | [1:48 <max temp>] | Set the maximum allowable temperature by sensor. If the temperature rises above this value, a critical alarm is generated. |
| -th | [1:48 <high temp>] | Set the threshold for the high temperature alarm by sensor. If the temperature rises above this value, a warning alarm is generated. |
| -tl | [1:48 <low temp>] | Set the threshold for the low temperature alarm by sensor. If the temperature goes below this value, a warning alarm is generated. |
| -tmn | [1:48 <min temp>] | Set the threshold for the minimum allowable temperature by sensor. If the temperature goes below this value, a critical alarm is generated. |

### Humidity Sensor Thresholds

| Option | Argument | Description |
|---|---|---|
| -h | [1:48] | View the current humidity on the selected sensor. |
| -hmx | [1:48 <max humidity>] | Set the maximum allowable humidity by sensor. If the humidity rises above this value, a critical alarm is generated. |
| -hh | [1:48 <high humidity>] | Set the threshold for the high humidity alarm by sensor. If the humidity rises above this value, a warning alarm is generated. |
| -hl | [1:48 <low humidity>] | Set the threshold for the low humidity alarm by sensor. If the humidity goes below this value, a warning alarm is generated. |
| -hmn | [1:48 <min humidity>] | Set the threshold for the minimum allowable humidity by sensor. If the humidity goes below this value, a critical alarm is generated. |

### Example:

```
apc> zw -n 1 New_Name
Old Name : Wireless Sensor
New Name : New_Name
E000: Success
```

**Error Messages:** E000, E200, E201, E202, E203, E204

# zwsyslog

**Access:** Super User, Administrator

**Description:** Enable or disable forwarding of Zigbee wireless Sensor Data Packets (SDP) to a configured syslog server. This command is typically used for troubleshooting with Schneider Electric support.

**Parameters:**

| Option | Argument | Description |
|---|---|---|
| `-d` | `enable \| disable` | Enable: Enable forwarding of SDP over Syslog.<br>Disable: Disable forwarding of SDP over Syslog. |

**Example:**

```
apc> zwsyslog -d enable
E000: Success
```

**Error Messages:** `E000, E102`

# How to Export Configuration Settings

## Summary of the Procedure

A Super User/Administrator can retrieve the .ini file of a Rack Monitor 250 and export it to another Rack Monitor 250 or to multiple Rack Monitor 250s. The steps are below; see details in the sections following.

1. Configure a Rack Monitor 250 with the desired settings, and retrieve the .ini file from that Rack Monitor 250.
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 Monitor 250 to transfer a copy to one or more other devices. For a transfer to multiple Rack Monitor 250s, 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.se.com, and select you location. Then select **Support > Documentation & Software Downloads** and enter the article number or title of the FAQ in the Search bar.

## Contents of the .ini File

The config.ini file you retrieve from an 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 Monitor 250 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 Monitor 250) blocks the exporting of values for the `SystemIP`, `SubnetMask`, `DefaultGateway`, and `BootMode`.

# Detailed Procedures

## Retrieve .ini File

If possible, use the interface of a Rack Monitor 250 to configure it with the settings to export. (Directly editing the .ini file risks introducing errors).

Then retreive *config.ini*from the configured Rack Monitor 250 via FTP, SCP, or the Web UI:

**To use FTP**

1. Open a connection to the Rack Monitor 250 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 Monitor 250:

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

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

   To export configuration settings to multiple Rack Monitor 250s, see FAQ article FA156117: *How can I mass configure a Network Management Card (NMC) or NMC embedded product?* To find an FAQ article on www.se.com, enter the title or number of the article in the search bar. On the resulting page, select **Faq** to narrow your search results to only FAQ articles.

**To use SCP**

Use the following command:

```
scp -c <cihper> 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 Monitor 250s.

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 Monitor 250s 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 Monitor 250

To transfer the .ini file to another Rack Monitor 250, do either of the following:

- From the Web UI of the receiving Rack Monitor 250, 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 Monitor 250, 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 Monitor 250 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 Monitor 250:

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

# Transfer the File To Multiple Rack Monitor 250s

To transfer the .ini file to multiple Rack Monitor 250s, 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 Monitor 250s.
- 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 on www.se.com, enter the title or number of the article in the search bar. On the resulting page, select **Faq** to narrow your search results to only FAQ articles.

# The Upload Event and Error Messages

## The Event and Its Error Messages

The following event occurs when the receiving Rack Monitor 250 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 Monitor 250 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 Monitor 250 from which you download the config.ini file must be discovered successfully in order for its configuration to be included. If the Rack Monitor 250 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 Monitor 250 not discovered`

If you did not intend to export the Rack Monitor 250 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 155 for information about which values are overridden.

Because the overridden values are device-specific and not appropriate to export to other Rack Monitor 250, 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 Monitor 250 and configure other settings through its user interface. See for instructions to download and install the Device IP Configuration Wizard.

# Updating Firmware

When you update the firmware on the Rack Monitor 250:

- 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 Monitor 250 support the same features in the same manner. Here, upgrading simply means placing the firmware file on the Rack Monitor 250; there is no installation required. Check regularly on www.apc.com for any new updates.

# Firmware File Transfer Methods

To update the firmware of one or more NMCs **to firmware version 2.5.x or earlier**, use one of these five methods:

- On a Windows operating system, use the **Firmware Update Utility** downloaded from . See Use the Firmware Update Utility, page 160.
- On any supported operating system, use **FTP** or **SCP** to transfer the `.nmc3` file. See Use FTP or SCP to Update One Rack Monitor 250, page 161.
- For a Network Management Card that is NOT on your network, use **XMODEM** through a USB virtual communication port via the boot loader to transfer the . nmc3 file from your computer to the NMC. See .
- Use a **USB drive** to transfer the `.nmc3` file from your computer to the NMC. See Use a USB Drive To Transfer and Update Files, page 162
- For updates to multiple Rack ATS units, see How To Update Multiple Rack Monitor 250s, page 162.

# Use the Firmware Update Utility

This Firmware Update Utility is part of the firmware update package available on www.se.com/ww/en/download. (*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 Monitor 250.

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 159 for the different upgrade methods after extraction.

# Use FTP or SCP to Update One Rack Monitor 250

**FTP**

To use FTP to update a Rack Monitor 250 over the network:

- The must be on the network with its system IP, subnet mask, and default gateway configured.
- The FTP server must be enabled at the Rack Monitor 250. 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 Monitor 250, 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 or Administrator. The default username and password for the Super User are both **apc**.
6. Use the `put` command to send the .nmc3 file: `put` *`filename.nmc3`*

   For example:

   (where `x-x-x-x` 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 Monitor 250, follow these steps:

**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 Monitor 250. The following example uses `x-x-x-x` to represent the version number of the firmware:

   **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

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. Download the firmware update files and unzip them if needed. Copy the **app. nmc3** firmware file into the **apcfirm** folder.

   **NOTE:** Only use firmware applications intended for your device type and NMC.
3. Use a text editor to create a file named **nmc3.rcf** and save it to the **apcfirm** folder. (The file extension must be .rcf, not .txt for example.)

   Add only the following text to the file: `NMC3=application_name.nmc3`, where `application_name` is filename of the firmware update file.

   For example: If the update firmware file is
   , the text file should say `NMC3=apc_hw21_ats5g_x-x-x-x.nmc3.`

   Save the changes to the nmc3.rcf file.
4. Insert the flash drive into a USB port on your Rack Monitor 250.
5. Use the Web UI, the CLI, or the **Reset** button on the front of the Rack Monitor 250 to reboot the management interface. Wait for the reboot to finish.

Check that the update was completed successfully using the procedures in Verifying Upgrades and Updates, page 163.

# How To Update Multiple Rack Monitor 250s

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 the following:
  - Use the Firmware Update Utility, page 160, or
  - FAQ article FA156099: *How do I perform a mass firmware upgrade on APC network enabled products?* on www.se.com. To find an FAQ article on www.se.com, enter the title or number of the article in the search bar. On the resulting page, select **Faq** to narrow your search results to only FAQ articles.
- **Export configuration settings:** You can create batch files and use the .ini file utility to retrieve configuration settings from multiple Rack Monitor 250 and export them to other Rack Monitor 250. 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.se.com. To find an FAQ article on www.se.com, enter the title or number of the article in the search bar. On the resulting page, select **Faq** to narrow your search results to only FAQ articles.
  - Read the release notes (release notes are included with the utility file).
- **Use FTP or SCP to update multiple Rack Monitor 250s:** To update multiple Rack Monitor 250s using an FTP client or using SCP, write a script which automatically performs the procedure.

  **NOTE:** To find an FAQ article, go to www.se.com, and select you location. Then select **Support > Documentation & Software Downloads** and enter the article number or title of the FAQ in the Search bar.

# 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

You can verify the firmware version in the following ways:

- Check the Web UI under **About > Network**.
- Use the `nbabout` command in the CLI.
- Use an SNMP GET to the MIB II sysDescr OID.

# Downgrading Installed Firmware

Downgrading the firmware to a previous version is not supported in firmware v3.4.2.3 and newer.

# Troubleshooting

## Access Problems

For problems that persist or are not described here, contact the APC Customer Care at www.apc.com.

| Problem | Solution |
|---|---|
| Unable to ping the Rack Monitor 250 | The Rack Monitor 250 supports the ability to disable IPv4 Ping Response for security reasons. This setting is located in the Web UI under **Configuration > Security > Ping Response**. Ensure IPv4 Ping Response is enabled. Verify that other access methods such as HTTPS, FTP, Telnet, or SSH are enabled and functional.<br><br>If the Status LED is green, try to ping another node on the same network segment as the Rack Monitor 250. If that fails, it is not a problem with the Rack Monitor 250. If the Status LED is not green, or if the ping test succeeds, perform the following checks:<br>• Verify all network connections.<br>• Verify the IP addresses of the Rack Monitor 250 and the NMS.<br>• If the NMS is on a different physical network (or subnetwork) from the Rack Monitor 250, verify the IP address of the default gateway (or router).<br>• Verify the number of subnet bits for the subnet mask of the Rack Monitor 250 . |
| Cannot allocate the communications port through a terminal program | Before you can use a terminal program to configure the Rack Monitor 250, you must shut down any application, service, or program using the communications port. |
| Cannot access the CLI through a USB serial connection | • Make sure a USB A-USB mini B cable is connected to the correct USB port.<br>• Make sure that the baud rate is configured correctly: 9600, 81N. |
| Cannot access the CLI remotely | • 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 from each other.<br>• For SSH, the Rack Monitor 250 may be creating a host key. The Rack Monitor 250 can take up to one minute to create the host key, and SSH is inaccessible for that time. |
| Cannot access the Web UI | • Verify that HTTP or HTTPS access is enabled.<br>• Make sure you are specifying the correct URL — one that is consistent with the security system used by the Rack Monitor 250. SSL requires **https**, not **http**, at the beginning of the URL.<br>• Verify that you can ping the Rack Monitor 250.<br>• Verify that you are using a Web browser supported for the Rack Monitor 250. See Web User Interface, page 31.<br>• If the Rack Monitor 250 has just restarted and SSL/TLS security is being set up, the Rack Monitor 250 may be generating a server certificate. The Rack Monitor 250 can take up to one minute to create this certificate, and the SSL/TLS server is not available during that time. |

# SNMP Problems

| Problem | Solution |
|---|---|
| Unable to perform a GET | • Verify the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3).<br>• Use the CLI or Web UI to confirm that the NMS has access.<br>See SNMP Options, page 82. |
| Unable to perform a SET | • Verify that SNMP is enabled. SNMPv1 and SNMPv3 are disabled by default.<br>• Verify the read/write (SET) community name (SNMPv1) or the user profile configuration (SNMPv3).<br>• 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 SNMP Options, page 82. |
| Unable to receive traps at the NMS | • Make sure the trap type (SNMPv1 or SNMPv3) is correctly configured for the NMS as a trap receiver.<br>• 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.<br>• For SNMPv3, check the user profile configuration for the NMS, and run a trap test. See SNMP Options, page 82, , and SNMP Traps, page 54 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. |

# Specifications

## Appliance Specifications

| | |
|---|---|
| **Electrical** | |
| Input voltage, nominal, for AC Line Inlet | 100–240 VAC; 50/60 Hz |
| Maximum total current draw for AC Line Inlet | 10 A (defined by Switched Outlet load + 0.25 A) |
| Maximum output voltage for Switched Outlet | Defined by input voltage |
| Maximum output current for Switched Outlet | 10 A (defined by Switched Outlet load) |
| Voltage for Voltage Output contacts | 12 VDC, 24 VDC |
| Current for Voltage Output contacts | 75 mA total for 12 V and 24 V load |
| Current capacity of Relay Output contacts | 1 A, 30 V AC/DC (rated for Class 2 circuits only) |
| **Physical** | |
| Dimensions (H x W x D) | 43.6 x 431.8 x 59.2 mm (1.72 x 17.00 x 2.33 in.) |
| Weight | 1.26 kg (2.80 lb) |
| **Environmental** | |
| Elevation (above MSL)<br>Operating<br>Storage | <br>0 to 3000 m (0 to 10,000 ft)<br>0 to 15 000 m (0 to 50,000 ft) |
| Temperature<br>Operating<br>Storage | <br>0 to 45° C (32 to 113 °F)<br>-15 to 65 °C (5 to 149 °F) |
| Humidity<br>Operating<br>Storage | <br>10 to 95%, non-condensing<br>0 to 95%, non-condensing |
| **Compliance** | |
| EMC | • EN55032:2015/A11:2020 Class A, BS EN 55032:2015/A11:2020, Class A<br>• EN55035;2017/A11:2020, Class A, BS EN 55035:2017/A11:2020, Class A<br>• FCC Part 15, Subpart B, Class A Section 15.107 and 15.109<br>• ICES 003:Issue 7 Class A<br>• AS/NZS CISPR 32:2015 AMD 1:2020 Class A<br>• VCCI CISPR 32-1:2016-11, Class A |
| Safety | • cULus-EU<br>• CE<br>• UKCA<br>• CMIM<br>• PSE-UL<br>• RCM<br>• EAC |
| Wireless (NBWC100U) | • RED Directive 2014/53/EU<br>• FCC 47 CFR Part 15<br>• FCC ID: SNSNBWC100U<br>• ICES-003<br>• IC: 3351C-NBWC100U<br>• Japan Radio Law Article 38, Section 24(1)<br>• ANATEL 05272-16-10099 |

## System Specifications

| | |
|---|---|
| **A-Link** | |
| Maximum combined length of all A-Link cables | 1000 m (3,280 ft) |
| Maximum number of NetBotz Rack Sensor Pod150s that can be cascaded on the A-Link bus† | six (6) |
| Maximum number of sensors (Temperature/Humidity Sensors with Digital Display[AP9520TH]) that can be cascaded on theA-Link bus† | eight (8) |
| **Beacon** | |
| Maximum length of cable | 100 m (330 ft) |
| **NetBotz 0–5 V Sensor Cable (NBES0305)** | |
| Maximum length of cable | 30.48 m (100 ft) |
| **3.65 m (12 ft) Door Switch Sensor for APC Racks (NBES0303), 15.24 m (50 ft) Door Switch Sensor for Rooms or Third Party Racks (NBES0302)** | |
| User input response times | 200 mS |
| Maximum cable length | 30.48 m (100 ft) |
| Gap distance | Less than 2.54 cm (1 in) in air |
| **Dry Contact Cable (NBES0304)** | |
| User input response times | 200 mS |
| Maximum cable length | 30.48 m (100 ft) |
| **Temperature Sensor (AP9335T)** | |
| Temperature accuracy | ±1 ºC (± 2ºF), from 0 to 40ºC (32 to 104ºF) |
| Sensor operating temperature | –10 to 70ºC (14 to 159ºF) |
| Maximum length of cable | 15.2 m (50 ft) |
| **Temperature/Humidity Sensor (AP9335TH)** | |
| Temperature accuracy | ±1 ºC (± 2ºF), from 32 to 0 to 40ºC (104ºF) |
| Humidity accuracy | ± 4% RH, 20 to 90% RH, at 25ºC (77ºF)<br>± 8% RH, 30 to 80% RH, from 15 to 30ºC (59 to 95ºF) |
| Sensor operating temperature | –10 to 70ºC (14 to 159ºF) |

# Two-year Factory Warranty

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

## Terms of Warranty

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

## Non-transferable Warranty

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

## Exclusions

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

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

**IN NO EVENT SHALL APCSCHNEIDER ELECTRIC, ITS OFFICERS, DIRECTORS, AFFILIATES OR EMPLOYEES BE LIABLE FOR ANY FORM OF INDIRECT, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, ARISING OUT OF THE USE, SERVICE OR INSTALLATION, OF THE PRODUCTS, WHETHER SUCH DAMAGES ARISE IN CONTRACT OR TORT, IRRESPECTIVE OF FAULT, NEGLIGENCE OR STRICT LIABILITY OR WHETHER APCSCHNEIDER ELECTRIC HAS BEEN ADVISED IN ADVANCE**

**OF THE POSSIBILITY OF SUCH DAMAGES. SPECIFICALLY, APCSCHNEIDER ELECTRIC IS NOT LIABLE FOR ANY COSTS, SUCH AS LOST PROFITS OR REVENUE, LOSS OF EQUIPMENT, LOSS OF USE OF EQUIPMENT, LOSS OF SOFTWARE, LOSS OF DATA, COSTS OF SUBSTITUTES, CLAIMS BY THIRD PARTIES, OR OTHERWISE.**

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

# Warranty Claims

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

# Worldwide Customer Support

Support for this product is available at https://se.com/support.

# 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

© 2026 APC. All rights reserved.

TME14430