

NetBotz[®]

Rack Monitor 250

User Guide

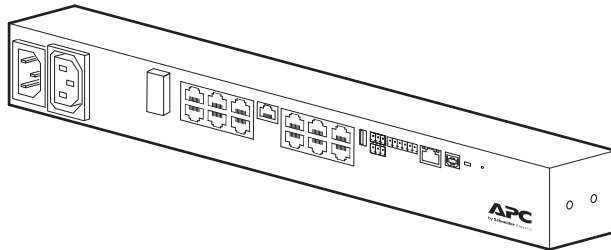
NBRK0250

NBACS125

NBACS1356

990-9890F

Publication Date: March 2019



APC by Schneider Electric Legal Disclaimer

The information presented in this manual is not warranted by APC by Schneider Electric to be authoritative, error free, or complete. This publication is not meant to be a substitute for a detailed operational and site specific development plan. Therefore, APC by Schneider Electric assumes no liability for damages, violations of codes, improper installation, system failures, or any other problems that could arise based on the use of this Publication.

The information contained in this Publication is provided as is and has been prepared solely for the purpose of evaluating data center design and construction. This Publication has been compiled in good faith by APC by Schneider Electric. However, no representation is made or warranty given, either express or implied, as to the completeness or accuracy of the information this Publication contains.

IN NO EVENT SHALL APC BY SCHNEIDER ELECTRIC, OR ANY PARENT, AFFILIATE OR SUBSIDIARY COMPANY OF APC BY SCHNEIDER ELECTRIC OR THEIR RESPECTIVE OFFICERS, DIRECTORS, OR EMPLOYEES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL, OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, CONTRACT, REVENUE, DATA, INFORMATION, OR BUSINESS INTERRUPTION) RESULTING FROM, ARISING OUT, OR IN CONNECTION WITH THE USE OF, OR INABILITY TO USE THIS PUBLICATION OR THE CONTENT, EVEN IF APC BY SCHNEIDER ELECTRIC HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. APC BY SCHNEIDER ELECTRIC RESERVES THE RIGHT TO MAKE CHANGES OR UPDATES WITH RESPECT TO OR IN THE CONTENT OF THE PUBLICATION OR THE FORMAT THEREOF AT ANY TIME WITHOUT NOTICE.

Copyright, intellectual, and all other proprietary rights in the content (including but not limited to software, audio, video, text, and photographs) rests with APC by Schneider Electric or its licensors. All rights in the content not expressly granted herein are reserved. No rights of any kind are licensed or assigned or shall otherwise pass to persons accessing this information.

This Publication shall not be for resale in whole or in part.

Table of Contents

Introduction	1
Types of User Accounts	2
Watchdog Features	2
Network interface watchdog mechanism	2
Resetting the network timer	2
Getting Started	3
Access	3
Automatic logout	3
Security lockout	3
Recover from a lost password	4
Command Line Interface.....	5
How to Access the CLI	5
Local access	5
Remote access through Telnet	6
Remote access through SSH	6
About the Main Screen	6
How to use the CLI	8
Command help syntax	8
Command response codes	9
Argument quoting	10
Escape sequences	10
Prompts for user input during command execution	10
Delimiter	10
Options and arguments inputs	11
Rack Monitor 250 System Command Descriptions	12
? or help	12
about	13
alarmcount	13
boot	14
bye, exit, or quit	14
cd	15
cipher	15
clrrst	17
console	17
date	18
delete	19
dir	19
dns	20
email	21
eventlog	22
exit	22
firewall	23
format	23
ftp	24
help	24
lang	25
lastrst	25
ledblink	25
logzip	26
netstat	26
ntp	27
ping	27
portSpeed	28

prompt	29
pwd	29
quit	29
radius	29
reboot	31
resetToDef	31
session	32
smtp	33
snmp	34
snmpv3	34
snmptrap	35
system	36
tcpip	37
tcpip6	38
user	39
userflt	40
web	41
whoami	42
xferINI	42
xferStatus	43
Rack Monitor 250 Device Command Descriptions	44
modbus	44
nbabout	45
nbbeacon	45
nboutlet	46
nbrack	47
nbrelay	48
nbsensor	48
spabout	51
spsensor	51
zw	54
zwsyslog	55
Web Interface	56
Access the Web Interface	56
Web Interface Features	57
Quick status links	57
Current session preferences	57
Help	57
Quick links	57
Limited Status Access	57
Display Menu Tree	58
Home Tab	59
NetBotz Alarms	60
Rack Access	60
Reset Alarms Link	60
Status Tab	61
View and Manage Wireless Sensors	61
View and Manage Wired Sensors	62
Filter wired sensors	63
Mass-configure sensor settings	64
Configure individual sensor settings	65
View and Manage Outputs	66
View Alarms	67

View the Network Status	68
Current IPv4 settings	68
Current IPv6 settings	68
Domain name system status	68
Port speed	68
Control Tab.....	69
Manage User Sessions	69
Reset/Reboot the Network Interface	69
View and Manage Outputs	70
Lock/Unlock Rack Access Handles	70
Configuration Tab.....	71
Configure Settings for an Appliance or Sensor Pod.....	71
Filter modules	71
Configure appliance settings	71
Configure Sensor Pod 150 settings	71
Configure Settings for Wired Sensors	72
Filter wired sensors	72
Mass-configure sensor settings	73
Configure individual sensor settings	74
Configure Wireless Sensors.....	75
The Wireless Sensor Network	75
Disable/Enable the Wireless Sensor Network	76
Add sensors to the Wireless Sensor Network	76
Modify wireless sensor settings	76
Configure Output Settings	77
Configure Rack Access	78
Register a new proximity card	78
Registered users	78
Unregistered users	79
User Authentication Methods	79
Rack access handles	80
Schedule automatic unlocking events	80
Configure Security	81
Session management settings	81
Ping response	81
Local users	82
Default settings	83
Remote users	84
Configure the RADIUS server	85
Configure a RADIUS server on UNIX® with shadow passwords	85
Supported RADIUS servers	86
Firewall.....	86
Enable/disable the firewall	86
Set the active policy	86
View active rules	86
Create/edit a policy	87
Import a firewall policy	88
Test a firewall policy	88

Configure Network Settings	89
TCP/IP Settings	89
Port speed	92
DNS server settings	92
Network configuration for web access	93
SSL certificate	94
Console	94
SNMPv1 configuration	95
SNMPv3 configuration	97
Enable Modbus	98
FTP server	99
Notification	99
Event actions	100
Configure event actions	100
E-mail notifications	102
SNMP trap receivers	104
SNMP traps test screen	104
General Options	105
Identification	105
Set the date and time	105
Use a configuration file (.ini)	106
Configure quick links	106
Syslog	107
Servers	107
Settings	108
Test	108
Tests Tab.....	109
LED Blink test	109
Logs Tab.....	110
Event Log	110
Color code the event log	110
Filter the event log	110
Delete the event log	111
Reverse lookup	111
Event log size	111
Data Log	112
Graph the data log	112
Data log collection interval	113
Configure data log rotation	113
Data log size	114
Use FTP or SCP to Retrieve Log Files	114
Use FTP to retrieve event.txt or data.txt	114
FTP delete	114
Use SCP to retrieve event.txt or data.txt	115
Firewall Log	115
About the Rack Monitor 250	116
Network	116
Support	116
Device IP Configuration Wizard.....	117
System requirements	117
Installation	117
How to Export Configuration Settings.....	118
Contents of the .ini file	118

Detailed Procedures	118
Use FTP to retrieve the .ini file	118
Customize the .ini file	119
Export the .ini file	119
The Upload Event and Error Messages	120
Errors generated by overridden values	120
Related Topics	120
CLI Script File (.csf) Settings	121
Firmware Upgrades	122
Firmware Module Files	122
Firmware File Transfer Methods	123
Use the Firmware Upgrade Utility on Windows systems	123
Use the Utility for Manual Upgrades, Primarily on Linux.	123
Use FTP to Upgrade the Rack Monitor 250	124
Use SCP to Upgrade the Rack Monitor 250	124
Use XMODEM to Upgrade the Rack Monitor 250	125
Use the Firmware Upgrade Utility for Multiple Upgrades on Windows	125
Verify Upgrades	126
Verify the Success of the Transfer	126
Last Transfer Result codes	126
Verify the Version Numbers of Installed Firmware	126
Wireless Firmware Upgrades	127
Troubleshooting	128
Rack Monitor 250 Access Problems	128
SNMP Issues	129
Source Code Copyright Notice	130

Introduction

The APC by Schneider Electric NetBotz[®] Rack Monitor 250 is a rack-mountable central hardware appliance for an environmental monitoring and control system. Once installed, you monitor and control your system using a network or serial connection.

The Rack Monitor 250 includes ports for connecting the following devices:

- Temperature and humidity sensors (with or without digital displays)
- Fluid detection sensors
- Third-party dry contact sensors
- Door switch sensors
- Rack door handles
- Smoke sensors
- Vibration sensors

You can expand your system in the following ways:

- Connect the Rack Monitor 250 to your building management system.
- Connect up to six NetBotz Rack Sensor Pod 150s and additional sensors.
- Add up to 47 sensors to the wireless sensor network.

See the *NetBotz Rack Monitor 250 Installation and Quick Configuration manual* on www.apc.com for more information.

The Rack Monitor 250 uses the following standards:

- 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)
- Network Time Protocol (NTP)

NOTE: The Rack Monitor 250 cannot be connected to or networked with any other NetBotz appliances, such as the Rack Monitor 570. It uses unique software that is not compatible with other NetBotz appliances.

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.

Types of User Accounts

The Rack Monitor 250 has various levels of access (Super User, Administrator, Device User, Read-Only User, and Network-Only User), which have user name and password requirements. Both user names and passwords are case-sensitive and have a 64 byte maximum, supporting up to 64 ASCII characters (fewer for multi-byte languages).

The Rack Monitor 250 is initially configured with three default user accounts: a Super User account, a Device account, and a Read only account. It is recommended that non-default user name and passwords be set for all users. You can create additional accounts for any type of user except the Super User.

- An **Administrator** or the **Super User** can use all of the menus in the Web UI and all of the commands in the CLI. The Super User and administrators can create, edit, and enable or disable other types of user accounts. Administrator user types can be deleted, but the **Super User** cannot be deleted.

The default user name and password for the **Super User** are both **apc**. The **Super User** cannot be renamed or deleted, but it can be disabled. It is recommended that the Super User account is disabled once any additional Administrator accounts are created. Make sure there is at least one Administrator account enabled before the Super User account is disabled.

- 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 grayed out.

The default user name for this account is **device**, and the default password is **apc**.

- A **Read-Only User** has access to the same menus as a Device User, but without the capability to change configurations, control devices, delete data, or use file transfer options. Links to configuration options are visible but 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** can only log on using the Web UI and CLI (Telnet or SSH). A user with network-only access has read/write permission to the network related menus only.

See "Local users" on page 86 for more information.

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 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 and restarts its network interface.

Resetting the network timer

To 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 that response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network and is on the same subnet. The network traffic of that computer will reset the 9.5-minute timer frequently enough to prevent the Rack Monitor 250 from restarting.

Getting Started

You must configure the following TCP/IP settings before the Rack Monitor 250 can operate on a network:

- IP address of the Rack Monitor 250
- Subnet mask
- IP address of the default gateway

NOTE: 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 that is usually running. The Rack Monitor 250 uses the default gateway to test the network when traffic is very light.

NOTE: Do not use the IPv4 loop back address (127.0.0.1), or the IPv6 loop back address (::1) as the default gateway address for the Rack Monitor 250. Doing so disables the appliance and requires you to reset TCP/IP settings to their defaults using a local serial login.

For more information on configuring the TCP/IP settings, see the *NetBotz Rack Monitor 250 Installation Manual* in printed form, or available as a PDF on www.apc.com.

Access

You can log on to the Rack Monitor 250 using the following methods:

- Local access to the Command Line Interface (CLI) from a computer with a direct serial connection.

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.

For more information, see the Frequently Asked Questions (FAQ) article FA158350. Go to www.apc.com. Navigate to **Support > Resources and Tools > FAQs**. Then enter the article number in the search bar.

- Telnet or Secure SHell (SSH) access to the CLI from a remote computer.
- Web access: either directly or through StruxureWare Data Center Expert®.

Automatic logout

By default, users are automatically logged out of the Rack Monitor 250 Web UI and CLI after 3 minutes of inactivity.

You can adjust the default logout time through the Web UI

1. Navigate to **Configuration > Security | Local Users > Management**.
2. Click the user name hyperlink for the account you want to change.
3. Under **Session Timeout**, modify the number of minutes.

Automatic Logout	Duration (min)
Default	3
Minimum	1
Maximum	60 (1 Hr)

Security lockout

If a valid user name is used with an invalid password consecutively, for the number of times specified in **Configuration > Security > Local Users > Default Settings**, the account will be locked until a Super User re-enables the account.

NOTE: A Super User cannot be locked out.

Recover from a lost password

1. Connect the USB A–USB mini B configuration cable to the console port on the Rack Monitor 250 and to a USB port of the computer.

NOTE: 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. For more information, see FAQ article FA158350 on www.apc.com.

2. Open a terminal program such as HyperTerminal or PuTTY, configure the port as follows, and press ENTER.

```
Default baud rate : 9600 bps
Data Bits         : 8
Parity            : None
Stop Bits         : 1
Flow Control      : None
```

3. Press ENTER on the computer, repeatedly, until the **User Name** prompt is displayed. If the **User Name** prompt is not displayed, verify the following:
 - The USB port is not in use by another application.
 - The terminal settings are correct.
 - The correct cable is being used.
 - SCROLL LOCK is not turned on.
4. Press and release the **Reset** button near the power LED once. The Status LED will turn off for 5–7 seconds, then flash rapidly orange and green. Press the **Reset** button a second time while the Status LED flashes to temporarily reset the user name and password to their default values (**apc/apc**).
5. Press ENTER as many times as necessary to display the **User Name** prompt, then use the default user name and password (**apc** and **apc**) to log on.

NOTE: If you take longer than 30 seconds to log on, you must repeat steps 4 and 5.

6. At the CLI, use the following commands to change the password setting for the Super User account, for which the user name is always **apc**, and the password is now temporarily **apc**:

```
user -n apc -pw yourNewSuperUserPassword
```

Example: to change the Super User's password to p@ssword type:

```
user -n apc -pw p@ssword
```

NOTE: Because the Super User can also reset the password for any account, you can reset other user's passwords as well.

Example: to change the password for user bmadmin to p@ssword type:

```
user -n bmadmin -pw p@ssword
```

NOTE: Changing user name information is not supported in the CLI. To change a user name, you must delete and re-create the user account. The Super User will also have access now to log in and adjust the password for any other user.

7. Type `quit`, `exit`, or `bye` to log off. Reconnect any USB cable you have disconnected, and restart any service you have disabled.

Command Line Interface

The Command Line Interface (CLI) is used primarily to view system status and issue commands to the system. Like DOS commands in Windows or the terminal session commands in Linux, the CLI handles word-like commands. These commands have parameters and options that can be specified at the CLI prompt (`apc>`).

How to Access the CLI

You can access the CLI locally using a USB A–USB mini B serial connection, or remotely using a secured Telnet or Secure Shell (SSH) connection. Telnet provides the basic authentication of a user name and password. SSH encrypts all transmitted data, including user name and password. Telnet is enabled by default. The interface, user accounts, and user access rights are the same whether you access the CLI through SSH or Telnet.

You must always provide an authentic user name and password to access the CLI. User names and passwords are case-sensitive.

User name prompt: "User Name : " (User<space>Name<space>:<space>).

Password prompt: "Password : " (Password<space><space>:<space>).

Local access

1. Connect the USB A–USB mini B configuration cable to the console port on the Rack Monitor 250 and to a USB port of the computer.

NOTE: 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, www.fidichip.com. For more information, see FAQ article FA158350 on www.apc.com.

2. Run a terminal program (HyperTerminal, etc.). Configure the port as follows, and press ENTER (repeatedly if necessary).

```
Default baud rate      : 9600 bps
Data Bits              : 8
Parity                 : None
Stop Bits              : 1
Flow Control           : None
```

4. At the prompts, enter user name and password.
5. At the end of the session, log off. Remember to reconnect any USB cable you may have disconnected.

Remote access through Telnet

1. Access a computer on the same network as the Rack Monitor 250.

Open a terminal program that provides telnet support or type "telnet" and the IP address of the Rack Monitor 250 at a DOS or command prompt and press ENTER.

Example:

```
telnet 139.225.6.133
```

NOTE: The Rack Monitor 250 uses Telnet port 23 by default. If the Rack Monitor 250 has been configured to use a non-default port number (between 5000 and 32768), you must include a colon or a space (depending on your Telnet client) between the IP address and the port number.

2. Enter user name and password. The default user name and password for the Super User are both **apc**.

Remote access through SSH

Data transmitted over SSH is encrypted using SSL (Secure Sockets Layer) encryption. To use SSH, you must install a properly configured SSH client on your computer.

About the Main Screen

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

Schneider Electric                Network Management Card AOS   vx.x.x
(c)Copyright 2018 All Rights Reserved NETBOTZ 250 App           vx.x.x
-----
Name      : apcxxxxxx                Date : 05/30/2018
Contact   : Don Adams                Time : 5:58:30
Location  : Building 3                User : Administrator
Up Time   : 0 Days 21 Hours 21 Minutes Stat : P+ N4+ N6+ A+
```

- Two fields identify the operating system (**Network Management Card AOS**) and Application Module (**NetBotz 250 App**) firmware versions.

```
Network Management Card AOS   vx.x.x
NetBotz 250 APP               vx.x.x
```

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

```
Name      : apcxxxxxx
Contact   : Don Adams
Location  : Building 3
```

- The **Up Time** is the duration since the last power cycle/reset of the Rack Monitor 250 network interface.

```
Up Time   : 0 Days 21 Hours 21 Minutes
```

- The two fields **Date** and **Time** identify when the screen was most recently refreshed.

Date : 05/30/2018

Time : 5:58:30

- The **User** field reports your log-in account type.

User : Administrator

- The **Stat** field reports the Rack Monitor 250 IPv4 & IPv6 status, and other system variables. See the Alarm Status Field table.

Stat : P+ N4+ N6+ A+

P+	The operating system (AOS) is functioning properly.
----	---

IPv4 only	IPv6 only	IPv4 and IPv6*	Description
N4+	N6+	N4+ N6+	IPv4 AND IPv6 Network Status. The network is functioning properly.
N4?	N6?	N4? N6?	A BOOTP request cycle is in progress.
N4-	N6-	N4- N6-	The Rack Monitor 250 failed to connect to the network.
N4!	N6!	N4! N6!	Another device is using the IP address of the Rack Monitor 250.

* 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 the AOS status is not P+, contact the APC by Schneider Electric Customer Care Center at www.apc.com/support even if you can still access the Rack Monitor 250.

How to use the CLI

At the command line interface, you can use commands to view and configure settings for the appliance. To use a command, type the command, option (if applicable), and any applicable arguments. Commands and arguments are not case sensitive. Options are case sensitive.

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

- Type `?` 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 `?` or the word `help`. For example, to view RADIUS configuration options, type:

```
radius ?
```

or

```
radius help
```

NOTE: See “Command help syntax” on page 8 for more detailed information.
- 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 typed in the command line.
- Type `exit`, `quit`, or `bye` to close the connection to the command line interface.

Command help syntax

When you use `?` or `help` to obtain information about a specific command, the following syntax defines how that command can be used:

Item	Description
-	Options are preceded by a hyphen.
[...]	If a command accepts multiple options or an option accepts mutually exclusive arguments, the values may be enclosed in brackets.
<...>	Angle brackets indicate user-entered text.
	A vertical line between items indicates that the items are mutually exclusive. You must use only 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. Type the `ftp` command, the port option, and the argument 5010:

```
ftp -p 5010
```
2. After the first command succeeds, type the `ftp` command, the enable/disable option, and the enable selection:

```
ftp -S enable
```

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

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

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

The command will fail if you type an argument that is not specified.

Command response codes

All CLI commands issue:

`<three digit response code>:<space>` (followed by a readable text (response message))

This can be followed by `<cr><lf>` and the output of the command (if applicable).

Example:

E000: Success (followed by the output of the command, if applicable)

These response codes allow automated processes to detect error conditions without having to match error message text.

Successful command operations have a response code 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`

Response Codes

Code	Message	Notes
E000	Success	N/A
E001	Successfully Issued	N/A
E002	Success, Reboot Required	N/A
E100	Command Failed	N/A
E101	Command Not Found	N/A
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	N/A
E104	User Level Denial	N/A
E105	Command Prefill	Not actually used in code, but it is set aside.
E106	Data Not Available	Or the provided data cannot be read.
E107	Serial Lost Communications	Serial communications with Rack Monitor 250 has been lost
E200	The provided arguments were invalid. To view 'command' help, type 'command ?'.	The command was recognized, but subsequent arguments were not.
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.	A read-only user was prevented from configuring the device.
E203	The target item is not configurable.	User failed to input a target or target was out of range.
E204	The requested operation cannot be completed with the device(s) specified.	The current hardware available does not allow the user input to be acted upon.
E205	System error: The requested operation could not be completed.	An 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.

Argument quoting

Argument values may optionally be enclosed in double quote characters (ASCII 0x22). String values beginning or ending with spaces, or containing commas or semicolons, must be enclosed in quotes for both input and output. Quote and backslash ("\", decimal code 92) characters appearing inside strings should NOT be encoded using traditional escape sequences (see Escape Sequences below).

All binary characters (ASCII decimal ranges 0..31, 127..159) that appear inside strings are treated as unreadable characters and rejected. When a quote or backslash character is supplied as a part of an input string, the input string must be enclosed in double quotes.

Escape sequences

Escape sequences, traditionally a backslash followed by a lower case letter or by a combination of digits, are ignored and should not be used to encode binary data or other special characters and character combinations.

The result of each escape sequence is parsed as if it were both a backslash and the traditionally escaped character.

Example:

```
<command> <arg1> [<agr2> <arg3a | arg3b> [<arg4a | arg4b | arg4c>]]  
- arg1 must be used, but arg2 - 4 are optional.  
- If arg2 is used, then arg3a or arg3b must also be used.  
- arg4 is optional, but arg1 - 3 must precede arg4.
```

With most commands, if the last argument is omitted, the command provides information, otherwise the last argument is used to change/set new information.

Example:

```
apc> ftp -p (displays the port number when omitting the arg2)  
  
E000: Success  
FTP Port:          5001  
  
apc> ftp -p 21 (sets the port number to arg2)  
E000: Success
```

Prompts for user input during command execution

Certain commands require additional user input (ex. transfer .ini prompting for baud rate). There is a fixed timeout of 1 minute for such prompts. If you do not enter any text within the timeout period, then the command prints E100: Command Failed. and the command prompt is redisplayed.

Delimiter

The Rack Monitor 250 CLI uses <space> (ASCII 0x20) as the delimiter between commands and arguments. Extra white space between commands and arguments is ignored.

Command responses have all fields delimited with commas for efficient parsing.

Options and arguments inputs

Entering a command with no options or arguments returns the current value of all options available from that command.

Entering the command and an option with no arguments returns the current value of that option only.

Any command followed by a question mark "?" returns help explaining the command.

```
<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>
```

Rack Monitor 250 System Command Descriptions

Courier font is used to show the user input or text output of the Rack Monitor 250. Text enclosed in '< >' is a user-defined variable.

? or help

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

Parameters: [<command>]

Example 1:

```
apc> ?
System Commands:
-----
For command help: command ?

?          about      alarmcount  boot        bye         cd
cipher     clrrst     console    date        delete     dir
dns        email      eventlog   exit        firewall   format
ftp        help       lang       lastrst     ledblink   logzip
netstat    ntp        ping       portspeed   prompt     pwd
quit       radius     reboot     resetToDef  session    smtp
snmp       snmptrap  snmpv3     system      tcpip      tctpip6
user       userdflt  web        whoami      xferINI    xferStatus

Device Commands:
-----
modbus     nbabout    nbbeacon   nboutlet    nbrack     nbrelay
nbsensor   spabout    spsensor   zw          zwsyslog
```

Example 2:

```
apc> help boot
Usage: boot -- Configuration Options
    boot [-b <dhcpBootp | dhcp | bootp | manual>] (IPv4 Boot Mode)
         [-c <enable | disable>] (Require DHCPv4 Cookie)
         [-v <vendor class>]
         [-i <client id>]
         [-u <user class>]
```

Error Message: E000, E102

about

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

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

Parameters: None

Example:

```
apc> about
E000: Success
Hardware Factory
-----
Model Number:          AP9XXX
Serial Number:         ST0913012345
Hardware Revision:     HW05
Manufacture Date:      6/23/2018
MAC Address:           00 05 A2 18 00 01
Management Uptime:    0 Days 1 Hour 42 Minutes
```

Error Message: E000

alarmcount

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

Description: Displays alarms present in the system.

Parameters:

Option	Argument	Description
-p	all	View the number of active alarms reported by the Rack 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.

Example:

To view all active warning alarms, type:

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

Error Message: E000, E102

boot

Access: Super User, Administrator

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

Parameters:

Option	Argument	Description
-b <boot mode>	dhcp bootp manual	Define how the TCP/IP settings will be configured when the Rack Monitor 250 turns on, resets, or restarts. See "TCP/IP Settings" on page 93 for information about each boot mode setting.
-c	enable disable (Require DHCP Cookie)	dhcp boot mode only. Enable or disable the requirement that the DHCP server provide the APC cookie.
-v	<vendor class>	Vendor Class is APC
-i	<client id>	The MAC address of the NMC, Which uniquely identifies it on the network.
-u	<user class>	The name of the application firmware module.

Example:

```
apc> boot
E000: Success

Boot Mode:          manual
DHCP Cookie:        enable
Vendor Class:        <device class>
Client ID:           XX XX XX XX XX XX
User Class:          <user class>
```

Error Message: E000, E102

bye, exit, or quit

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

Description: Exit from the CLI session.

Parameters: None

Example:

```
apc> exit
Bye
```

Error Message: None

cd

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

Description: Set the working directory of the file system. The working directory is set back to the root directory '/' when you log out of the CLI.

Parameters: <directory name>

Example:

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

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

Error Message: E000, E102

cipher

Access: Super User, Administrator

Description: Enable or disable cryptographic algorithms for Web UI sessions. You cannot enable or disable these algorithms directly from the Web UI. You must reboot your appliance after enabling or disabling algorithms for changes to take effect.

There are three categories of algorithms: Authentication algorithms, Block Cipher algorithms, and MAC algorithms. Available and Blocked Cipher Suites are also listed.

NOTE: Disabling the only algorithm will block all SSL/TLS sessions.

Parameters:

Option	Argument	Description
-3des	<enable disable>	Triple-DES
-aes	<enable disable>	AES
-dh	<enable disable>	DH
-rsake	<enable disable>	RSA Key Exchange
-rsaau	<enable disable>	RSA Authentication
-sha1	<enable disable>	SHA
-sha2	<enable disable>	SHA256
-ecdhe	<enable disable>	ECDHE

Example 1: Disable the triple-DES block cipher.

```
apc> cipher -3des disable
E002: Success
Reboot required for change to take effect.
```

Example 2: Retrieve a list of each available cryptographic algorithm and its status.

```
apc> cipher
E000: Success
Key Exchange Algorithms
-----
                DH                enabled
                RSA Key Exchange   enabled
                ECDHE              enabled

Authentication Algorithms
-----
                RSA Authentication  enabled

Cipher Algorithms
-----
                triple-DES          enabled
                AES                 enabled

MAC Algorithms
-----
                SHA                 enabled
                SHA256             enabled

Available Cipher Suites
-----
1      TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
2      TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
3      TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
4      TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
5      TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
6      TLS_DHE_RSA_WITH_AES_128_CBC_SHA
7      TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
8      TLS_DHE_RSA_WITH_AES_256_CBC_SHA
9      TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
10     SSL_RSA_WITH_3DES_EDE_CBC_SHA
11     TLS_RSA_WITH_AES_128_CBC_SHA
12     TLS_RSA_WITH_AES_256_CBC_SHA
13     TLS_RSA_WITH_AES_128_CBC_SHA256
14     TLS_RSA_WITH_AES_256_CBC_SHA256

Blocked Cipher Suites
-----
(the settings above disable the suites listed here)

None
```

Error Message: E000, E102

clrrst

Access: Super User, Administrator

Description: Clear reset reason.

Parameters: None

Example:

```
apc> clrrst
E000: Success
```

Error Message: E000

console

Access: Super User, Administrator

Description: Define whether users can access the CLI using Telnet, which is enabled by default, or Secure SHell (SSH), which 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 CLI.

Parameters:

Option	Argument	Description
-s	enable disable (ssh)	Enable or disable access to the CLI through SSH. Enabling SSH enables SCP.
-t	enable disable (telnet)	Disable or enable access to the CLI through Telnet.
-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 serial port connection (9600 bps by default).

Example 1:

To enable SSH access to the CLI, type:

```
apc> console -s enable
```

Example 2:

To change the Telnet port to 5000, type:

```
apc> console -pt 5000
Telnet:      enabled
SSH:         disabled
Telnet Port: 5000
SSH Port:    22
Baud Rate:   9600
```

Error Message: E000, E102.

date

Access: Super User, Administrator

Definition: Get and set the date and time of the system.

To configure an NTP server to define the date and time for the Rack Monitor 250, see “Set the date and time” on page 109.

Parameters:

Option	Argument	Description
-d	<"datestring">	Set the current date. The format must match the current -f setting.
-t	<00:00:00>	Set 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	Set 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 to specify your time zone. This lets you 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 July 1, 2018, type:

```
date -d "2018-07-01"
```

Example 3:

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

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

Error Message: E000, E100, E102

delete

Access: Super User, Administrator

Description: Delete a file in the file system.

Parameters:

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

Example:

```
apc> delete /event.txt
E000: Success
```

Error Messages: E000, E102

dir

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

Description: Displays the content of the working directory.

Parameters: None

Example:

```
apc> dir
E000: Success

--wx-wx-wx  1 apc      apc      3145728 Jun 23  2018 aos.bin
--wx-wx-wx  1 apc      apc      3145728 Jun 23  2013 app.bin
-rw-rw-rw-  1 apc      apc           45000 Jul  1  2018 config.ini
drwxrwxrwx  1 apc      apc           0 Mar 18  2018 ssl/
drwxrwxrwx  1 apc      apc           0 Mar 18  2018 ssh/
drwxrwxrwx  1 apc      apc           0 Mar 18  2018 logs/
drwxrwxrwx  1 apc      apc           0 Mar 18  2018 sec/
drwxrwxrwx  1 apc      apc           0 Mar 18  2018 dbg/
drwxrwxrwx  1 apc      apc           0 Mar 18  2018 fw1/
drwxrwxrwx  1 apc      apc           0 Mar 18  2018 rms/
```

Error Messages: E000

dns

Access: Super User, Administrator, Network-Only User

Definition: View or configure the manual Domain Name System (DNS) settings.

Parameters:

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

Example 1:

```
apc> dns -h
E000: Success
Host Name:           HostName
```

Example 2:

```
apc> dns -h myHostName
```

Error Message: E000, E102

email

Access: Super User, Administrator, Network-Only User

Description: Use the following commands to configure the parameters for email.

Parameters:

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

Example:

```
apc> email -o1 short
```

Error Message: E000, E102

eventlog

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

Key	Description
ESC	Close the event log and return to the CLI.
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: 04/23/2018 Time: 13:22:26
-----
T/H sensors: Normal      Outputs: Normal
Input Sensors: Normal

Date      Time      Event
-----
04/23/2018 13:17:22  apc CLI user `apc' logged in from
10.218.197.121
<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

Error Message: E000, E100

exit

See “bye, exit, or quit” on page 14.

firewall

Access: Super User, Administrator

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

Parameters:

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

Error Message: E000, E102

format

Access: Super User, Administrator

Description: Format the flash file system. This deletes all configuration data (including network settings), event and data logs, certificates and keys.

Parameters: None

Example:

```
apc> format
```

```
Format FLASH file system
```

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

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

```
apc>
```

Error Message: None

ftp

Access: Super User, Administrator, Network-Only User

Description: Get/set the FTP server configuration of the Network Interface, to allow/restrict FTP access.

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

Parameters:

Option	Argument	Definition
-p	<port number>	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. Valid port numbers are 21 and 5000–32768.
-S	enable disable	Configure access to the FTP server.

Example:

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

```
apc> ftp -p 5001
```

```
E000: Success
```

```
apc> ftp
```

```
E000: Success
```

```
Service: Enabled
```

```
Ftp Port: 5001
```

```
apc> ftp -p 21
```

```
E000: Success
```

Error Message: E000, E102

help

See “? or help” on page 12.

lang

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

Description: Language in use.

Parameters: None

Example: .

```
apc> lang
E000: Success
Languages
enUs - English
```

Error Message: E000

lastrst

Access: Super User, Administrator

Description: Last reset reason.

Parameters: None

Example:

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

Error Message: E000

ledblink

Access: Super User, Administrator

Description: Sets the blink rate to the LED on the Rack Monitor 250.

Parameters: <duration time in minutes>

Example:

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

Error Message: E000, E102

logzip

Access: Super User, Administrator

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

Parameters:

Option	Argument	Definition
-m	<email recipient>	Email recipient number (1-4).

Example:

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

Error Message: E000, E102

netstat

Access: Super User, Administrator, Network-Only User

Description: Displays active network addresses.

Parameters: None

Example: .

```
apc> netstat
Current IP Information:
Family  mHome Type      IPAddress                Status
IPv6    4      auto      FE80::2C0:B7FF:FE51:F304/64  configured
IPv6    0      manual    ::1/128                   configured
IPv4    0      manual    127.0.0.1/32              configured
```

Error Message: None

ntp

Access: Super User, Administrator, Network-Only User

Description: Synchronizes the time of the Network Interface to the time of the specified NTP server. The time is defined as Coordinated Universal Time (UTC), formerly Greenwich Mean Time. The timezone must be set correctly using the date command. See “date” on page 18.

Parameters:

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

Example 1:

To enable the override of manual setting, type:

```
apc> ntp -OM enable
```

Example 2:

To specify the primary NTP server, type:

```
apc> ntp -p 150.250.6.10
```

Error Message: E000, E102

ping

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

Description. Send a network ICMP message ('ping') to any external network device.

Parameters:

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

Example:

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

Error Message: E000, E100, E102

portSpeed

Access: Super User, Administrator, Network-Only User

Description: Get/set the network port speed.

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

Parameters:

Option	Arguments	Description
-s	auto 10H 10F 100H 100 F	Define the communication speed of the Ethernet port. The auto command lets the Ethernet devices negotiate to transmit at the highest possible speed. See "Port speed" on page 96 for more information about the port speed settings.
H = Half Duplex		10 = 10 Meg Bits
F = Full Duplex		100 = 100 Meg Bits

Example:

```
apc> portspeed
E000: Success
Port Speed: Auto_negotiation
Current Port Speed: 100 Full_Duplex
```

```
apc> portspeed -s 10h
E000: Success
```

```
apc> portspeed
E000: Success
Port Speed: 100 Half_Duplex
Current Port Speed: 100 Half_Duplex
```

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

Error Message: E000, E102

prompt

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

Description: Change the format of the prompt, either short or long

Parameters:

Option	Argument	Description
-s	long	The prompt includes the account type of the currently logged-in user.
	short	The default setting. The prompt is four characters long: 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, Network-Only User

Description: Used to output the path of the current working directory.

Parameters: None

Example:

```
apc> pwd
```

```
/
```

Error Message: None

quit

See “bye, exit, or quit” on page 14.

radius

Access: Super User, Administrator

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

Additional authentication parameters for RADIUS servers are available in the Web UI of the Rack Monitor 250.

For a summary of RADIUS server configuration and a list of supported RADIUS servers, see “Configure the RADIUS server” on page 89.

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

Parameters:

Option	Argument	Description
-a	local radiusLocal radius	Configure RADIUS authentication: local—RADIUS is disabled. Local authentication is enabled. radiusLocal—RADIUS, then Local Authentication. RADIUS and local authentication are enabled. Authentication is requested from the RADIUS server first. If the RADIUS server fails to respond, local authentication is used. radius—RADIUS is enabled. Local authentication is disabled.
-p1 -p2	<server port>	The server port of the primary or secondary RADIUS server. NOTE: RADIUS servers use port 1812 by default to authenticate users. The Rack Monitor 250 supports ports 1812, 5000 to 32768.
-o1 -o2	<server IP>	The IP address of the primary or secondary RADIUS server.
-s1 -s2	<server secret>	The shared secret between the primary or secondary RADIUS server and the Rack Monitor 250.
-t1 -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 existing RADIUS settings for the Rack Monitor 250, type `radius` and press ENTER:

```
apc> radius
E000: Success
Access:                               Local Only
Primary Server:                        0.0.0.0
Primary Server Port:                   1812
Primary Server Secret:                 <Password Hidden>
Primary Server Timeout:                 5
Secondary Server:                      0.0.0.0
Secondary Server Port:                 1812
Secondary Server Secret:               <Password Hidden>
Secondary Server Timeout:              5
```

Example 2:

To enable RADIUS and local authentication, type:

```
apc> radius -a radiusLocal
```

Example 3:

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

```
apc> radius -t2 10
```

Error Message: E000, E102

reboot

Access: Super User, Administrator, Network-Only User

Description: Restart the Rack Monitor 250 interface only. Forces the network device to reboot. You must confirm this operation by entering a “YES” after the command has been entered.

Parameters: None

Example:

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

Error Message: E000, E100

resetToDef

Access: Super User, Administrator

Description: Reset all parameters to their default.

Parameters:

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

Example:

To reset all of the configuration changes except the TCP/IP settings for the Rack Monitor 250, type:

```
apc> resetToDef -p keepip
Enter 'YES' to continue or <ENTER> to cancel : : <user enters 'YES'>
all User Names, Passwords.
Please wait...
Please reboot system for changes to take effect!
```

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	<session ID>	Delete session
-m	enable disable	Multi-User Enable
-a	enable disable	Remote Authentication Override

Example:

```
apc> session
```

```
User                Interface        Address                Logged In Time        ID
-----
apc                  Serial                00:00:05                1
```

Error Message: E000, E102

smtp

Access: Super User, Administrator

Description: Internet standard for electronic mail.

Parameters:

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

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: View the existing SNMPv1 settings, enable or disable SNMP, and configure basic SNMP parameters.

Parameters:

Option	Arguments	Description
-c	<Community>	Identify the group of Rack Monitor 250
-a	read write writeplus disable	Set the access level
-n	<IP or Domain Name>	The host's name or address
-S	enable disable	Enable or disable the respective version of SNMP

Example:

To change the name of SNMP access control community 3, enter:

```
apc> snmp -c3 myCommunity
E000: Success
```

Error Message: E000, E102

snmpv3

Access: Super User, Administrator, Network-Only User

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

Parameters:

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

Example:

To change the authentication protocol of SNMP access control 2 to SHA-1, type:

```
apc> snmpv3 -ap2 sha
E000: Success
```

Error Message: E000, E102

snmptrap

Access: Super User, Administrator, Network-Only User

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

Parameters:

Option	Arguments
-c{n}	<Community>
-r{n}	<Receiver NMS IP>
-l{n}	<language code>
-t{n}	snmpV1 snmpV3 (Trap Type)
-g{n}	enable disable (Trap Generation)
-a{n}	enable disable (Auth Trap)
-u{n}	profile1 profile2 profile3 profile4 (User Name)
n = Trap receiver # = 1,2,3,4,5 or 6	

Example:

To change the trap type of SNMP trap receiver 1 to SNMPv3, type:

```
apc> snmptrap -t1 snmpV3
E000: Success
```

Error Message: E000, E102

system

Access: Super User, Administrator

Description: View and set the system identification, contact, and location. View up time, date and time, the logged-on user, and the high-level system status P, N, A. See “About the Main Screen” on page 6 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. NOTE: These values are also used by StruxureWare Data Center Expert and the Rack Monitor 250's SNMP agent.
-c	<system-contact>	
-l	<system-location>	
-m	<system-message>	When defined, a custom message will appear on the log on screen for all users.
-s	enable disable	Enable or disable System-host name sync. This feature synchronizes the host name 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).

Example 1:

To set the device location as Test Lab, type:

```
system -l "Test Lab"
```

Example 2:

To set the system name as Rack 5, type:

```
system -n "Rack 5"
```

Error Message: E000, E102

tcpip

Access: Super User, Administrator, Network-Only User

Description: View and manually configure these network settings for the Rack Monitor 250.

Parameters:

Option	Argument	Description
-i	<IP 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.
-S	enable disable	Enable or disable IPv4.

Example 1:

To view the network settings of the Rack Monitor 250, type `tcpip` and press ENTER:

```
apc> tcpip
E000: Success

Active IPv4 Settings
-----
Active IPv4 Address:          10.150.60.232
Active IPv4 Subnet Mask:     255.255.255.0
Active IPv4 Gateway:        10.150.60.1

Manually Configured IPv4 Settings
-----
IPv4:                          enabled
Manual Settings:              disabled

IPv4 Address:                 0.0.0.0
Subnet Mask:                  0.0.0.0
Gateway:                      0.0.0.0
MAC Address:                  00 C0 B2 32 D7 7A
Domain Name:                  example.com
Host Name:                    apc52D270
```

Example 2: To manually configure an IP address of 150.250.6.10 for the Rack Monitor 250, type:

```
tcpip -i 150.250.6.10
```

Error Message: E000, E102

tcpip6

Access: Super User, Administrator, Network-Only User

Description: Enable IPv6 and 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. Do not use the loopback address (::1) as the default gateway.
-d6	router statefull statelss never	Set the DHCPv6 mode, with parameters of router controlled, statefull (for address and other information, they maintain their status), stateless (for information other than address, the status is not maintained), 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:         00 C0 B7 92 F2 71
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 Rack Monitor 250, type:

```
tcpip6 -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 configured users. You cannot edit a user name; you must delete it and then create a new user. For information on the permissions granted to each account type, see “Types of User Accounts” on page 2.

Parameters:

Option	Argument	Description
-n	<user>	Specify these options for a user.
-pw	<user password>	
-pe	<user permission>	
-d	<user description>	
-e	enable disable	Enable overall access.
-st	<session timeout>	Specify how long a session lasts waits before logging off a user when the keyboard is idle.
-sr	enable disable	Bypass RADIUS by using the serial console (CLI) connection, also known as Serial Remote Authentication Override
-el	enable disable	Indicate the Event Log color coding.
-lf	tab csv	Indicate the format for exporting a log file.
-ts	us metric	Indicate the temperature scale, fahrenheit or celsius.
-df	mm/dd/yyyy dd.mm.yyyy mmm-dd- yy dd-mmm-yy yyyy-mm-dd	Specify a date format.
-lg	<language code (e.g. enUs)>	Specify a user language.
-del	<user name>	Delete a user.
-l	no argument	Display the current user list.

Example:

To change the log off time for the user “jdoe” to 10 minutes, enter:

```
user -n jdoe -st 10
```

Error Message: E000, E102

userdfit

Access: Super User, Administrator

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

- Determine default values 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 values are used when a value is not provided by the authenticating server. For example, if a RADIUS server does not provide the user with a temperature preference, the value defined in this section will be used.

Parameters:

Options	Argument	Description
-e	enable disable	By default, user will be enabled or disabled upon creation.
-pe	<Administrator Device Read-Only Network-Only>	Specify the user's permission level and account type.
-d	<user description>	Provide a user description.
-st	<session timeout in minutes>	Provide a default session timeout.
-bl	<bad login attempts>	Number of incorrect login attempts a user has before the system disables their account. Upon reaching this limit, a message is displayed informing the user the account has been locked. The Super User or an Administrator-level account is needed to re-enable the account to allow the user to log back in. NOTE: A Super User account cannot be locked out, but can be manually disabled if necessary.
-el	enable disable	Enable or disable event log color coding.
-lf	tab csv	Specify the log export format, tab or CSV.
-ts	<us metrics>	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>	Specify the preferred date format.
-lg	<language code (enUs, etc)>	User language
-sp	enable disable	Strong password
-pp	<interval in days>	Required password change interval

Error Message: E000, E102

web

Access: Super User, Administrator, Network-Only User

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.
-s	enable disable	Enable or disable access to the user interface for HTTPS. When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate.
-mp	SSL3.0 TLS1.0 TLS1.1 TLS1.2	Specify the minimum HTTPS protocol to use.
-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.

Example 1:

To prevent all access to the Web UI, type:

```
web -s disable
```

Example 2:

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

```
apc> web
E000: Success

Service:      http
Http Port:    5000
Https Port:   443
```

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

Error Message: E000, E102

whoami

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

Description: Provides login information on the current user.

Parameters: None

Example:

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

Error Message: None

xferINI

Access: Super User, Administrator

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

- If there are any system or network changes, the CLI 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 Rack Monitor 250, you must reset the baud rate to the default to reestablish communication with the Rack Monitor 250.

Parameters: None

Example:

```
apc> xferINI
Enter 'YES' to continue or <ENTER> to cancel : <user enters 'YES'>
----- 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. See “Verify Upgrades” on page 130 for descriptions of the transfer result codes.

Parameters: None

Example:

```
apc> xferStatus
E000: Success
Result of last file transfer: Failure unknown
```

Error Message: E000

Rack Monitor 250 Device Command Descriptions

modbus

Access: Super User, Administrator

Description: View or configure modbus options.

Parameters:

Option	Argument	Definition
-a	enable disable	Enable or disable Modbus.
-br	9600 19200	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.
-s	<1 - F7>	Specify the Modbus slave address in hexadecimal.
-rDef	no argument	Restore default settings.
-tE	enable disable	Enable or disable Modbus TCP.
-tP		View the Modbus TCP port number.

Example 1:

To enable modbus, type:

```
modbus -a enable
```

Example 2:

To disable modbus, type:

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

apc> modbus
E000: Success

Slave Address = 0x1
Status = DISABLED
Baud Rate = 9600
Parity = EVEN (8, E, 1)
TCP Status = DISABLED
TCP Port Number = 502
```

Error Message: 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	Definition
-n	<new>	Set a name for the appliance (up to 20 characters).
-l	<new>	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:

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

Error Message: 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). Enter a <new> value (where applicable) to configure settings.

Parameters:

Option	Argument	Definition
-n	<new>	Set a name for the beacon (up to 20 characters).
-l	<new>	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 Message: E000, E200, E201, E202, E203, E204

nboutlet

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

Description: View information about the switched outlet. Enter a <new> value (where applicable) to configure settings.

Parameters:

Option	Argument	Definition
-n	<new>	Set a name for the outlet (up to 20 characters).
-l	<new>	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 Message: E000, E200, E201, E202, E203, E204

nbrack

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

Description: View or configure rack access information. Enter a <new> value (where applicable) to configure settings.

Parameters:

Option	Argument	Definition
-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 <new>]	Identify a registered user (1–200) and assign him or her a user name.
-rc	[1:200 <new>]	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 the door sensors.
-ls	[1:2 <locked unlocked>]	Set the state of the rack locks.
-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 Message: 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. Enter a <new> value (where applicable) to configure settings.

Parameters:

Option	Argument	Definition
-n	<new>	Set a name for the relay (up to 20 characters).
-l	<new>	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 Message: 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 (see the *Installation Manual* on www.apc.com for instructions to cascade sensors). 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). Enter a <new> value (where applicable) to configure settings.

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:

Option	Argument	Definition
-n	[1:14 <new>]	Set a name for the sensor (up to 20 characters).
-l	[1:14 <new>]	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).

Option	Argument	Definition
Temperature sensor thresholds.		
-t	[1:14]	View the current temperature.
-tmx	[1:14 <new>]	Set the maximum allowable temperature. If the temperature rises above this value, a critical alarm is generated.
-th	[1:14 <new>]	Set the threshold for the high temperature alarm. If the temperature rises above this value, a warning alarm is generated.
-tl	[1:14 <new>]	Set the threshold for the low temperature alarm. If the temperature goes below this value, a warning alarm is generated.
-tmn	[1:14 <new>]	Set the threshold for the minimum allowable temperature. If the temperature goes below this value, a critical alarm is generated.
-thy	[1:14 <new>]	Set hysteresis for temperature alarms. 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. All rate of change threshold violations result in critical alarms.		
-tlim	[1:14 <new>]	Set the maximum number of degrees the temperature can increase within a specified time before an alarm is generated.
-tlit	[1:14 <new>]	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 <new>]	Set the maximum number of degrees the temperature can decrease before an alarm is generated.
-tldt	[1:14 <new>]	Set the number of hours. If the temperature decreases too much within the time period you specify, an alarm is generated.
Short term rate of change thresholds: Set alarms to indicate a change in temperature or humidity over several minutes. All rate of change threshold violations result in critical alarms.		
-tsim	[1:14 <new>]	Set the maximum number of degrees the temperature can increase within a specified time before an alarm is generated.
-tsit	[1:14 <new>]	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 <new>]	Set the maximum number of degrees the temperature can decrease before an alarm is generated.
-tsdt	[1:14 <new>]	Specify a number of minutes. If the temperature decreases too much within the time period you specify, an alarm is generated.

Option	Argument	Definition
Humidity sensor thresholds.		
-h	[1:14]	View the humidity level.
-hmx	[1:14 <new>]	Set the maximum allowable humidity. If the humidity rises above this value, a critical alarm is generated.
-hh	[1:14 <new>]	Set the threshold for the high humidity alarm. If the humidity rises above this value, a warning alarm is generated.
-hl	[1:14 <new>]	Set the threshold for the low humidity alarm. If the humidity goes below this value, a warning alarm is generated.
-hmn	[1:14 <new>]	Set the threshold for the minimum allowable humidity. If the humidity goes below this value, a critical alarm is generated.
-hhy	[1:14 <new>]	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 high humidity threshold of 26% and a hysteresis value of 5, the clearing point for a high humidity alarm would be 21% (26 minus 5).

Example:

```
apc> nbsensor -n 1 New_Name
Old Name : Sensor NB:1
New Name : New_Name
E000: Success
```

Error Message: 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 sensor pod by its reference number (1-12). You can view the reference number on the LED display of your sensor pod. Enter a <new> value (where applicable) to configure settings.

Parameters:

Option	Argument	Definition
-n	[1:12 <new>]	Enter a name for the sensor pod (up to 20 characters).
-l	[1:12 <new>]	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 Message: 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 sensor 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). Enter a <new> value (where applicable) to configure settings.

Parameters:

Option	Argument	Definition
-n	[1:12 [1:6] <new>]	Set a name for the sensor (up to 20 characters).
-l	[1:12 [1:6] <new>]	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).

Option	Argument	Definition
Temperature sensor thresholds.		
-t	[1:12 [1:6]]	View the current temperature.
-tmx	[1:12 [1:6] <new>]	Set the maximum allowable temperature. If the temperature rises above this value, a critical alarm is generated.
-th	[1:12 [1:6] <new>]	Set the threshold for the high temperature alarm. If the temperature rises above this value, a warning alarm is generated.
-tl	[1:12 [1:6] <new>]	Set the threshold for the low temperature alarm. If the temperature goes below this value, a warning alarm is generated.
-tmn	[1:12 [1:6] <new>]	Set the threshold for the minimum allowable temperature. If the temperature goes below this value, a critical alarm is generated.
-thy	[1:12 [1:6] <new>]	Set hysteresis for temperature alarms. 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. All rate of change threshold violations result in critical alarms.		
-tlim	[1:12 [1:6] <new>]	Set the maximum number of degrees the temperature can increase within a specified time before an alarm is generated.
-tlit	[1:12 [1:6] <new>]	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] <new>]	Set the maximum number of degrees the temperature can decrease before an alarm is generated.
-tldt	[1:12 [1:6] <new>]	Set the number of hours. If the temperature decreases too much within the time period you specify, an alarm is generated.
Short term rate of change thresholds: Set alarms to indicate a change in temperature or humidity over several minutes. All rate of change threshold violations result in critical alarms.		
-tsim	[1:12 [1:6] <new>]	Set the maximum number of degrees the temperature can increase within a specified time before an alarm is generated.
-tsit	[1:12 [1:6] <new>]	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] <new>]	Set the maximum number of degrees the temperature can decrease before an alarm is generated.
-tsdt	[1:12 [1:6] <new>]	Specify a number of minutes. If the temperature decreases too much within the time period you specify, an alarm is generated.

Option	Argument	Definition
Humidity sensor thresholds.		
-h	[1:12 [1:6]]	View the humidity level.
-hmx	[1:12 [1:6] <new>]	Set the maximum allowable humidity. If the humidity rises above this value, a critical alarm is generated.
-hh	[1:12 [1:6] <new>]	Set the threshold for the high humidity alarm. If the humidity rises above this value, a warning alarm is generated.
-hl	[1:12 [1:6] <new>]	Set the threshold for the low humidity alarm. If the humidity goes below this value, a warning alarm is generated.
-hmn	[1:12 [1:6] <new>]	Set the threshold for the minimum allowable humidity. If the humidity goes below this value, a critical alarm is generated.
-hhy	[1:12 [1:6] <new>]	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 high humidity threshold of 26% and a hysteresis value of 5, the clearing point for a high humidity alarm would be 21% (26 minus 5).

Example:

```
apc> spsensor -n 2 New_Name
Old Name : Sensor SP 06:2
New Name : New_Name
E000: Success
```

Error Message: E000, E200, E201, E202, E203, E204

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. Enter a <new> value (where applicable) to configure settings.

Parameters:

Option	Argument	Definition
-c	no argument	View the number of commissioned sensors.
-ch	[1:48]	View the wireless channel of the sensor.
-n	[1:48 <new>]	View or configure sensor name (up to 20 characters).
-l	[1:48 <new>]	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.
-s	[1:48]	View the signal strength.
-sl	[1:48 <new>]	Set the threshold for low signal strength. If the signal strength goes below this value, an alarm is generated.
-smn	[1:48 <new>]	Set the threshold for the minimum allowable signal strength. If the signal strength goes below this value, an alarm is generated.
-b	[1:48 <new>]	View the battery voltage.
-bl	[1:48 <new>]	Set the low battery threshold. If the battery voltage drops below this threshold, an alarm is generated.
-bmn	[1:48 <new>]	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 settings		
-t	[1:48]	View the temperature.
-tmx	[1:48 <new>]	Set the threshold for the maximum allowable temperature. If the temperature rises above this value, an alarm is generated.
-th	[1:48 <new>]	Set the high temperature threshold. If the temperature rises above this threshold, an alarm is generated.
-tl	[1:48 <new>]	Set the low temperature threshold. If the temperature drops below this threshold, an alarm is generated.
-tmn	[1:48 <new>]	Set the threshold for the minimum allowable temperature. If the temperature drops below this value, an alarm is generated.

Option	Argument	Definition
Humidity settings		
-h	[1:48]	View the humidity.
-hmx	[1:48 <new>]	Set the threshold for the maximum allowable humidity. If the humidity rises above this value, an alarm is generated.
-hh	[1:48 <new>]	Set the high humidity threshold. If the humidity rises above this threshold, an alarm is generated.
-hl	[1:48 <new>]	Set the low humidity threshold. If the humidity drops below this threshold, an alarm is generated.
-hmn	[1:48 <new>]	Set the threshold for the minimum allowable temperature. If the humidity drops below this value, an alarm is generated.

Example:

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

Error Message: 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 APC by Schneider Electric support.

NOTE: You must configure a syslog server on the Rack Monitor 250 to use the zwsyslog command. See “Servers” on page 111 for instructions to configure a syslog server.

Parameters:

Option	Argument	Definition
-d	enable disable	Enable: Enable forwarding of SDP over Syslog. Disable: Disable forwarding of SDP over Syslog.

Example:

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

Error Message: E000, E102

Web User Interface

The Web User Interface (Web UI) provides options to view the status and manage the Rack Monitor 250.

Modern Web browsers are compatible with the Rack Monitor 250 Web UI. Use the most recent version of your browser to mitigate the risk of software security vulnerabilities.

Access the Web UI

To access the Rack Monitor 250 in a Web browser, you must disable any proxy server services. Access to the Rack Monitor 250 through a proxy server is not available at this time. If a proxy server is required, it must be configured so the IP address of the Rack Monitor 250 is not proxied.

Type the IP address of the Rack Monitor 250 in the Web browser's address field:

- For an IP address of 139.225.6.133, when the Rack Monitor 250 uses the default port (80), enter:
`http://139.225.6.133` if HTTP is your access mode.
`https://139.225.6.133` if HTTPS is your access mode.
- For a System IP address of 139.225.6.133, when the Rack Monitor 250 uses a non-default port (5000, in this example), enter:
`http://139.225.6.133:5000` if HTTP is your access mode.
`https://139.225.6.133:5000` if HTTPS is your access mode.
- If your DNS system has been configured with entries for the Rack Monitor 250 (Web1 in this example), enter:
`http://Web1` if HTTP is your access mode.
`https://Web1` if HTTPS is your access mode.

Web UI Features

When you log on to the Rack Monitor 250 Web UI, a quick status area in the top right displays information about the system. Click the headings in the menu bar to display popup menus listing related options.

Quick status links

The Quick Status area in the upper right corner of every screen displays the number and severity of active alarms. Click any Quick Status icon to return to the home screen.



Blue “informational” icon



Green “device operating normally” icon



Yellow “Attention required” warning icon



Red “Alarm detected” critical icon

Current session preferences

Click the user name link to access your user preferences. Go to **Configuration > Security > Local Users > Management** for more user settings.

Help

Click **Help** in the upper right corner to view context-sensitive information.

Quick links

There are three user configurable links on the lower left of each page. By default, the links access the following Web pages:

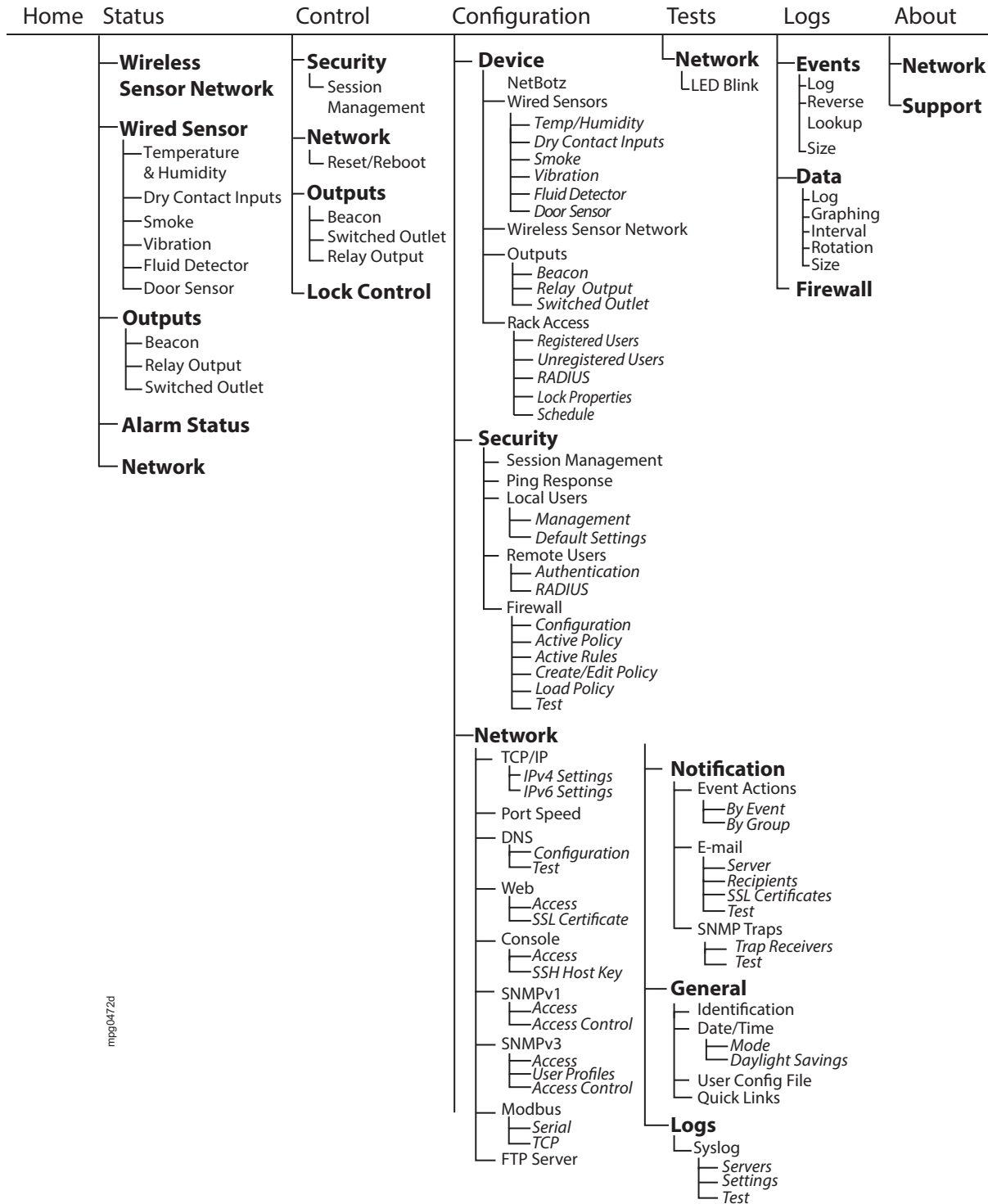
- **Link 1:** Website homepage
- **Link 2:** Demonstrations of web-enabled products
- **Link 3:** Information on Schneider Electric Remote Monitoring Services

Limited Status Access

The Limited Status Access option provides a read-only, public Web page with basic device status without requiring you to log on. This feature is disabled by default. Go to **Configuration > Network > Web > Access** to enable it. Check the **Use as default page** box to display this device status page instead of the log on screen when you access the device with only its IP address or host name. To log on to the device from the device status page, use the **Log On** link on the menu bar.

Otherwise, when only the Limited Status Access option is enabled, click the **Limited Status** hyperlink on the log on screen in the lower left corner to access the basic device status screen.

Display Menu Tree



mjpg0472d

Home Tab

Home is the default page when you log on. To change the login page to a different page, go to that page, then click the green pushpin at the top right side of the browser window.

NetBotz 250
Rack Monitor

apc | English | Log Off | Help |

Home Status Control Configuration Tests Logs About

Home

Door Sensors
2 Connected
No Alarms Present [More >](#)

Beacon
Beacon NB: Off [More >](#)

Relay Output
Relay: Open [More >](#)

Switched Outlet
Outlet: Off [More >](#)

Rack Access
No Alarms Present

	Status	Lock	Handle	Door
Door 1	Secure	Locked	Open	Closed
Door 2	Secure	Locked	Closed	Closed

[Lock Control >](#)

Recent Device Events

Date	Time	Event
08/07/2018	14:24:28	Door 2 locked from Unknown access.
08/07/2018	14:24:28	Door 2 communications established.
08/07/2018	14:24:27	Door 1 locked from Unknown access.
08/07/2018	14:24:27	Door 1 communications established.
08/07/2018	14:24:27	Wireless coordinator communication restored.

[More Events >](#)

APC's Web Site | Testdrive Demo | APC Monitoring

© 2018, Schneider Electric. All rights reserved.
Site Map | Updated: 08/08/2018 at 07:44

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

A maximum of ten alarms is displayed for each device. Recent Device Events displays the last five device events. View the Alarm Status page to see all alarms for all connected devices, or the Event Log to see all device events.

NetBotz Alarms

View alarms for modules. (This area appears only if a module is in an alarm state.)

For the following sensor types, view the number of connected sensors and their status. Click **More** to view all connected sensors of this type. Click the name of each sensor to view its settings.

- Wireless sensors
- Temperature & humidity sensors
- Dry contact input sensors
- Vibration sensors
- Smoke sensors
- Fluid detector
- Door sensors

For the following sensor types, click the name of the sensor to view its settings.

- Beacon
- Output relay
- Switched outlet

Rack Access

View the status of Door 1 and Door 2. Click the link to control the lock:

- **Status:** Secure or not secure
- **Lock:** Locked or unlocked
- **Handle:** Open or closed
- **Door:** Open or closed

Click **Lock Control** to control the lock.

Reset Alarms Link

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.

Status Tab

On these pages, you can view detailed information about wireless sensors, wired sensors, outputs, alarms, and current network settings. You can also configure settings for sensors and outputs.

View and Manage Wireless Sensors

Path: Status > Wireless Sensor Network

View all connected wireless temperature and temperature/humidity sensors.

Setting	Description
Status	Critical (device requires immediate attention), Warning (attention required), and Normal . By default, all information is sorted by Status. To sort by another column heading, click its name.
Name	Name of the monitored device (up to 20 characters). Click a sensor name to configure the device.
Extended Address	The extended address (MAC) of each sensor in the wireless network.
Location	The location of each sensor in the wireless network (up to 20 characters).
Type	The sensor type of each sensor in the wireless network.
Temperature	The temperature reading on each sensor in the wireless network.
Humidity	The humidity reading on each sensor in the wireless network.
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 in the wireless network.

You can also select a sensor by its **Name** to edit settings for that sensor:

Setting	Description
Name	Enter a name (up to 20 characters).
Extended Address	The extended address (MAC) of the wireless sensor.
Location	Enter the location of the sensor (up to 20 characters).
Alarm Generation	Enable or disable. When Alarm Generation is disabled, the system continues to monitor the state of the sensor, but does not generate an alarm. Alarms are not recorded in the event log when Alarm Generation is disabled.
Temperature/ Humidity Thresholds	<ul style="list-style-type: none">• Maximum: The maximum allowable value. If the temperature or humidity rises above this value, a critical alarm is generated.• High: If the temperature or humidity rises above this value, a warning alarm is generated.• Low: If the temperature or humidity falls below this value, a warning alarm is generated.• Minimum: The minimum allowable value. If the temperature or humidity falls below this value, a critical alarm is generated.
Battery/Signal Thresholds	<ul style="list-style-type: none">• Low: If the battery voltage or signal strength drops below its low threshold for the sensor, an alarm occurs.• Minimum: If the battery voltage or signal strength drops below its minimum threshold for the sensor, an alarm occurs.

View and Manage Wired Sensors

Path: Status > Wired Sensor > Sensor Type

On these pages, you can view information for all sensors, create a filter to show only specific sensors, use the mass configuration feature to configure all sensors on a page, or configure individual sensor settings.

All wired sensors display the following information:

Setting	Description
Status	Critical (device requires immediate attention), Warning (attention required), and Normal . By default, all information is sorted by Status.
Name	Select a sensor name to configure the sensor settings.
Location	The location of each sensor.
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.

Each wired sensor type displays additional information. Select the sensor name to configure its settings.

Setting	Description
Temperature and Humidity	
Temperature	Temperature of the air surrounding the sensor. To change the temperature units for this user session only, click the thermometer icon. To change the temperature units for the current and future sessions for one user, select Configuration > Security > Local Users > Management . Select the user, then Temperature Scale . To change the temperature units for the current and future sessions for all users, select Configuration > Security > Local Users > Default Settings , then select Temperature Scale .
Humidity	Relative humidity of the air surrounding the sensor.
Dry Contact Inputs State	Open/Low or Closed/High
Smoke State	No Smoke, or Smoke Detected
Vibration State	No Vibration, or Vibration Detected
Fluid Detector State	No Fluid, or Fluid Detected
Door Sensor State	Open or closed

Filter wired sensors

Show only sensors that meet the criteria of your filter. Sensors that do not match all selected criteria will not be shown. Select **Create Filter**, then enter one or more filter settings.

Setting	Description
Status	Select one or more alarm statuses. Critical: Critical alarm Warning: Warning alarm Information: Informational alarm Normal: No alarm
State	Select the current state of the sensor.
Name	Enter the name of the sensor (up to 20 characters). Then select filter parameters: <ul style="list-style-type: none">• Case Sensitive: Select to make the filter case sensitive.• Whole Word: Include only complete word matches. If this is not selected, the filter will include partial word matches.
Location	Enter a sensor location. Then select filter parameters: <ul style="list-style-type: none">• Case Sensitive: Select to make the filter case sensitive.• Whole Word: Include only complete word matches. If this is not selected, the filter will include partial word matches.
Module Name	Filter by the appliance or sensor pod that sensors are attached to. Enter the Module Name of an appliance or sensor pod, and select filter parameters: <ul style="list-style-type: none">• Case Sensitive: Select to make the filter case sensitive.• Whole Word: Include only complete word matches. If this is not selected, the filter will include partial word matches.
Temperature	Enter a temperature value. From the drop down list, select whether to view sensors that detect a temperature Less Than , Equal To , or Greater Than that value.
Humidity	Enter a humidity value. From the drop down list, select whether to view sensors that detect a humidity Less Than , Equal To , or Greater Than that value.

You can select **Clear Filter** to remove the filter, or you can create a new filter to override the previous one.

Mass-configure sensor settings

Change the settings for all sensors of a certain type at once.

Select **Mass Configuration**, then select the settings you want to configure. Then click **Next** to configure those settings. Available settings depend on the type of device.

Setting	Description
General	<ul style="list-style-type: none"> • Name: The name of the sensor • Location: The location of the sensor <p>Enter up to 20 characters in each field. You can use these wild cards:</p> <ul style="list-style-type: none"> • %m: the parent module ID • %p: the sensor port number • %l: the parent module location
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.
Severity	Select the severity of alarms generated for these sensors. Alarm severities for temperature and humidity sensors are not editable.
Normal State	Select the normal state of the sensor. An alarm is generated when the sensor changes to an abnormal state.
Alarm Generation	When Alarm Generation is disabled, the system continues to monitor the state of the sensors, but does not generate alarms. Alarms are not recorded in the event log when Alarm Generation is disabled.
Temperature/Humidity Thresholds	<ul style="list-style-type: none"> • Maximum: The maximum allowable value. If the temperature or humidity rises above this value, a critical alarm is generated. • High: If the temperature or humidity rises above this value, a warning alarm is generated. • Low: If the temperature or humidity falls below this value, a warning alarm is generated. • Minimum: The minimum allowable value. If the temperature or humidity falls below this value, a critical alarm is generated. • Hysteresis: This value specifies how far above or below a threshold the temperature or humidity must return to clear a threshold violation. <p>For Maximum and High threshold violations, the clearing point is the threshold minus the hysteresis. For Minimum and Low threshold violations, the clearing point is the threshold plus the hysteresis.</p>
Rate Of Temperature Change	<p>Configure the acceptable short-term and long-term changes in temperature. When the rate of change is exceeded, the appliance generates a critical alarm.</p> <ul style="list-style-type: none"> • S.T. Increase: Short-term temperature increase • L.T. Increase: Long-term temperature increase • S.T. Decrease: Short-term temperature decrease • L.T. Decrease: Long-term temperature decrease • Reset Rate Alarms: Clear all existing rate of change alarms.

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

Configure individual sensor settings

Path: Configuration > Device > Wired Sensor > Sensor Type

Select a sensor's name to configure its settings. Available settings vary by sensor type.

Setting	Description
General	<ul style="list-style-type: none"> • Name: The name of the sensor • Location: The location 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.
Severity	Select the severity of alarms generated for these sensors. Alarm severities for temperature and humidity sensors are not editable.
Normal State	Select the normal state of the sensor. An alarm is generated when the sensor changes to an abnormal state.
Alarm Generation	When Alarm Generation is disabled, the system continues to monitor the state of the sensors, but does not generate alarms. Alarms are not recorded in the event log when Alarm Generation is disabled.
Temperature/Humidity Thresholds	<p>Select Threshold Settings to set the following threshold values for temperature and humidity:</p> <ul style="list-style-type: none"> • Maximum: The maximum allowable value. If the temperature or humidity rises above this value, a critical alarm is generated. • High: If the temperature or humidity rises above this value, a warning alarm is generated. • Low: If the temperature or humidity falls below this value, a warning alarm is generated. • Minimum: The minimum allowable value. If the temperature or humidity falls below this value, a critical alarm is generated. • Hysteresis: This value specifies how far above or below a threshold the temperature or humidity must return to clear a threshold violation. For Maximum and High threshold violations, the clearing point is the threshold minus the hysteresis. For Minimum and Low threshold violations, the clearing point is the threshold plus the hysteresis.
Rate Of Temperature Change	<p>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.</p> <ul style="list-style-type: none"> • S.T. Increase: Short-term temperature increase • L.T. Increase: Long-term temperature increase • S.T. Decrease: Short-term temperature decrease • L.T. Decrease: Long-term temperature decrease • Reset Rate Alarms: Clear all existing rate of change alarms.

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

View and Manage Outputs

Path: Status > Outputs > Output type

Select an output (Beacon, Output Relay, and Switched Outlet). Devices connected to these outputs are controlled by the output settings.

The following information is shown for all outputs:

Setting	Description
Module Name	Name of Module to which the output is connected.
Module Location	Location of Module to which the output is connected, the Rack Monitor 250 or the Sensor Pod 150. 'Unknown' if no location is configured.
Alarm Status	Critical (device requires immediate attention), Warning (attention required), and Normal. By default, all information is sorted by Status. To sort by another column heading, click its name.

You can configure the following settings for each output:

Setting	Description
Name	Enter a name for the output (up to 20 characters).
Location	Enter the location of the sensor (up to 20 characters).
Normal State	Set the normal state of the output (excluding the beacon): On/Off or Open/Closed
Control	Change the state of the output to On/Off or Open/Closed.
Alarm Mapping	The beacon, output relay and switched outlet can be activated by alarm states of sensors on the NetBotz module only. <ol style="list-style-type: none">1. Select one or more alarm states that will change the state of the output.2. By default, each sensor connected to the NetBotz module is mapped to activate the output when the sensor is in an abnormal state. Click the name of the alarm state to view the sensors connected to the module.3. Select sensors to include in the alarm. Any selected sensor, in its abnormal state, activates the output.

NOTE: The Output pages under the Status, Control, and Configuration menus are the same, and contain all the tasks for each menu option.

View Alarms

Path: Status > Alarm Status

The Alarm Status page displays the alarm status of system devices: **Critical** (device requires immediate attention), **Warning** (attention required), or **Normal** (no alarms present).

Setting	Description
Module Alarms	View alarms for modules. (This area appears only if aRack Monitor 250 or Sensor Pod 150 module is in an alarm state.)
Wireless Sensors	View the number of connected sensors and their status. Click the name of a sensor in the alarm state to view its settings.
Temperature & Humidity Sensors	View the number of connected sensors and their status. Click the name of a sensor in the alarm state to view its settings.
Dry Contact Input Sensors	View the number of connected sensors and their status. Click the name of a sensor in the alarm state to view its settings.
Vibration Sensors	View the number of connected sensors and their status. Click the name of a sensor in the alarm state to view its settings.
Smoke Sensors	View the number of connected sensors and their status. Click the name of a sensor in the alarm state to view its settings.
Fluid Detector	View the number of connected sensors and their status. Click the name of a sensor in the alarm state to view its settings.
Beacon	View the status of the beacon. Click the name of the beacon to view its settings.
Relay Output	View the status of the relay output. Click the name of the relay output to view its settings.
Switched Outlet	View the status of the switched outlet. Click the name of the switched outlet to view its settings.
Rack Access	View the status of Door 1 and Door 2: <ul style="list-style-type: none">• Status: Secure or not secure• Lock: Locked or unlocked• Handle: Open or closed\• Door: Open or closed
Reset Alarms link	If communication with a device is lost, or a temperature sensor's rate-of-change is exceeded, the Reset Alarms link appears. Click the link to clear the alarm if, for example, you intentionally disconnected a sensor, or you want to acknowledge a rate of change alarm.

View the Network Status

Path: Status > Network

Network Status provides an overview of critical network status information, including current IPv4 and IPv6 settings, DNS status, and port speed.

You can configure network settings on the **Configuration > Network** pages.

Current IPv4 settings

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

Current IPv6 settings

Setting	Description
Type	How the IPv6 settings are assigned.
IP Address	The IP address of the unit.
Prefix Length	The range of addresses for the sub-network.

Domain name system status

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

Port speed

Current Speed: The current speed assigned to the Ethernet port.

Control Tab

You can use these pages to manage user sessions, reset the network interface, view and manage outputs, and manually control rack access handles.

Manage User Sessions

Path: Control > Security > Session Management

NetBotz 250
Rack Monitor

apc | English | Log Off | Help

Home Status Control Configuration Tests Logs About

Current Sessions

Session Management			
User	Interface	Address	Logged In Time
apc	Web	10.218.125.126	00:13:32

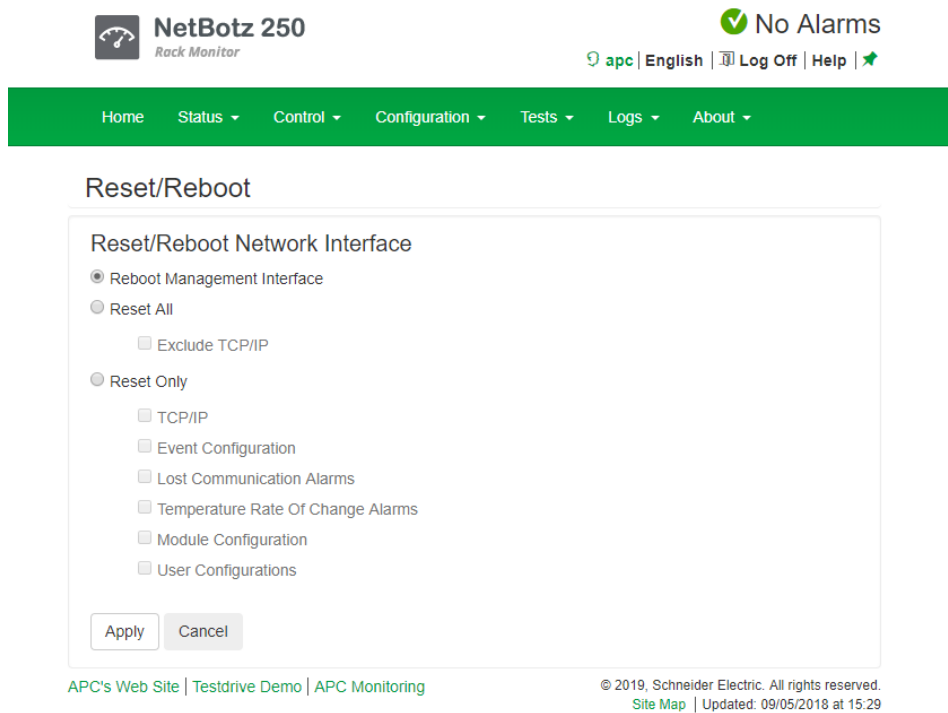
APC's Web Site | Testdrive Demo | APC Monitoring

© 2019, Schneider Electric. All rights reserved.
Site Map | Updated: 09/05/2018 at 15:10

This page lists all of the currently logged in users, the interface from which they are logged in, their IP addresses, and the amount of time they have been logged in. To terminate a specific user session, with the appropriate authority, select the user name and click **Terminate**.

Reset/Reboot the Network Interface

Path: Control > Network > Reset/Reboot



Action	Description
Reboot Management Interface	Restarts the device's network interface without turning off and restarting the device itself.
Reset All	<ul style="list-style-type: none"> • If you do not select "Exclude TCP/IP," all configured values and settings are reset to their default values, including the setting that determines how this device must obtain its TCP/IP configuration values. The default is DHCP. • If you select "Exclude TCP/IP," all configured values and settings, except the setting that determines how this device must obtain its TCP/IP configuration values, are reset to their default values.
Reset Only	<p>Select one or more of the following options:</p> <ul style="list-style-type: none"> • TCP/IP: Resets only the setting that determines how this device must obtain its TCP/IP configuration values. The default is DHCP. • Event Configuration: Resets events to their default configuration. Any specially configured event or group will also revert to the default value. • Lost Communication Alarms: Clears lost communication alarms if, for example, you intentionally disconnected a sensor. • Temperature Rate of Change Alarms: Clears temperature rate of change alarms to acknowledge a rate of change. • Module Configuration: Resets the to its default configuration. • User Configurations: Resets all users to their default configuration.

View and Manage Outputs

Path: Control > Outputs

Select an output (Beacon, Output Relay, and Switched Outlet). Devices connected to these outputs are controlled by the output settings.

The following information is shown for all outputs:

Setting	Description
Module Name	Name of Module to which the output is connected.
Module Location	Location of Module to which the output is connected, the Rack Monitor 250 or the Sensor Pod 150. 'Unknown' if no location is configured.
Alarm Status	Critical (device requires immediate attention), Warning (attention required), and Normal. By default, all information is sorted by Status. To sort by another column heading, click its name.

You can configure the following settings for each output:

Setting	Description
Name	Enter a name for the output (up to 20 characters).
Location	Enter the location of the sensor (up to 20 characters).
Normal State	Set the normal state of the output (excluding the beacon): On/Off or Open/Closed
Control	Change the state of the output to On/Off or Open/Closed.
Alarm Mapping	The beacon, output relay and switched outlet can be activated by alarm states of sensors on the NetBotz module only. <ol style="list-style-type: none">1. Select one or more alarm states that will change the state of the output.2. By default, each sensor connected to the NetBotz module is mapped to activate the output when the sensor is in an abnormal state. Click the name of the alarm state to view the sensors connected to the module.3. Select sensors to include in the alarm. Any selected sensor, in its abnormal state, activates the output.

NOTE: The Output pages under the Status, Control, and Configuration menus are the same, and contain all the tasks for each menu option.

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.

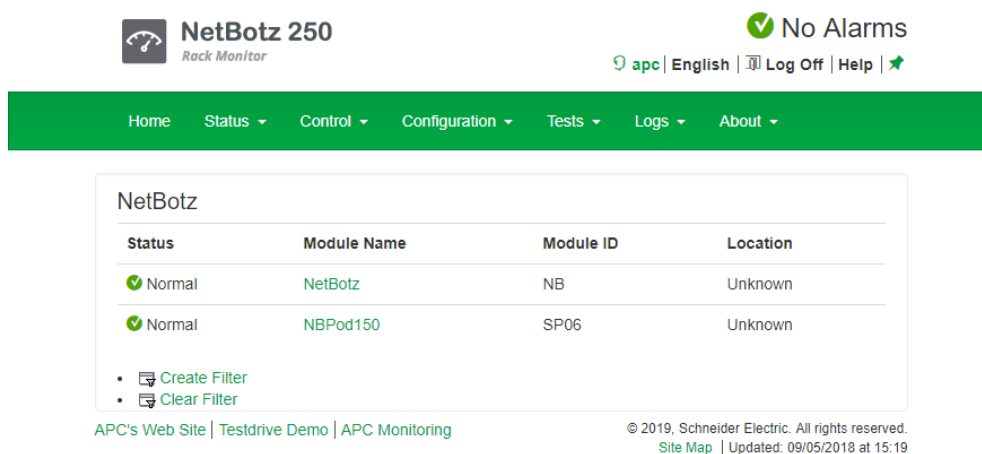
Configuration Tab

You can use these pages to view and configure settings for modules (the appliance and attached sensor pods), wired sensors, wireless sensors, and outputs. You can also configure rack access, security settings, firewall policies, network settings, notifications, general system settings, and Syslog settings.

Configure Settings for an Appliance or Sensor Pod

Path: Configuration > Device > NetBotz

On this page, you can create a filter to show only specific modules (the host appliance and attached Sensor Pod 150 units). You can also select a **Module Name** to view factory information and configure settings for a specific module and any connected devices.



The screenshot shows the NetBotz 250 Rack Monitor web interface. At the top left is the NetBotz 250 logo with the text "Rack Monitor". To the right, it says "No Alarms" with a green checkmark icon. Below that are links for "apc", "English", "Log Off", and "Help". A green navigation bar contains links for "Home", "Status", "Control", "Configuration", "Tests", "Logs", and "About". The main content area is titled "NetBotz" and contains a table with the following data:

Status	Module Name	Module ID	Location
Normal	NetBotz	NB	Unknown
Normal	NBPod150	SP06	Unknown

Below the table are two links: "Create Filter" and "Clear Filter". At the bottom left, there are links for "APC's Web Site", "Testdrive Demo", and "APC Monitoring". At the bottom right, there is a copyright notice: "© 2019, Schneider Electric. All rights reserved." and a "Site Map" link, along with the text "Updated: 09/05/2018 at 15:19".

Filter modules

Show only modules that meet the criteria of your filter. Modules that do not match all selected criteria will not be shown. Select **Create Filter**, then enter one or more filter setting.

Setting	Description
Status	Select one or more alarm statuses: Lost Comm: Lost communication Critical: Critical alarm Warning: Warning alarm Information: Informational alarm Normal: No alarm FW Upgrade: The module firmware is being upgraded
Module Name	Enter a Module Name . Then select filter parameters: <ul style="list-style-type: none">• Case Sensitive: Select to make the filter case sensitive.• Whole Word: Include only complete word matches. If this is not selected, the filter will include partial word matches.
Location	Enter a module location. Then select filter parameters: <ul style="list-style-type: none">• Case Sensitive: Select to make the filter case sensitive.• Whole Word: Include only complete word matches. If this is not selected, the filter will include partial word matches.
Module ID	Enter the Module ID of an appliance or sensor pod. NOTE: The module number for each Sensor Pod 150 is also displayed on its Identifier LED.

You can select **Clear Filter** to remove the filter, or you can create a new filter.

Configure appliance settings

Enter the **Name** and **Location** of the Rack Monitor 250. Select an attached device to configure settings for that device. (See “Configure Settings for Wired Sensors” on page 74, “Configure Wireless Sensors” on page 78, or “Configure Output Settings” on page 81)

Configure Sensor Pod 150 settings

Enter the **Name and Location** of the sensor pod. Select **Blink Identifier LED** to make the Identifier LED on the selected Sensor Pod 150 module blink for the number of minutes you specify. Select an attached device to configure settings for that device (see “Configure Settings for Wired Sensors” on page 74).

Configure Settings for Wired Sensors

Path: Configuration > Device > Wired Sensor > Sensor Type

On these pages, you can do the following:

- Create a filter to show only specific wired sensors.
- Use the **Mass Configuration** feature to configure settings for all sensors of a certain type.
- Select sensors by **Name** to configure settings for individual sensors.
- Select a **Module Name** to view information for the appliance or sensor pod a sensor is connected to.

The screenshot shows the NetBotz 250 Rack Monitor web interface. At the top left is the logo for NetBotz 250 Rack Monitor. At the top right, it displays 'No Alarms' with a green checkmark icon, and navigation links for 'apc', 'English', 'Log Off', and 'Help'. Below this is a green navigation bar with links for 'Home', 'Status', 'Control', 'Configuration', 'Tests', 'Logs', and 'About'. The main content area is titled 'Vibration Sensors' and contains a table with the following data:

Status	Name	State	Location	Module Name
Normal	Sensor NB:2	No Vibration	Unknown	NetBotz

Below the table, there are three action links: 'Mass Configuration...', 'Create Filter', and 'Clear Filter'. At the bottom of the page, there is a footer with 'APC's Web Site | Testdrive Demo | APC Monitoring' on the left and '© 2019, Schneider Electric. All rights reserved. Site Map | Updated: 09/05/2018 at 15:21' on the right.

Filter wired sensors

Show only sensors that meet the criteria of your filter. Sensors that do not match all selected criteria will not be shown. Select **Create Filter**, then enter one or more filter settings.

Setting	Description
Status	Select one or more alarm statuses. Critical: Critical alarm Warning: Warning alarm Information: Informational alarm Normal: No alarm
State	Select the current state of the sensor.
Name	Enter the name of the sensor (up to 20 characters). Then select filter parameters: <ul style="list-style-type: none">• Case Sensitive: Select to make the filter case sensitive.• Whole Word: Include only complete word matches. If this is not selected, the filter will include partial word matches.
Location	Enter a sensor location. Then select filter parameters: <ul style="list-style-type: none">• Case Sensitive: Select to make the filter case sensitive.• Whole Word: Include only complete word matches. If this is not selected, the filter will include partial word matches.
Module Name	Filter by the appliance or sensor pod that sensors are attached to. Enter the Module Name of an appliance or sensor pod, and select filter parameters: <ul style="list-style-type: none">• Case Sensitive: Select to make the filter case sensitive.• Whole Word: Include only complete word matches. If this is not selected, the filter will include partial word matches.
Temperature	Enter a temperature value. From the drop down list, select whether to view sensors that detect a temperature Less Than , Equal To , or Greater Than that value.
Humidity	Enter a humidity value. From the drop down list, select whether to view sensors that detect a humidity Less Than , Equal To , or Greater Than that value.

You can select **Clear Filter** to remove the filter, or you can create a new filter to override the previous one.

Mass-configure sensor settings

Change the settings for all sensors of a certain type at once.

Select **Mass Configuration**, then select the settings you want to configure. Then click **Next** to configure those settings. Available settings depend on the type of device.

Setting	Description
General	<ul style="list-style-type: none"> • Name: The name of the sensor • Location: The location of the sensor <p>Enter up to 20 characters in each field. You can use these wildcards:</p> <ul style="list-style-type: none"> • %m: any parent module IDs • %p: any sensor port number • %l: the parent module location
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.
Severity	Select the severity of alarms generated for these sensors. Alarm severities for temperature and humidity sensors are not editable.
Normal State	Select the normal state of the sensor. An alarm is generated when the sensor changes to an abnormal state.
Alarm Generation	When Alarm Generation is disabled, the system continues to monitor the state of the sensors, but does not generate alarms. Alarms are not recorded in the event log when Alarm Generation is disabled.
Temperature/Humidity Thresholds	<ul style="list-style-type: none"> • Maximum: The maximum allowable value. If the temperature or humidity rises above this value, a critical alarm is generated. • High: If the temperature or humidity rises above this value, a warning alarm is generated. • Low: If the temperature or humidity falls below this value, a warning alarm is generated. • Minimum: The minimum allowable value. If the temperature or humidity falls below this value, a critical alarm is generated. • Hysteresis: This value specifies how far above or below a threshold the temperature or humidity must return to clear a threshold violation. For Maximum and High threshold violations, the clearing point is the threshold minus the hysteresis. For Minimum and Low threshold violations, the clearing point is the threshold plus the hysteresis.
Rate Of Temperature Change	<p>Configure the acceptable short-term and long-term changes in temperature. When the rate of change is exceeded, the appliance generates a critical alarm.</p> <ul style="list-style-type: none"> • S.T. Increase: Short-term temperature increase • L.T. Increase: Long-term temperature increase • S.T. Decrease: Short-term temperature decrease • L.T. Decrease: Long-term temperature decrease • Reset Rate Alarms: Clear all existing rate of change alarms.

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

Configure individual sensor settings

Path: Configuration > Device > Wired Sensor > Sensor Type

Select a sensor's name to configure its settings. Available settings vary by sensor type.

Setting	Description
General	<ul style="list-style-type: none"> • Name: The name of the sensor • Location: The location 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.
Severity	Select the severity of alarms generated for these sensors. Alarm severities for temperature and humidity sensors are not editable.
Normal State	Select the normal state of the sensor. An alarm is generated when the sensor changes to an abnormal state.
Alarm Generation	When Alarm Generation is disabled, the system continues to monitor the state of the sensors, but does not generate alarms. Alarms are not recorded in the event log when Alarm Generation is disabled.
Temperature/Humidity Thresholds	<p>Select Threshold Settings to set the following threshold values for temperature and humidity:</p> <ul style="list-style-type: none"> • Maximum: The maximum allowable value. If the temperature or humidity rises above this value, a critical alarm is generated. • High: If the temperature or humidity rises above this value, a warning alarm is generated. • Low: If the temperature or humidity falls below this value, a warning alarm is generated. • Minimum: The minimum allowable value. If the temperature or humidity falls below this value, a critical alarm is generated. • Hysteresis: This value specifies how far above or below a threshold the temperature or humidity must return to clear a threshold violation. For Maximum and High threshold violations, the clearing point is the threshold minus the hysteresis. For Minimum and Low threshold violations, the clearing point is the threshold plus the hysteresis.
Rate Of Temperature Change	<p>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.</p> <ul style="list-style-type: none"> • S.T. Increase: Short-term temperature increase • L.T. Increase: Long-term temperature increase • S.T. Decrease: Short-term temperature decrease • L.T. Decrease: Long-term temperature decrease • Reset Rate Alarms: Clear all existing rate of change alarms.

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

Configure Wireless Sensors

Path: Configuration > Device > Wireless Sensor Network



No Alarms

[apc](#) | [English](#) | [Log Off](#) | [Help](#) |

Home Status ▾ Control ▾ Configuration ▾ Tests ▾ Logs ▾ About ▾

Wireless Network Configuration

Coordinator Status

Coordinator Connected

Coordinator Address: 00c0b700008c86fc

Firmware Version: 1.0.3

Serial Number: 8A1504N00833

Wireless Sensor Commission List

Name	Extended Address	Serial Number	Firmware Version	Active	Type
Wireless_081fb6	2829860000081fb6	5A1818T36331	1.1.2	Active	Temperature

Wireless Network Auto Join

[APC's Web Site](#) | [Testdrive Demo](#) | [APC Monitoring](#)

© 2019, Schneider Electric. All rights reserved.
[Site Map](#) | Updated: 09/05/2018 at 15:35

The Wireless Sensor Network

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

- The **host appliance** (your 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 USB Type A port on the NetBotz appliance. The coordinator comes installed on the NetBotz Rack Monitor 250.
- **Routers** extend the range of the wireless sensor network. Routers pass information between themselves and the coordinator, and between the coordinator and end devices. Routers are optional. In a data center environment where obstructions are common, routers are recommended if sensors are more than 50 feet from the coordinator. Each router is powered by an AC-USB adapter, not directly connected to the NetBotz appliance.
- **End devices** monitor attached and internal sensors and send data back to the host appliance through the network. End devices are powered by batteries.

The following devices can be configured on your wireless network:

Wireless device	Range	Network role
USB Coordinator & Router (NBWC100U)	up to 30.5 m (100 ft), line of sight	coordinator or router
Wireless Temperature Sensor (NBWS100T)	up to 30.5 m (100 ft), line of sight	end device
Wireless Temperature/Humidity Sensor (NBWS100H)	up to 30.5 m (100 ft), line of sight	end device

NOTE: In a data center environment where obstructions are common, a range of 15 m (50 ft) is typical for any wireless device.

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:** Choose the USB Coordinator & Router that will become the coordinator. **Note the extended address of the coordinator.** Choose one or more USB Coordinator & Routers to become routers.
2. **Mount the sensors.** Choose the locations for the routers and end devices. Do not power the routers or end devices at this time.
3. **Power the coordinator first:** Connect one USB Coordinator & Router to a USB Type A port on the host appliance, or turn on the appliance.
4. **Apply power to the routers:** Power each router using an AC-USB adapter. Do not connect them directly to the appliance.
5. **Power the end devices:** To preserve battery life, do not power the end devices until after the coordinator and the routers are powered.

Complete the configuration of the wireless network on the Web UI of your appliance (see “Add sensors to the Wireless Sensor Network” on page 80).

Disable/Enable the Wireless Sensor Network

To disable the Wireless Sensor Network, click **Disable Coordinator**, then reboot the Network Management Interface (see “Reset/Reboot the Network Interface” on page 70 for instructions).

To enable the Wireless Sensor Network, click **Enable Coordinator**, then reboot the Network Management Interface (see “Reset/Reboot the Network Interface” on page 70 for instructions). Until you reboot the Network Management Interface, the **Coordinator Status** displays **No Wireless Coordinator Installed**.

Add sensors to the Wireless Sensor Network

1. Position and turn on your wireless sensor(s).
2. Enable **Auto Join** until all the wireless sensors in the network have been discovered, or click **Add New Sensor** to add sensors manually. Modify the sensor settings (see “Modify wireless sensor settings” on this page), then click **Apply**.

NOTE: You must enter the extended address (MAC) for each sensor you manually add to the network.

Modify wireless sensor settings

Select a sensor to modify its settings:

Setting	Description
Name	Enter a name (up to 20 characters).
Extended Address	The extended address (MAC) of the wireless sensor.
Location	Enter the location of the sensor (up to 20 characters).
Alarm Generation	Enable or disable. When Alarm Generation is disabled, the system continues to monitor the state of the sensor, but does not generate an alarm. Alarms are not recorded in the event log when Alarm Generation is disabled.
Temperature/ Humidity Thresholds	<ul style="list-style-type: none">• Maximum: The maximum allowable value. If the temperature or humidity rises above this value, a critical alarm is generated.• High: If the temperature or humidity rises above this value, a warning alarm is generated.• Low: If the temperature or humidity falls below this value, a warning alarm is generated.• Minimum: The minimum allowable value. If the temperature or humidity falls below this value, a critical alarm is generated.
Battery/Signal Thresholds	<ul style="list-style-type: none">• Low: If the battery voltage or signal strength drops below its low threshold for the sensor, an alarm occurs.• Minimum: If the battery voltage or signal strength drops below its minimum threshold for the sensor, an alarm occurs.

Configure Output Settings

Path: Configuration > Device > Outputs

Select an output (Beacon, Output Relay, and Switched Outlet). Devices connected to these outputs are controlled by the output settings.

The following information is shown for all outputs:

Setting	Description
Module Name	Name of Module to which the output is connected.
Module Location	Location of Module to which the output is connected, the Rack Monitor 250 or the Sensor Pod 150. 'Unknown' if no location is configured.
Alarm Status	Critical (device requires immediate attention), Warning (attention required), and Normal.

You can configure the following settings for each output:

Setting	Description
Name	Enter a name for the output (up to 20 characters).
Location	Enter the location of the sensor (up to 20 characters).
Normal State	Set the normal state of the output (excluding the beacon): On/Off or Open/Closed
Control	Change the state of the output to On/Off or Open/Closed.
Alarm Mapping	The beacon, output relay and switched outlet can be activated by alarm states of sensors on the NetBotz module only. <ol style="list-style-type: none">1. Select one or more alarm states that will change the state of the output.2. By default, each sensor connected to the NetBotz module is mapped to activate the output when the sensor is in an abnormal state. Click the name of the alarm state to view the sensors connected to the module.3. Select sensors to include in the alarm. Any selected sensor, in its abnormal state, activates the output.

NOTE: The Output pages under the Status, Control, and Configuration menus are the same, and contain all the tasks for each menu option.

Configure Rack Access

Register a new proximity card

1. Navigate to **Configuration > Device > Rack Access > Lock Properties**.
2. Select **Enable** to enable the card reader. Specify the **Auto-Relock** time. If desired, configure the **Door Open Alarm** for Door 1, Door 2, or both.

You can select the card type from the drop-down list. Otherwise, the appliance will automatically recognize the card type.

NOTE: See “Rack access handles” on page 84 for more information on available proximity cards and configuration options.

Click **Apply**.

3. Hold the proximity card in front of the proximity reader on the handle until you hear a beep.
4. Go to **Configuration > Device > User Access > Unregistered Users**.
5. Click the card ID number to specify the card user's **Name**, **Door Access** (Door 1, Door 2, or both), the **Granted Access Schedule** (24 x 7 by default), and enable **Account Access**. Click **Apply**.

NOTE: See “Unregistered users” on page 83 for more information about configuration options for unregistered users.

To view, modify, or delete registered users, go to **Configuration > Device > User Access > Registered Users**.

Registered users

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).
Door Access	The doors the access card is configured to unlock: Door 1 only, Door 2 only, or both doors.
Time Scheduled	Either Granted (the user's access schedule is configured) or Not Configured (the user's access schedule is not configured). Until the schedule is configured, this card cannot unlock enclosure doors.

Unregistered users

Path: Configuration > Device > Rack Access > Unregistered Users

View the ID number of any unconfigured access card that has been held in front of the lock, and the date and time it was held in front of the lock.

To register a user, select the number of the card that will be assigned to the user, and specify the following:

Setting	Description
Name	Enter a name for the user (up to 20 characters).
Contact	Enter the contact information for the user (up to 20 characters).
Card ID	The identification number of the card assigned to the user. This option is not configurable.
Account Access	Check the box to activate the card. To temporarily disable the access permission for the card without deleting the user, uncheck the box.
Door Access	Configure the card to open Door 1 only, the Door 2 only, or both doors.
Granted Access Schedule	Check the box for each day the card is permitted to unlock the doors, and configure the hours during each enabled day the user can access the rack. Valid values are 00:00 to 23:59.
Apply	Click to save your changes.
Cancel	Click to discard your changes.
Delete User	Click to erase the configured information and remove the card from the list of registered users. If the deleted card is held in front of the lock, the card number appears in the list of unregistered users.

User Authentication Methods

Path: Configuration > Device > Rack Access > RADIUS

Specify how users will be authenticated when they access the rack:

Setting	Description
Lock user authentication	<ul style="list-style-type: none">• 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. <p>NOTE: The message “No RADIUS servers have been configured” indicates you must add a properly configured RADIUS server so that RADIUS authentication can operate.</p>
RADIUS server settings	RADIUS New password/Confirm password: The complex password for RADIUS (1 - 64 characters) is enabled by default. The default RADIUS password is the serial number of the NetBotz appliance, displayed in the About > Network option.

Rack access handles

Path: Configuration > Device > Rack Access > Lock Properties

Both rack access handles must be the same model, either two 125 kHz handles or two 13.56 MHz handles. Use Door 1 and Door 2 ports for door switches used with handles; otherwise, use the universal sensor ports for door switches used without handles.

The proximity card type must be the same for both handles.

Setting	Description
Card Reader	Enable or disable the card reader on the door lock. When disabled, you must use a key to access the enclosure.
Card Format	<p>The rack access feature supports multiple access card formats. You can set the expected card format, or allow the appliance to recognize the card format automatically.</p> <p>Cards compatible with the 125 kHz Handle Kit (NBHN125 or NBACS125):</p> <ul style="list-style-type: none"> • H10301 - Standard 26 bit: An access card with a 26-bit card ID number and a facility code. • H10302 - 37 bit w/o facility code: An access card with a 37-bit card ID number and no facility code. • H10304 - 37 bit w/ facility code: An access card with a 37-bit card ID number and a facility code. • CORP1000 - Corporate 1000: An access card with a 35-bit card ID number and a unique company ID code. <p>Cards compatible with the 13.56 MHz Handle Kit (NBHN1356 or NBACS1356):</p> <ul style="list-style-type: none"> • MIFAREC4 - Mifare Classic 4 byte card. • MIFAREC7 - Mifare Classic 7 byte. • MIFAREDF - Mifare DESfire. • MIFAREPL - Mifare Plus. • iCLASS - iCLASS 8byte
Auto-Relock	Enter the number of seconds that elapse before the door re-locks, if the door is not opened within this period of time.
Door Open Alarm	Check the box to enable the alarm for Door 1, Door 2, or both, and enter the number of minutes the door can remain open before an alarm occurs.

Schedule automatic unlocking events

Path: Configuration > Device > Rack Access > Schedule

Schedule a date and time to automatically unlock the doors.

Setting	Description
One-time Schedule	Enable or disable the scheduled unlock.
Date	Specify the date the doors will unlock.
Time	Specify the time the doors will unlock, in hours and minutes. Valid values are 00:00 to 23:59.
Unlock Doors	Unlock Door 1, Door 2, or both doors.
Remain Unlocked	Choose the units (minutes or hours) and enter the number of minutes or hours the doors will remain unlocked before causing an alarm.
Disable relock for the duration	Check the box to prevent the door from locking if it is closed during the scheduled unlock.

Configure Security

Session management settings

Path: Configuration > Security > Session Management

Allow concurrent logins: Check to allow multiple simultaneous logged in users. Otherwise, only one user can be logged into the system at a time.

NOTE: Each interface (FTP, HTTP, Console Telnet, Console USB Serial, etc...) counts as a logged in user.

NOTE: Precedence functionality of pre 6.x systems no longer applies. An attempted USB serial console login does NOT supersede an http login.

Remote Authentication Override: Check to allow user authentication by remote servers (RADIUS, for example) to supersede local user authentication.

See “Manage User Sessions” on page 69 for more information.

Ping response

Configuration > Security > Ping Response

Control whether or not the Rack Monitor 250 responds to a network ping. If enabled, and the Rack Monitor 250 does not respond to an IPv4 ping, see “Rack Monitor 250 Access Problems” on page 132.

Local users

Path: Configuration > Security > Local Users > Management

Create and manage user profiles on the Rack Monitor 250. The initial view is a list of the current user profiles, separated by type. Click any user name to edit that user account, or click **Add User** to create a new user account.

Setting	Description
Access	Check the box to enable access to log into the Rack Monitor 250. Clear the box to disable access.
User Name	The name of the selected user. Set the case-sensitive user name (the 64 byte maximum supports up to 64 ASCII characters, less for multi-byte languages). You cannot modify a user name after you create the user account. To change the user name after the account has been created, you must delete the user and recreate it with the proper value. NOTE: The user name for the Super User cannot be changed.
Current Password	To make changes to the Super User account, enter the existing password.
New Password and Confirm Password	Set the case-sensitive password (64 byte maximum supports up to 64 ASCII characters; Less for multi-byte languages). Passwords with no characters (blank passwords) are not allowed.
User Type	(General User only): User account type used to determine various access permissions to the system: <ul style="list-style-type: none"> • Administrator: The Administrator user has full access just as the Super User does, but this user type can be deleted. • Device: The Device user has read-write access to the device-related menus only. The Administrator can enable or disable the Device user account. • Read-Only: The Read-Only User account has read-only access through the Web UI to view status, but not to control a device or change any configured value. The Administrator can enable or disable the Read-Only user account. • Network-Only: The Network-Only user has read-write access to the network-related menus only. The Administrator can enable or disable the Network-Only user account.
User Description	Field used for additional notes to describe this particular user.
Session Timeout	Amount of time (in minutes) the user has before they are logged out due to inactivity (3 minutes by default).
Serial Remote Authentication Override	Determines whether or not this account can login serially even when the NMC authentication is set to RADIUS.

Your changes will take effect after you log off. For more information about User Account types, see “Types of User Accounts” on page 2“.

Default settings

Path: Configuration > Security > Local Users > Default Settings

There are two main features for the default user settings:

1. Determine the default values when the Super User or Administrator account creates a new user. These values can be changed before the settings are applied to the system.
2. For remote users (user accounts not stored in the system that are remotely authenticated, such as RADIUS), these are the values 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.

Setting	Description
Access	Select Enable to allow access to the appliance.
User Type	Select the user type from the drop-down list. See “Types of User Accounts” on page 2 for detailed information.
User Description	Type the user description in the box.
Session Timeout	The number of minutes a user can be inactive before he or she is automatically logged out.
Bad Login Attempts	The number of incorrect login attempts before the system disables the account. When users reach this limit, a message is displayed informing them that the account has been locked. The Super User or an Administrator can re-enable the account to allow the user to log back in. NOTE: A Super User account cannot be automatically disabled, but it can be manually disabled.
Event Log Color Coding	Configure whether text in the event log is color-coded based on event severity.
Export Log Format	Configure the event log format when exported (downloaded). Tab (default) allows fields to be tab-delimited; CSV is comma-separated.
Temperature Scale	Specify the temperature scale preference. The default temperature scale is Metric, Celsius (°C); the US Customary scale, Fahrenheit (°F), is also available. This value can be changed at a later time.
Date Format	Select the user interface date format from the drop-down box.
Strong Passwords	Select Enable to require new passwords to have these features: <ul style="list-style-type: none">• at least one lowercase character• at least one uppercase character• at least one number• at least and one symbol
Password Policy	Enter the duration (in days) after which the user will be required to change their password. A value of 0 days disables this feature.

Remote users

Authentication.

Path: Configuration > Security > Remote Users > Authentication

Select how to administer remote access to the Rack Monitor 250. For information about local authentication (not using the centralized authentication of a RADIUS server), see the *Security Handbook*, available at www.apc.com.

APC by Schneider Electric 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 that supports up to 64 ASCII characters, less for multi-byte languages. Passwords with no characters (blank passwords) are not allowed.

Select one of the following:

Setting	Description
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. Only the RADIUS server will be contacted. Local authentication is disabled. If the RADIUS server fails to authenticate the user, access is denied.

NOTE: The message "No RADIUS servers have been configured" indicates that you must add a properly configured RADIUS server so that RADIUS authentication can operate.

If RADIUS Only is selected, and the RADIUS server is unavailable, improperly identified, or improperly configured, the only way to recover is through a serial USB connection to the CLI, and change the **Access** setting to **Local Authentication Only** or **RADIUS, then Local Authentication** to regain access.

NOTE: The **Serial Remote Authentication Override** option must be enabled for any local user attempting to log in using the CLI when RADIUS only is selected.

RADIUS.

Configuration > Security > Remote Users > RADIUS

You can set up the device to use a RADIUS server to authenticate remote users. Specify up to two properly configured RADIUS servers. To add a server, click Add Server. To modify an existing server, click the server's name.

Setting	Description
RADIUS Server	The name or IP address of the RADIUS server.
Port	The port the RADIUS server listens on, 1812 by default. NOTE: You can change the port setting to any unused port 5000-32768.
Secret	The secret shared by the RADIUS server and the device.
Reply Timeout	The time the device waits for a response from the RADIUS server (1-30 seconds).
Test Settings	Enter the user name and password of any account on the device to test your settings before you apply them.
Skip Test and Apply	Applies the settings without verifying they are configured correctly.

Configure the RADIUS server

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*.

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. See your RADIUS server documentation for information about the RADIUS users file.
3. VSAs can be used instead of Service-Type attributes provided by the RADIUS server. Using VSAs needs a dictionary entry and RADIUS users file. In the dictionary file, define the names for ATTRIBUTE and VALUE, but not the numeric values. If numeric values are changed, RADIUS authentication and authorization fails. VSAs take precedence over standard RADIUS attributes.

Configure 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 Service-Type to Device.

```
DEFAULTAuth-Type = System
APC-Service-Type = Admin
```

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

```
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.

Firewall

Path: Configuration > Security > Firewall

The Rack Monitor 250 provides a configurable network firewall. The firewall can allow or deny network traffic to and from the appliance based on user-configured rules, which are ordered by priority. In the Web UI, you can use the firewall policy editor to create or edit a custom firewall policy.

Though the Rack Monitor 250 can store multiple firewall policies, only one policy can be active at once. When a firewall is enabled and a custom policy file is applied, the policy is checked for syntax errors. If an error is found, the policy will not be loaded.

A sample firewall policy (.fwl) is provided in the file system for reference. It is available for download via FTP or SCP, from the `/firewall` directory of the file system.

Use the **Test Policy** option to test and verify a custom firewall policy. It is recommended that a firewall policy be tested before it is applied to a production environment.

Enable/disable the firewall

Path: Configuration > Security > Firewall > Configuration

Enable or disable the overall firewall functionality.

Set the active policy

Path: Configuration > Security > Firewall > Active Policy

Select an active policy from the available firewall policies.

View active rules

Path: Configuration > Security > Firewall > Active Rules

View the individual rules that are currently enforced based on the active policy.

Create/edit a policy

Path: Configuration > Security > Firewall > Create/Edit Policy

Create a new policy, edit an existing policy, or delete an existing policy.

To 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 the filename does not have this file extension, .fwl will be appended to the name automatically.

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

It is recommended that you do not edit active policies. Instead, disable the firewall, edit the policy, test it, and then re-enable the policy.

To edit a policy,

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 2 rules conflict, the rule with the higher priority will determine what happens. The highest priority is 1; the lowest is 250.
Type	host: In the IP/any field, you will enter a single IP address. subnet: In the IP/any field, you will enter a subnet address. range: In the IP/any field, you will enter a range of IP addresses.
IP/any	Specify the IP address or range of addresses this rule applies to, or select one of the following: <ul style="list-style-type: none">• any: The rule applies regardless of the IP address.• anyipv4:The rule applies for any IPv4 address.• anyipv6:The rule applies for any IPv6 address.
Port	Specify a port the rule will apply to. <ul style="list-style-type: none">• None: The rule will apply to any port.• Common Configured ports: Select a standard port.• Other: Specify a non-standard port number.
Protocol	Specify which protocol the rule applies to. <ul style="list-style-type: none">• any: any protocol• tcp: used for reliable information transfer between applications• udp: alternative to TCP used for faster, lower bandwidth information transfer. Though it has fewer delays, UDP is less reliable than TCP.• icmp: used to report errors for troubleshooting• icmpv6: used to report errors for troubleshooting on applications using IPv6
Action	allow: Allow the packet that matches this rule. discard: Discard the packet that matches this rule.
Log	If this rule applied to a packet, regardless of whether the packet is blocked or allowed, this will add an entry to the Firewall Log (see "Firewall Log" on page 119).

Import a firewall policy

Path: Configuration > Security > Firewall > Load Policy

Load a policy file (.fwl suffix) from a source external to this device.

Test a firewall policy

Path: Configuration > Security > Firewall > Test Policy

Temporarily enforce the rules of a chosen policy.

NOTE: The firewall is disabled by default..

Configure Network Settings

TCP/IP Settings

IPv4 settings.

Path: Configuration > Network > TCP/IP > IPv4 Settings

The default TCP/IP configuration setting, DHCP, assumes a properly configured DHCP server is available to provide TCP/IP settings to the Rack Monitor 250.

Otherwise, you can configure the default setting for BOOTP. A user configuration (.ini) file can function as a BOOTP or DHCP boot file. For more information, see the TCP/IP configuration section of the Network Management Card User's Guide, available from www.apc.com.

View and configure current IPv4 settings, and enable or disable IPv4. You can also opt to manually override the automatic settings for System IP, Subnet Mask, and Default Gateway.

Setting	Description
Manual	Configure the IPv4 settings (IP address, subnet mask, and default gateway) manually. Click Apply .
BOOTP	A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Rack Monitor 250 requests a network assignment from any BOOTP server: <ul style="list-style-type: none">• If it receives a valid response, the network services start.• If it finds a BOOTP server, and receives a valid response, the device requests network assignment from any BOOTP server, and network services are initiated.• If a request to that server fails or times out, the Rack Monitor 250 stops requesting network settings until it is restarted.• By default, if no valid response is received with the new settings, and previously configured network settings exist, five attempts to connect will be made (the original and four retries), then the prior settings will be used.
DHCP	At 32-second intervals, the device requests network assignment from any DHCP server: <ul style="list-style-type: none">• Optionally, the device requires the vendor specific cookie from the DHCP server in order to accept the lease and start the network services.• If it finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted. <p>Vendor Cookie: Check to require vendor specific cookie to accept DHCP address (disabled by default).</p> <p>NOTE: The default values for these three settings generally do not need to be changed:</p> <ul style="list-style-type: none">• Vendor Class: APC• Client ID: The MAC address of the device. If you change this value, the new value must be unique on the LAN.• User Class: The name of the application firmware module, NB250.

Advanced DHCP Configuration. You can use a 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, the MAC address of the Rack Monitor 250 by default.
 - A User Class Identifier, NB250 by default, the identification of the application firmware installed on the Rack Monitor 250.
2. A properly configured DHCP server responds with a DHCP offer that includes all the settings 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. This cookie is not required by default.

```
Option 43 = 01 04 31 41 50 43
```

where:

- 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.

For additional information on supported DHCP (DHCPv4) options sent and received by the Rack Monitor 250, see the FAQ article FA156110 on www.apc.com.

For more detail about how a DHCP server can configure the network settings for a Rack Monitor 250, see “DHCP Configuration” in the Network Management Card 2 User’s Guide, available from www.apc.com.

IPv6 Settings.

Path: Configuration > Network > TCP/IP > IPv6 Settings

Current IPv6 Settings

Setting	Description
Type	Indicates the IP address is assigned Manually or Automatically.
IP Address	The IPv6 address of the device.
Prefix Length	Indicates the number of bits used to identify the network.

IPv6 Configuration

Setting	Description
Enable	Check to enable or disable IPv6 communications.
Manual Configuration	Check the box to enable manual configuration, and then enter the system IPv6 address and default gateway if you are not using automated addressing.
Auto Configuration	Check the box to enable obtaining addressing prefixes from the router, if available, to automatically configure IPv6 addresses.
DHCPv6 Mode	
Router Controlled	Select to control DHCPv6 by the M (Managed Address Configuration) and O (Other Stateful Configuration) flags received in IPv6 Router Advertisements. When a router advertisement is received, the Rack Monitor 250 checks whether the M and O flags are set. The Rack Monitor 250 interprets the state of the M and O 'bits' for the following cases: <ul style="list-style-type: none">• Neither is set: Indicates the local network has no DHCPv6 infrastructure. The Rack Monitor 250 uses Router Advertisements and/or manual configuration to get non-link-local addresses and other settings.• M, or M and O are set: Full DHCPv6 address configuration occurs. DHCPv6 is used to obtain addresses AND other configuration settings. This is known as DHCPv6 stateful. Once the M flag is received, the DHCPv6 address configuration stays in effect until the interface has been closed, even if subsequent Router Advertisement packets are received where the M flag is not set. If an O flag is received first, and an M flag is received subsequently, the Rack Monitor 250 performs full address configuration when it receives the M flag.• Only O is set: The Rack Monitor 250 sends a DHCPv6 Info-Request packet. DHCPv6 is used to configure 'other' settings, such as location of DNS servers, but NOT to provide addresses. This is known as DHCPv6 stateless.
Address and Other Information	With this radio box selected, DHCPv6 is used to obtain addresses AND other configuration settings. This is known as DHCPv6 stateful.
Non-Address Information Only	With this radio box selected, DHCPv6 is used to configure "other" settings (such as location of DNS servers), but NOT to provide addresses. This is known as DHCPv6 stateless.
Never	With this radio box selected, DHCPv6 is NOT used for any configuration settings.

Port speed

Path: Configuration > Network > Port Speed

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

Setting	Description
Auto-Negotiation	Ethernet devices negotiate to transmit at the highest possible speed. If the supported speeds of two devices do not match, the slower speed is used.
10 Half-Duplex	10 Mbps communication in one direction at a time.
10 Full-Duplex	10 Mbps communication in both directions on the same channel simultaneously.
100 Half-Duplex	100 Mbps communication in both directions on the same channel simultaneously.
100 Full-Duplex	100 Mbps communication in one direction at a time.

DNS server settings

Configuration.

Path: Configuration > Network > DNS > Configuration

The Rack Monitor 250 supports the use of Domain Name System (DNS) servers. If a DNS name is configured, you can access the Rack Monitor 250 by its assigned DNS name instead of IP address. For the Rack Monitor 250 to send email, the primary DNS server must be defined.

Setting	Description
Override Manual DNS Settings	When selected, configuration data from other sources, typically DHCP, take precedence over the manual configurations. Check the box to override manual DNS settings, and specify the IP address of the Primary DNS Server and, optionally, the Secondary DNS Server . The primary server is always tried first.
System Name Synchronization	Select Enable to synchronize the system name with the host name so both fields automatically contain the same value. Click the System Name link to view the system name on the Configuration > General > Identification page.
Host Name	Configure a host name.
Domain Name (IPv4/IPv6)	Configure the domain name, added automatically whenever you enter only a host name in a field that accepts domain names (except e-mail addresses).
Domain Name (IPv6)	

DNS Network Test.

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.

Setting	Description
Last Query Response	The result of your last query. If the query succeeded, the result is a domain name, IP address, or mail exchange. If the query failed, an error message gives the reason for the failure.
Query Type	Specify the query type by: <ul style="list-style-type: none">• Host: The URL name of the server.• FQDN: The fully qualified domain name of the server.• IP: The IP address of the server.• MX: The mail exchange used by the server.
Query Question	The value for the selected query type: the URL, the IP address, the fully qualified domain name (for example, myserver.mydomain.com), or the mail exchange address.

Network configuration for Web access

Path: Configuration > Network > Web > Access

Enable/disable access to the Web UI. You must log out of the Rack Monitor 250 Web UI to activate your changes. You must use a computer with telnet access to re-enable Web access.

Setting	Description
Enable HTTP	Sets Hypertext Transfer Protocol (HTTP) as the means of access to the Web UI. Access through HTTP is by user name and password; neither is encrypted, and data is not encrypted during transmission.
Enable HTTPS	Sets Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) as the means of access to the Web UI. HTTPS encrypts user names, passwords, and data during transmission, and uses digital certificates for authentication.
HTTP Port*	The port (80 by default) that HTTP uses to communicate.
HTTPS Port*	The port (443 by default) that HTTPS uses to communicate.
Minimum Protocol	The minimum HTTPS protocol to use. Select SSL 3.0, TLS 1.0, TLS 1.1 (the default) or TLS 1.2.
Require Authentication Cookie	If enabled, a session cookie will be used for authentication tracking within the browser. NOTE: The cookie will be removed when the session ends.
Limited Status Access	Select whether or not to display a read-only, public Web page with basic device status. This feature is disabled by default. Select the 'Use as default page' option to show the page as the default landing page when a user accesses the device with the IP address or hostname.

* For either port, you can use any unused port from 5000 to 32768 for additional security. Use a colon (:) in the address field of the browser to specify the port number.

For port number 5000 and IP address 152.214.12.114:

`http://152.214.12.114:5000`

`https://152.214.12.114:5000`

SSL certificate

Path: Configuration > Network > Web > SSL Certificate

You can load a 1024 bit or 2048 bit SSL certificate to the Rack Monitor 250 using SHA-1 or SHA-256 (hash algorithms).

View the status of an installed SSL Certificate, and add, replace, or remove a security certificate. **If you install an invalid certificate, or if no certificate is loaded when you enable SSL**, restarting the device creates 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, but a security alert message displays whenever you log on. In a default certificate, the Organizational Unit field displays “Internally Generated Certificate,” and the Common Name field reports the serial number of the device.

Setting	Description
Status	Not installed: A certificate is not installed, or was installed by FTP or SCP to an incorrect location. Generating: A certificate is being generated because no valid certificate was found. Loading: A certificate is being activated on the Rack Monitor 250. Valid certificate: A valid certificate was installed or was generated by the Rack Monitor 250. Click the link to view the certificate’s contents.
Certificate Action	Add or Replace Certificate File: Enter or browse to the certificate file created with the Security Wizard. Remove: Delete the current certificate.

NOTE: For detailed information on enhancing the security of your system, see the *Security Handbook*, available on www.apc.com.

Console

Console Access.

Path: Configuration > Network > Console > Access

Configure access to the CLI.

Setting	Description
Enable Telnet	Telnet transmits user names, passwords, and data without encryption.
Enable SSH	Secure SHell (SSH) version 2 transmits user names, passwords and data in encrypted form. Enabling Secure SHell (SSH) enables SCP automatically.
Telnet Port	The TCP/IP port (23 by default) Telnet uses to communicate.
SSH Port	The TCP/IP port (22 by default) SSH uses to communicate.

NOTE: To enhance security, change the port setting to any unused port from 5000 to 32768, and specify the non-default port to gain access. Telnet clients require you to append either a space and the port number or a colon and the port number to the command line to access the CLI. For **SSH**, see your SSH client documentation to specify a non-default port in the command line that starts SSH.

User Host Key Configuration.

Path: Configuration > Network > Console > SSH Host Key

View the status of an installed SSH Host Key, and add, replace, or remove a Host Key. If the host key has been removed or if no host key was loaded, and you enable SSH, the device restarts, and it generates a host key. Allowing the device to generate its own host key could make the SSH server unavailable for use for as long as one minute.

Setting	Description
Status	Indicates whether the current SSH Host Key is valid.
Add or Replace	To use a host key you created with the Security Wizard, load the host key before you enable SSH. Browse to or enter the path name of the host key file created with the Security Wizard, and click Apply.
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; Microsoft Windows operating systems do not. Clients are available from various vendors.

SNMPv1 configuration

All user names, passwords, and community names for Simple Network Management Protocol (SNMP) are transferred over the network as plain text. If your network requires encryption, disable SNMPv1 access or set the access for each community to Read. (Read access can receive status information and use SNMP traps.)

NOTE: SNMPv2c is supported under SNMPv1 in this configuration.

StruxureWare Data Expert is Schneider Electric's platform of integrated software applications and suites that help maximize business performance while making the best of enterprise resources. To manage the Rack Monitor 250 on the public network of a StruxureWare system, you must have SNMP enabled in the Rack Monitor 250 interface. Read access will allow StruxureWare to receive traps from a Rack Monitor 250. Write access is required while you use the interface of the Rack Monitor 250 to set StruxureWare as a trap receiver.

Access.

Path: Configuration > Network > SNMPv1 > Access

Enable SNMPv1 as a method of communication with this device.

For detailed information on enhancing the security of your system, see the *Security Handbook*, available on www.apc.com.

Access Control.

Path: Configuration > Network > SNMPv1 > Access Control

You can configure up to four access control entries to specify which NMS can have access to the Rack Monitor 250.

- If you leave the default access control entry unchanged for a community, that community has access to this device from any location on the network.
- If you configure multiple access control entries for one community name, the limit of four entries requires that one or more of the other communities must have no access control entry. If no access control entry is listed for a community, that community has no access to this device.

Select a **Community Name** to configure access control settings for that community.

Setting	Description
Community Name	The name that a NMS must use to access the community. The maximum length is 15 ASCII characters, and the default community names for the four communities are public , private , public2 , and private2 .
NMS IP/Host Name	The IP address, IP address mask, or host name that controls access by NMSs. A host name or a specific IP address (such as 149.225.12.1) allows access only by the NMS at that location. IP addresses that contain 255 restrict access as follows: <ul style="list-style-type: none">• 149.225.12.255: Access only by an NMS on the 149.225.12 segment.• 149.225.255.255: Access only by an NMS on the 149.225 segment.• 149.255.255.255: Access only by an NMS on the 149 segment.• 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.
Access Type	The actions an NMS can perform through the community. <ul style="list-style-type: none">• Disable: No GETS or SETS at any time.• Read: GETS only, at any time.• Write: GETs and SETs at any time. NOTE: In the multi-user system, this now allows SETs while users are logged in which operates in the same manner as Write+.• Write+: GETS and SETS at any time.

SNMPv3 configuration

For SNMP GETs, SETs, and trap receivers, SNMPv3 uses a system of user profiles to identify users.

Access.

Path: Configuration > Network > SNMPv3 > Access

Enable SNMPv3 as a method of communication with this device.

User Profile.

Path: Configuration > Network > SNMPv3 > User Profile

The four default user profiles (apc snmp profile1” through “apc snmp profile 4”) have no authentication and no privacy (no encryption of data). To edit the following settings for a user profile, click a user name in the list.

Setting	Description
User Name	The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters.
Authentication Passphrase	A phrase of up to 32 bytes, ASCII characters; that verifies the NMS communicating with this device through SNMPv3, 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 up 32 bytes, ASCII English characters, that ensures the privacy of the data (by means of encryption) that a NMS is sending to this device or receiving from this device through SNMPv3.
Authentication Protocol	The APC by Schneider Electric implementation of SNMPv3 supports SHA or MD5 authentication. Authentication will not occur unless SHA or MD5 is selected here.
Privacy Protocol	The Schneider Electric implementation of SNMPv3 supports AES or DES as the protocol for encrypting and decrypting data. Privacy of transmitted data requires that AES or DES is selected here. 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 NMSs have access to this device. The opening page for access control, by default, assigns one entry to each of the four user profiles. To edit the access control settings for a user profile, click its user name.

- If you leave the default access control entry unchanged for a user profile, all NMSs that use that profile have access to this device.
- If you configure multiple access entries for one 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.

Setting	Description
Access	Mark the “Enable” check box to activate the access control specified by the parameters in this access control entry
User Name	From the drop-down list, select the user profile to which this access control entry will apply.
NMS IP/Host Name	The IP address, IP address mask, or host name that controls access by the NMS. <ul style="list-style-type: none">• A host name or a specific IP address (such as 149.225.12.1) allows access by only the NMS at that location. An IP address mask that contain 255 restricts access as follows:<ul style="list-style-type: none">• 149.225.12.255: Access only by an NMS on the 149.225.12 segment.• 149.225.255.255: Access only by an NMS on the 149.225 segment.• 149.255.255.255: Access only by an NMS on the 149 segment.• 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment.

Enable Modbus

Enable Modbus to allow a Building Management System to monitor the Rack Monitor 250. The Rack Monitor 250 supports Modbus serial (RTU) and Modbus TCP.

Serial (RTU) Access.

Path: Configuration > Network > Modbus > Serial

Set the baud rate for Modbus access (9600 or 19200 bps), and define the Target Unique ID. The Target Unique ID is an identifier from 1 to 247, and must be unique on the Modbus bus. The default settings are 9600 baud, 8 data bits, parity Even, and 1 stop bit.

The Rack Monitor 250 sets the value for stop bits automatically based on parity according to the Modbus standard. When parity is set to None, 2 stop bits are used.

TCP Access.

Path: Configuration > Network > Modbus > TCP

Enable Modbus TCP to view the Rack Monitor 250 through your building management service's interface. Specify the port for the TCP connection, 502 by default, or 5000 to 32768.

You must log off for the changes to take effect.

FTP server

Path: Configuration > Network > FTP Server

Enable File Transfer Protocol (**FTP**) Server access.

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

By default, the FTP server communicates with the Rack Monitor 250 through TCP/IP port 21. Both the specified port and the port one number lower than the specified port are used.

For enhanced security, change the default **port**. Allowed non-default port numbers are 5001 to 32768. Append port name preceded by a space or colon depending on the FTP client used.

For example, for port 5001 and IP address 152.214.12.114:

```
ftp 152.214.12.114:5001
```

For detailed information on enhancing and managing the security of your system, see the Security Handbook, available from www.apc.com.

Notification

Path: Configuration > Notification

You can configure Event Actions to occur in response to an event, or group of events. To configure multiple events simultaneously by severity level or category, use the “By Group” option under Event Actions. For a summary of the configured event notifications, select the appropriate category or subcategory.

These actions notify users of the event in any of several ways:

- **Active**, automatic notification. The specified users or monitoring devices are contacted directly.
- **Indirect** notification in the event log. If no direct notification is configured, users must check the log to determine which events have occurred.

To configure an individual event, click the event name, and select the appropriate notification parameters.

Select the types of notification to be used for:

- **Event Log**: Record the event in the event log.
- **Syslog**: Notify the defined Syslog servers to record the event in the Syslog system log.
- **E-mail**: Notify the defined e-mail recipients selected.
- **Trap**: Notify the configured trap receivers selected with an SNMP trap.

Event actions

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. For more information on how to configure and use data logging, See “Logs Tab” on page 114.
 - Queries (SNMP GETs)
 - For more information, see See “SNMPv1 configuration” on page 99 and “SNMPv3 configuration” on page 101. 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.

Configure event actions

Configure event actions 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. To find an event, click on a column heading to see the lists under the **Device Events**, **System Events**, **Rack Events**, or **Wireless categories**. You can also click on a sub-category under these headings, like **Security** or **Temperature**.
2. Click on the event name to view or change the current configuration, such as recipients to be notified by e-mail, 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.

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

- “Servers” on page 111
- “E-mail Recipients” on page 107
- “SNMP trap receivers” on page 108

Configure event actions by group.

Path: Configuration > Notification > Event Actions > By Group

1. Select how to group events for configuration:
 - Select **Events by Severity**, and then select one or more severity levels. You cannot change the severity of an event.
 - Select **Events by Category**, and then select all events in one or more pre-defined categories.
2. Click **Next** to move to the next screen to do the following:
 - a. Select event actions for the group of events.
 - To select any action except **Logging** (the default), you must first have at least one relevant recipient or receiver configured.
 - If you selected **Logging** and have configured a Syslog server, select **Event Log** or **Syslog** on the next screen.
3. Click **Next** to move to the next screen to do the following:
 - a. If you selected **Logging** on the previous screen, select **Enable Notifications** or **Disable Notification**.
 - b. If you selected **Email Recipients** on previous screen, select the recipients to configure.
 - c. If you selected **Trap Receivers** on previous screen, select the trap receiver to configure.
4. Click **Next** to move to the next screen to do the following:
 - a. If you are configuring **Logging** settings, view the pending actions and click **Apply** to accept the changes or click **Cancel** to revert to the previous settings.
 - b. If you are configuring **Email Recipients** or **Trap Receivers**, select **Enable Notifications** or **Disable Notification** and set the notification timing settings (see “Notification parameters” on page 105 for more information on these settings).
5. Click **Next** to move to the next screen to do the following:
 - a. View the pending actions and click **Apply** to accept the changes or click **Cancel** to revert to the previous settings.

Notification parameters. Configuration fields define e-mail parameters for notifications of events.

They are usually accessed by clicking 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, and no notification is sent.
Repeat at an interval of n	The notification is sent repeatedly at the specified interval (the default is every 2 minutes until the condition clears).
Up to n times	During an active event, the notification repeats for this number of times.
or	
Until condition clears	The notification is sent repeatedly until the condition clears or is resolved.

NOTE: For events that have an associated clearing event, you can also set these parameters.

E-mail notifications

Path: Configuration > Notification > E-mail

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 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.

E-mail Server Settings.

Path: Configuration > Notification > E-mail > Server

View current primary and secondary DNS server addresses, and configure the Outgoing Mail server and Advanced email settings.

Setting	Description
From Address	<ul style="list-style-type: none">• user@[IP_address]: if an IP address is specified as Local SMTP Server• user@domain: if DNS is configured and the DNS name is specified as Local SMTP Server 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. NOTE: This definition is required only when the SMTP server is set to Local.
Port	The SMTP default port is 25. Alternative ports: 465 and 587 for SSL/TLS encrypted email, or 5000 to 32768.
Authentication	Enable this if the SMTP server requires authentication. This performs a simple authentication, not SSL.
User Name, Password, and Confirm Password	If your mail server requires authentication, enter your user name and password here.
Use SSL/TLS	Select when encryption is used. <ul style="list-style-type: none">• Never: The SMTP server does not require nor support encryption.• If Supported: The SMTP server advertises support for STARTTLS, but doesn't require the connection to be encrypted. The STARTTLS command is sent after advertisement is given.• Always: The SMTP server requires the STARTTLS command to be sent on connection to it.• Implicitly: The SMTP server only accepts connections that begin encrypted. No STARTTLS message is sent to the server.
Require CA Root Certificate:	This should only be enabled if the security policy of your organization does not allow for implicit trust of SSL connections. If this is enabled, a valid root CA certificate must be loaded for encrypted e-mails to be sent.
File Name	This field is dependent on the root CA certificates installed, and whether or not a root CA certificate is required.

E-mail Recipients.

Path: Configuration > Notification > E-mail > Recipients

Specify up to four e-mail recipients. Click **Add Recipient** or the email address (if already configured) to configure the settings. **Active E-mail Server Settings** displays the current configuration.

Setting	Description
Generation	Enable sending email to this recipient (the default)
To Address	The user and domain names of the recipient. To use e-mail for paging, use the e-mail address for the recipient's mobile gateway account (for example, myacct100@skytel.com). The mobile gateway will generate the page. To bypass the DNS lookup of the IP address of the mail server, use the IP address in brackets instead of the e-mail domain name, e.g., use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly.
Language	The language which the e-mail notification will be sent in. This is dependent on the installed language pack (if applicable).
Server	<p>Local: This is through the site-local SMTP server. This recommended setting ensures that the e-mail is sent using the site-local SMTP server. 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.</p> <p>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.</p> <p>Custom: This setting enables each e-mail recipient to have its own server settings. These settings are independent of the settings given under "SMTP Server" above. If your mail server requires authentication, type your user name and password.</p>
Custom E-mail Server Settings	This setting enables each e-mail recipient to have its own server settings. These settings are independent of the SMTP server settings given under "E-mail Server Settings" on page 106. See "E-mail Server Settings" on page 106 for a description of each field.

E-mail SSL Certificates.

Path: Configuration > Notification > E-mail > SSL Certificates

Load a mail SSL certificate for greater security. The file must have an extension of .crt or .cer. Up to five files can be loaded at any given time. 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 E-mail.

Path: Configuration > Notification > E-mail > Test

Send a test message to a configured recipient. It is recommended to test the email configuration to prevent issues when critical e-mail notifications are required.

SNMP trap receivers

Path: Configuration > Notification > SNMP Traps > Trap Receivers

With Simple Network Management Protocol (SNMP) traps, you can automatically get notifications for significant events. They are a useful tool for monitoring devices on your network. The trap receivers are displayed by **NMS IP/Host Name**, where NMS stands for Network Management System. You can configure up to six trap receivers.

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.

To configure a new trap receiver, click ‘**Add Trap Receiver.**’ To edit (or delete) one, click 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 the **SNMPv1** or **SNMPv3** radio button 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

- **Community Name:** The name (“public” by default) used as an identifier when SNMPv1 traps are sent to this trap receiver.
- **Authenticate Traps:** When this option is enabled (the default), the NMS identified by the NMS IP/Host Name setting will receive authentication traps (traps generated by invalid attempts to log on to this device).

– SNMPv3

- **User Name:** Select the identifier of the user profile for this trap receiver.

SNMP traps test screen

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 a valid IP address. 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 is displayed.

General Options

Identification

Path: Configuration > General > Identification

Define the following values:

Setting	Description
Host Name Synchronization	Synchronizes the Name with the System Name, so both fields automatically contain the same value. A host name does not allow spaces. If Host Name Synchronization is enabled, spaces are not allowed in the Name. If Host Name Synchronization is turned off, spaces are allowed.
Name	The name assigned to the device, used by StruxureWare Data Center Expert, and the sysName OID in the SNMP agent.
Contact	The person responsible for the device. This value is used by StruxureWare Data Center Expert and the sysContact OID in the SNMP agent.
Location	The physical location of the device is used by StruxureWare Data Center Expert and the sysLocation OID in the SNMP agent.
System Message	When defined, a custom message appears on the log on screen for all users.

Set the date and time

Path: Configuration > General > Date/Time > Mode

Set the time and date used by the Rack Monitor 250. The **Current Settings** section displays the current date and time and other related settings. You can change these settings manually or from a Network Time Protocol (NTP) Server.

Manual Mode

- Enter the date and time for the Rack Monitor 250.
- Check the box to **Apply Local Computer Time** to match the date and time settings of the computer you are using.

Synchronize with NTP Server: Allow an NTP Server to define the date and time for the Rack Monitor 250.

Setting	Description
Time Zone	Select a time zone. The number of hours preceding each time zone in the list is the offset from Coordinated Universal Time (UTC), formerly Greenwich Mean Time.
Primary NTP Server	Enter the IP address or domain name of the primary NTP server.
Secondary NTP Server (Optional)	Enter the IP address or domain name of the secondary NTP server, when a secondary server is available.
Update Interval	Define how often, in hours, the Rack Monitor 250 accesses the NTP Server for an automatic update. Minimum: 1; Maximum: 8760 (1 year).
Update Using NTP Now	Initiate an immediate update of date and time from the NTP Server.
NOTE: If you select Override Manual NTP Settings, configuration data from other sources (typically DHCP) take precedence over the manual configurations set here.	

Daylight Saving.

Path: Configuration > General > Date/Time > Daylight Savings

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

When customizing Daylight Saving Time (DST):

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

Use a configuration file (.ini)

Path: Configuration > General > User Config File

Use the settings from one Rack Monitor 250 to configure another. Retrieve the config.ini file from the configured Rack Monitor 250, customize that file (e.g., change the IP address), and upload the customized file to the new Rack Monitor 250. The file name can be up to 64 characters, and must have the.ini suffix.

Setting	Description
Status	Reports the progress of the upload. The upload succeeds even if the file contains errors, but a system event reports the errors in the event log.
Upload	Browse to the customized file and upload it so that the current Rack Monitor 250 can use it to set its own configuration.
Download	Allows the download of the Configuration File (config.ini) file directly through the Web browser to the user's computer.

To retrieve and customize the file of a configured Rack Monitor 250, see “How to Export Configuration Settings” on page 122.

Instead of uploading the file to one Rack Monitor 250, you can export the file to multiple Rack Monitor 250s by using an FTP or SCP script. See “Export the .ini File to Multiple Rack Monitor 250s” on page 123 for more information.

Configure quick links

Path: Configuration > General > Quick Links

Quick Links provide quick access to useful websites, servers, devices, etc.

Click the link name in the **Display** column to change the URLs for the Quick Links in the bottom left corner of the Web UI pages. A **Name** (up to 40 characters) to identify the link and a URL (up to 100 characters) are required.

Each link has an option to Reset to Defaults.

By default, the links access the following Web pages:

- **Link 1:** Website homepage
- **Link 2:** Demonstrations of Schneider Electric web-enabled products
- **Link 3:** Information on Schneider Electric Remote Monitoring Services

Syslog

Servers

Path: Configuration > Logs > Syslog > Servers

Implementation of Syslog supports the sending of notifications to specific servers. The Syslog servers record events that occur at network devices in a log that provides a centralized record of events. Describing the Syslog in great detail is outside the scope of this manual. See RFC3164 online for more information about Syslog.

The Rack Monitor 250 can be configured to send a notification of events to up to four Syslog servers. To add a server, click **Add Server**. To modify an existing server, click the server's name.

Setting	Description
Syslog Server	Uses IPv4/ IPv6 addresses or host names to identify from one to four servers to receive Syslog messages sent by the appliance.
Port	The Rack Monitor 250 uses the default port 514 to send Syslog messages.
Language	Choose a language for any Syslog messages.
Protocol	Choose between UDP and TCP.

NOTE: To disable Syslog messages, See "Configure event actions" on page 104. In addition, Syslog messages can be disabled if the "Message Generation" option is not selected in Syslog Settings.

Settings

Path: Configuration > Logs > Syslog > Settings.

Setting	Description
Message Generation	Enable the generation and the logging of Syslog messages for events that have Syslog configured as a notification method.
Facility Code	Messages from this device will be categorized by Facility Code, and the associated facility categorization allows Syslog messages from different devices to be placed in separate logs.
Severity Mapping	<p>This section maps each severity level of the appliance or environment events to available Syslog priorities. The local options are Critical, Warning, and Informational. You should not need to change the mappings.</p> <ul style="list-style-type: none">• Emergency: The system is unusable• Alert: Action must be taken immediately• Critical: Critical conditions• Error: Error conditions• Warning: Warning conditions• Notice: Normal but significant conditions• Informational: Informational messages• Debug: Debug-level messages

Test

Path: Configuration > Logs > Syslog > Test

Setting	Description
Last Test Result	Result of Last Test Performed
Server	The message will be sent to all configured servers.
Severity	Select a severity level (Syslog priority) for the test message.
Test Message	Format the message to consist of the event type (APC, System, or Device, for example) followed by a colon, a space, and the event text (50 character max).

Tests Tab

The screenshot shows the NetBotz 250 Rack Monitor interface. At the top left is the logo for NetBotz 250 Rack Monitor. At the top right, it displays 'No Alarms' with a green checkmark icon, and navigation links for 'apc', 'English', 'Log Off', and 'Help'. Below this is a green navigation bar with menu items: Home, Status, Control, Configuration, Tests, Logs, and About. The main content area is titled 'Network Test' and contains a configuration box for 'LED Blink'. Inside this box, there is a section for 'LED Blink Duration' with a text input field containing the number '1' and a dropdown menu set to 'minutes'. Below the input field are two buttons: 'Apply' and 'Cancel'. At the bottom of the page, there is a footer with links for 'APC's Web Site', 'Testdrive Demo', and 'APC Monitoring', along with copyright information: '© 2019, Schneider Electric. All rights reserved. Site Map | Updated: 09/05/2018 at 15:39'.

LED Blink test

Path: Tests > Network > LED Blink

Initiate flashing the device's Status and Link LEDs on the Ethernet Port to help you locate the device.

Logs Tab

Creating a log is resource intensive. Depending on your device's configuration, it may take several minutes to generate and download a log. Your computer or Web browser may appear unresponsive during this time.

Filtering: By default, the event and data logs display the most recent events first. To see the data log listed together on a Web page, click **Launch Log in New Window**. The log entries can be cleared by clicking **Clear Log**.

NOTE: JavaScript must be enabled in your browser.

Event Log

Path: Logs > Events > Log

The screenshot shows the NetBotz 250 Rack Monitor interface. At the top, there is a header with the NetBotz 250 logo, 'Rack Monitor', and a 'No Alarms' status. Below the header is a navigation bar with links for Home, Status, Control, Configuration, Tests, Logs, and About. The main content area is divided into two sections: 'Event Log Filtering' and 'Event Log'. The 'Event Log Filtering' section has two radio buttons: 'Last' (selected) and 'From'. Under 'Last', there is a dropdown menu set to '2 hours'. Under 'From', there are input fields for date and time: '09/05/2018 13:42' to '09/05/2018 15:42'. Below these are buttons for 'Apply', 'Clear Log', 'Filter Log', and 'Launch Log in New Window'. The 'Event Log' section has a floppy disk icon for saving. Below it is a table with columns 'Date', 'Time', 'User', and 'Event'. The table contains two entries: one for '09/05/2018 15:42:02' by user 'apc' with the event 'Configuration change. Event log web display time selection.', and another for '09/05/2018 14:56:39' by user 'apc' with the event 'Web user 'apc' logged in from 10.218.125.126.'. At the bottom of the page, there is a footer with 'APC's Web Site | Testdrive Demo | APC Monitoring' and '© 2019, Schneider Electric. All rights reserved. Site Map | Updated: 09/05/2018 at 15:42'.

The Event Log lists the most recent events, including the date and time each event occurred, in reverse chronological order. System events are logged for most activities, including abnormal internal system events.

- To view details about what events are logged, go to **Configuration > Notification > Event Actions > By Event**.
- To disable event logging based on severity or event category, go to **Configuration > Notification > Event Actions > By Group**.
- To open or save the log in a text file, click the floppy disk icon (📁) on the right side, on the same line as the **Event Log** heading.

Color code the event log

You can configure event log color coding on a per-user basis.

Red text indicates a critical alarm event; orange indicates a warning event; blue text indicates an informational event; and green indicates a clearing event.

To enable color coding for a specific user:

1. Go to **Configuration > Security > Local Users > Management**, and select the user to configure.
2. In the **User Preferences** section, check the box to enable **Event Log Color Coding**.

Filter the event log

By default, the Event Log displays the most recent events first. To see the event log in a Web page, click **Launch Log in New Window**.

NOTE: JavaScript must be enabled in your browser to do this.

To display the entire event log, or to change the number of days or weeks for which event log information is displayed, select **Last**, choose an option from the drop-down list, and click **Apply**.

To display events logged during a specific time range, select **From**, specify the beginning and ending dates and times for which to display events, then click **Apply**.

NOTE: Enter the time using the 24-hour clock format.

Delete the event log

To delete all events recorded in the log, click **Clear Log**. Deleted events cannot be retrieved.

Reverse lookup

Path: Logs > Events > Reverse Lookup

When a network-related event occurs, reverse lookup logs both the IP address and, if a domain name entry exists, the domain name for the networked device associated with the event in the event log. Reverse lookup is disabled by default.

Enable this feature unless you have no DNS server configured or have poor network performance because of heavy network traffic.

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 in systems using Bootp or DHCP device configuration, enabling reverse lookup can improve your ability to identify the networked devices that are causing events.

Event log size

Path: Logs > Events > Size


Specify the size of the event log by number of events. The minimum number of events is 25, and the maximum is 1500. Resizing the Event Log also deletes all current log entries. Before you resize the log, you can offload the Event Log via FTP or SCP.

Data Log

Path: Logs > Data > Log

Each entry in the data log is listed by the date and time the data was recorded, with the data under the abbreviated column headings.

Use **Data Log Filtering** to omit information you do not want to display. Use the **Filter Log** drop-down list or limit the data to a single device, or use the **Last** or **From** radio buttons to filter the data log by date or time.

To open or save the log in a text file, click the floppy disk icon () on the right side, on the same line as the **Data Log** heading.

NOTE: You can also use FTP or SCP to retrieve the data.txt file, and import it into a spreadsheet, or other graphic software. See “Use FTP or SCP to Retrieve Log Files” on page 118 for detailed instructions.

Graph the data log

Path: Logs > Data > Graphing

Graphing large amounts of logged data may cause performance problems. Reduce the number of data points or data lines being graphed to improve performance.

Setting	Description
Graph Data	To graph multiple data items, select the column heading to specify the data to graph.
Graph Time	To graph all records, or to change the number of hours, days, or weeks for which data log information is graphed, select Last . Select an option from the drop-down list, then click Apply . To graph data logged during a specific time range, select From . Specify the beginning and ending dates and times for which to graph data, then click Apply . NOTE: Enter the time using the 24-hour clock format.
Apply	View the graph.
Cancel	Discard your changes.
Launch Graph in new Window	Display the graph in a new browser window that provides a full-screen view.
Change Data Filter	Use the drop-down list or limit the data to a single device.

Graph. At the lowest magnification, all data is displayed and you cannot move left or right. At higher magnification levels, left/right movement is allowed. The blue bar between the left and right arrows changes size to indicate how many of the total data records are being displayed, and their relative location. The blue bar is not a scroll bar; click any part of the gray line or blue bar to re-center the graph.

If the data items have the same unit of measurement, the units are displayed on the left side of the graph. If the data items do not have the same units, the units are displayed in the legend with their corresponding data item.

Graph Data Lines. Graph data lines are a visual representation of the stored data records. Move your cursor over any horizontal line to view the date and time, and the Y axis value for that data record. Click any point in the graph to center and magnify that point on the screen.

Data log collection interval

Path: Logs > Data > Interval

The system calculates and displays the length of time data is kept based on the interval and the data log size.

You can modify how often data is recorded. Decrease the interval time to record data more frequently, and keep the record for a shorter time. Increase the interval time to record data less frequently, and keep the record for a longer time.

To save the data log periodically to an FTP server, use the Rotation option.

Configure data log rotation

Path: Logs > Data > Rotation

There is a limited amount of solid state storage in the Rack Monitor 250. You can use Data Log Rotation to periodically back up the data log to an FTP server to avoid data loss from the system automatically deleting your data.

The file name and location must be specified, and new information is appended onto the specified file on the FTP server. You can password protect the data log repository if needed.

Setting	Description
Last Upload Result	Indicates whether the last upload of the data file to the FTP server succeeded or failed, or displays "None Available."
Data Log Rotation	Check to enable data log rotation.
FTP Server	The IP address or host name of the FTP server.
User Name	The user name required to send data to the stored log file. This user must also have read and write access to the stored log file and the directory (folder) where it is stored.
Password	The FTP server password required to send data to the stored log.
File Path	The path to the stored log file on the FTP server. You must specify a path that already exists on the FTP Server.
Filename	The file name where the log is saved. NOTE: Data is appended to the file, with no overwriting.
Unique Filename	If this option is selected, the log is saved to daily log files named by including the date as part of the filename. The file name is in the format MMDDYYYY_filename.txt, where filename is user configurable and MMDDYYYY represents the NMC date. NOTE: Data is appended to the file if the data records are from the same day, with no overwriting. Verify that the file size does not become too large for available disc space.
Parameters	Define the following: <ul style="list-style-type: none">• The interval to upload the data log to the server.• If an upload fails, how frequently to retry.• The maximum number of times the upload will be retried before being skipped.
Upload Now	Initiate the first upload immediately.

Data log size

Path: Logs > Data > Size

Specify the maximum size (number of entries) of the data log. When you resize the data log, all existing log entries are deleted. It is recommended that you retrieve the existing entries using the web, FTP or SCP before you resize the log.

After the data log reaches the maximum size, the oldest entries are deleted from the log as new entries are logged.

Use FTP or SCP to Retrieve Log Files

An Administrator or Device User can use **FTP** or **SCP** (if enabled) to retrieve an **event log** file (event.txt) or **data log** file (data.txt).

The file reports all events or data recorded since the log was last deleted or truncated after reaching maximum size.

NOTE: This file includes information not available to you in the Web UI. You can use SCP to retrieve the log file using encryption-based security protocols; retrieval by FTP is unencrypted.

Use FTP to retrieve event.txt or data.txt

Some FTP clients require a colon instead of a space between the IP address and the port number.

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

1. At the command prompt, type `ftp` and the Rack Monitor 250's IP address, and press ENTER.
`ftp>open ip_address port_number`

NOTE: For enhanced security, use a non-default port value. See "FTP server" on page 103 for more information. The default **Port** setting for the **FTP Server** is 21; if changed, use the current value.

2. Enter the **User Name** and **Password** for either Super User, Administrator, Device User or Read-Only.

NOTE: Credentials are case-sensitive.

3. Use the **get** command to retrieve 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.

FTP delete

You can clear the contents of either log via FTP. You will not be asked to confirm the deletion. If you clear the data log, the event log records a deleted-log event. The new event.txt file records the event.

After logging in, use the **del** command:

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

or

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

Use SCP to retrieve event.txt or data.txt

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

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

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

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

Firewall Log

Path: Logs > Firewall

This page contains a log of active Firewall Policies. Log entries contain information about the traffic and the rules action (allowed, discarded). These events are not logged in the main Event Log. The firewall log is cleared when the Rack Monitor 250 reboots.

About the Rack Monitor 250

Network

Path: About > Network

Customer Support uses the hardware and software information on this page to help troubleshoot problems with the Rack Monitor 250.

You can view: model number, serial number, hardware revision, manufacture date, MAC address, APC by Schneider Electric OS (AOS), Application Module (APP), and Boot Monitor (Bootmon) information.

Support

Path: About > Support

Access various support websites and consolidate data into a single zipped file for troubleshooting and customer support. The data includes the event and data logs, the configuration file (see “How to Export Configuration Settings” on page 122”), and complex debugging information.

Creating the support file is a two step process:

1. Click **Generate Logs** to gather and compress the data. This process can take several minutes. See the progress bar.
2. Click **Download** to transfer the compressed file to your computer. The file is now ready to send to Customer Support.

Available Data Includes:

- **Support Resources:** Contact e-mail addresses, websites, and phone numbers for additional sales, customer service, or technical support questions.
- **Technical Support Debug Information Download:** This feature captures an assortment of debug data into a single file and then allows the user to download that file to a local computer which is intended for technical support use.
- **Generate Logs:** A new internal debug archive containing various files for subsequent download and review by technical support is generated.
- **Download:** Initiates a download of the currently stored debug archive.

NOTE: Make sure you have previously clicked the “Generate Logs” button if no file is downloaded.

For problems not described here, or if the problem persists, contact **Worldwide Customer Support**, www.apc.com/support.

Device IP Configuration Wizard

The Device IP Configuration Wizard can discover Rack Monitor 250s that do not have an IP address assigned. Once discovered, you can configure the IP address settings for the cards. You can also search for devices already on the network by entering an IP range to define the search. The Utility scans the IP addresses in the defined range and discovers Rack Monitor 250 that already have a DHCP-assigned IP address.

NOTE: For detailed information on the Wizard, see FAQ article FA156064 on www.apc.com.

NOTE: To use the DHCP Option 12, see FAQ article FA156110 on www.apc.com.

System requirements

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

NOTE: Administrator access is required to run the Device IP Configuration Wizard.

Installation

To install the Device IP Configuration Wizard from a downloaded executable file

1. Go to <http://www.apc.com/tools/download>. In the **Filter By Software/Firmware** drop-down list, select **Software Upgrades - Wizards and Configurators**. Click **Submit**.
2. Download the Device IP Configuration Wizard.
3. Run the downloaded executable file.

When installed, the Device IP Configuration Wizard is available through the Windows Start menu options.

How to Export Configuration Settings

A Super User or Administrator can retrieve the .ini file of a Rack Monitor 250 and then export it to one or more Rack Monitor 250s. A .ini file can also be useful for backup purposes, in case of a future device failure. The basic procedure to retrieve and export a .ini file is below. See the following sections for details.

1. Configure a Rack Monitor 250 to have the settings you want to export.
2. Retrieve the .ini file from that Rack Monitor 250 using the Web UI (see “Use a configuration file (.ini)” on page 110) or FTP (see “Use FTP to retrieve the .ini file” on page 122).
3. Customize the file to change at least the TCP/IP settings. (See “Customize the .ini file” on page 122.)

NOTE: Retain the original customized file for future use. Each receiving Rack Monitor 250 network card uses the file to reconfigure its own settings, and then deletes it. **The file that you retain is the only record of your comments.**

4. Use a file transfer protocol supported by the Rack Monitor 250 to transfer a copy to one or more other Rack Monitor 250s. For a transfer to multiple Rack Monitor 250s, use an FTP or SCP script or the .ini file utility (see).

NOTE: The .ini file utility is available for download from the FAQ article [FA156117](#) on www.apc.com.

Contents of the .ini file

The config.ini file you retrieve from a Rack Monitor 250 contains the following:

- section headings and keywords (only those supported for the 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 equals sign and a value (either the default or a configured value).
- The `Override` keyword: With its default value, this keyword prevents the exporting of one or more keywords and their device-specific values, e.g., 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

Use FTP to retrieve the .ini file

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

1. If possible, use the interface of the Rack Monitor 250 to configure it with the settings to export. Directly editing the .ini file risks introducing errors.
2. To use FTP to retrieve config.ini from the configured Rack Monitor 250:
 - a. Open a connection to the Rack Monitor 250, using its IP Address:

```
ftp> open ip_address
```

- b. Log on using the Super User/Administrator user name and password.

- c. Retrieve the config.ini file containing the Rack Monitor 250's settings:

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

NOTE: By default, the file is written to the folder from which you launched FTP.

Customize the .ini file

Using a text editor, customizable features and meta data of the file include:

- Comments
 - Start each comment line with a semicolon (;)
- Section Headings, Keywords, and Pre-defined values
 - Not case-sensitive (defined string values are case-sensitive).

Enclose in quotation marks any values that contain leading or trailing spaces, or happen to have already been in quotation marks.

- Adjacent quotation marks indicate no value.
`LinkURL1=""`
- Indicates that the URL is intentionally undefined.
- To export:
 - Scheduled Events: Configure the values directly in the .ini file
 - System Time: Export the [SystemDate/Time] section as a separate .ini file. Alternatively, access the Network Time Protocol server, and configure `enabled` for `NTPEnable`:

```
NTPEnable=enabled
```

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.**

Export the .ini file

Export the .ini File to a Single Rack Monitor 250.

- Navigate to **Configuration > General > User Config File**. Click **Choose File**. In the navigation window, enter the full path of the file, or browse to the file location.
- Use any file transfer protocol supported by Rack Monitor 250s, i.e., FTP, FTP Client, SCP, or TFTP. The following example uses FTP:

- a. From the folder containing the copy of the customized .ini file, use FTP to log in to the Rack Monitor 250 to which you are exporting the .ini file:

```
ftp> open ip_address
```

- b. Export the copy of the customized .ini file to the rootdirectory of the receiving Rack Monitor 250:

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

Export the .ini File to Multiple Rack Monitor 250s.

- Use FTP or SCP, but write a script that incorporates and repeats the steps used for exporting the file to a single Rack Monitor 250.
- Use a batch processing file and the .ini file utility.

To create the batch file and use the utility, see FAQ article FA156117on www.apc.com.

The Upload Event and Error Messages

After the Rack Monitor 250 updates its settings using the .ini file, the user will see:

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

Errors generated by overridden values

The `Override` keyword and its value will generate error messages in the event log when it blocks the exporting of values. See “Contents of the .ini file” on page 122 for information about which values are overridden.

Because the overridden values are device-specific, ignore these messages as they are not applicable to or relevant for other Rack Monitor 250s. To prevent these error messages, you can delete the lines that contain the `Override` keyword and the lines that contain the values that they override. Do not delete or change the line containing the section heading.

Related Topics

On Windows operating systems, instead of transferring .ini files, you can use the Device IP Configuration Wizard to update the basic TCP/IP settings of Rack Monitor 250s and configure other settings through their user interface. See “Device IP Configuration Wizard” on page 121 for more information.

CLI Script File (.csf) Settings

A CLI script file is a configuration file with a '.csf' extension that contains CLI commands. The primary purpose of the CLI script file is to mass configure user accounts.

The file must contain one command per line. The syntax used must match the CLI format of the network interface. Send the file via FTP or SCP to the Rack Monitor 250 to process the commands.

Example: To configure users newadmin, newdevice and newdev1, enter:

```
user -n newadmin -pw apc -pe administrator -e enable
user -n newdevice -pw apc -pe device -e enable
user -n newdev1 -pw dv1 -pe device -e enable
```

Firmware Upgrades

When you upgrade the firmware on the Rack Monitor 250:

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

Regular upgrades also ensures that all Rack Monitor 250s support the same features, in the same manner. Obtain the free, latest firmware version from www.apc.com/tools/download

Firmware Module Files

A firmware version has three modules, and they must be upgraded (placed on the Rack Monitor 250) in this order:

Order	Module	Description
1	Boot Monitor (bootmon)	Roughly equivalent to the BIOS of a PC
2	APC by Schneider Electric Operating System (AOS)	Can be thought of as the Rack Monitor 250 operating system
3	Application Module	Specific to the device, e.g. the Rack Monitor 250

(Each module contains one or more Cyclical Redundancy Checks (CRCs) to protect its data from corruption).

The naming convention used for the APP Module and AOS indicate the context, the firmware version, type, and version number. This information is also useful for troubleshooting and enables you to determine if updated firmware is available at www.apc.com.

The APP Module name differs according to the device type. The AOS module is always named `aos`, and the boot monitor module is always named `bootmon`.

Version numbers of the firmware modules may differ, but compatible modules are released together. Never combine APP Module and AOS modules from different releases.

NOTE: If the bootmon must be updated, a bootmon module is included in the firmware release. Otherwise, the bootmon module that is installed on the card is compatible with the firmware update.

NOTE: When you transfer individual firmware modules, Bootmon must precede AOS, if bootmon update is required. The AOS module must be transferred to the Rack Monitor 250 before you transfer the APP Module.

The bootmon, the AOS, and the App Module file names share the same basic format:

- `apc_hardware-version_type_firmware-version.bin`
- `apc`: Indicates the context.
- `hardware-version`: `hw0n` where `n` identifies the hardware version on which you can use this file.
- `type`: Identifies which module.
- `version`: The version number of the file.
- `bin`: Indicates that this is a binary file

Firmware File Transfer Methods

Use one of these three methods:

- **Firmware Upgrade Utility on Windows.** On a Windows operating system, use the **Firmware Upgrade Utility** downloaded from www.apc.com.
- **Use FTP or SCP.** Use **FTP or SCP** to transfer the individual AOS and App Module firmware. To upgrade multiple Rack Monitor 250s using an FTP client or using SCP, write a script which automatically performs the procedure.
- **Export configuration settings.** You can create batch files and use a utility to retrieve configuration settings from multiple Rack Monitor 250s and export them to other Rack Monitor 250.
- **Use XMODEM through a serial connection.** Use **XMODEM** through a serial connection to transfer the individual firmware modules from your computer to the Rack Monitor 250. This method is also one which works with a Rack Monitor 250 NOT on your network.

Use the Firmware Upgrade Utility on Windows systems

On any supported Windows operating system, the Firmware Upgrade Utility automates the transferring of the firmware modules, in the correct module order. The utility only works with an Rack Monitor 250 that has an IPv4 or IPv6 address.

Unzip the downloaded firmware upgrade file and double-click the .exe file. Then enter the IP address, the user name, and the password in the dialog fields and click **Upgrade Now**. You can use the **Ping** button to test your entered details. To execute multiple upgrades on Windows, see “Use the Firmware Upgrade Utility for Multiple Upgrades on Windows” on page 129.

Use the Utility for Manual Upgrades, Primarily on Linux.

On non-Windows operating systems, the Firmware Upgrade Utility extracts the individual firmware modules, but does not upgrade the Rack Monitor 250. See “Firmware File Transfer Methods” for the different upgrade methods after extraction.

To extract the firmware files:

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

Use FTP to Upgrade the Rack Monitor 250

Before you begin:

- The Rack Monitor 250 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 see “FTP server” .
- This procedure assumes bootmon does not need upgrading. It is always necessary to upgrade the other two.

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

1. The firmware module files must be extracted, see See “Use the Utility for Manual Upgrades, Primarily on Linux.” on page 127.
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
```

For file information, See “Firmware Module Files” on page 126.

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 in using an account with the correct level of user access to perform file transfers (**apc** is the default user name and password).

6. Upgrade the AOS. (Always upgrade the AOS before the App Module).

```
ftp> bin
```

```
ftp> put apc_hw05_aos_ nnn.bin (where nnn is the firmware version number)
```

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

8. After 20 seconds, repeat step 3 through step 7, using the App Module file name at step 6.

Use SCP to Upgrade the Rack Monitor 250

To use Secure CoPy (SCP) to upgrade firmware for the Rack Monitor 250, follow these steps.

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

This procedure assumes bootmon does not need to be upgraded, it is always necessary to upgrade the other two though:

1. Locate the firmware modules, see See “Firmware Module Files” on page 126..
2. Use an SCP command line to transfer the AOS firmware module to the Rack Monitor 250. The following example uses *nnn* to represent the version number of the AOS module:

```
scp apc_hw05_aos_ nnn.bin apc@158.205.6.185:apc_hw05_aos_ nnn.bin
```

3. Use a similar SCP command line, with the name of the App Module, to transfer the App Module firmware to the Rack Monitor 250. (Always upgrade the AOS before the App Module).

Use XMODEM to Upgrade the Rack Monitor 250

To use XMODEM to upgrade one Rack Monitor 250 that is not on the network, you must extract the firmware files with the Firmware Upgrade Utility (see “Use the Utility for Manual Upgrades, Primarily on Linux.”).

To transfer the files (this procedure assumes bootmon does not need upgrading, it is always necessary to upgrade the other two though):

1. Select a serial port at the local computer and disable any service that uses the port.
2. Connect the provided USB A-USB mini B cable to the selected port and to the serial port at the Rack Monitor 250
3. Run a terminal program such as HyperTerminal, and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control.
4. Press the **Reset** button on the Rack Monitor 250, then immediately press the **Enter** key twice, or until the Boot Monitor prompt displays: `BM>`
5. Type `XMODEM`, then press `ENTER`.
6. From the terminal program’s menu, select `XMODEM`, then select the binary AOS firmware file to transfer using `XMODEM`.
After the `XMODEM` transfer is complete, the Boot Monitor prompt returns:
(Always upgrade the AOS before the App Module).
7. To install the App Module, repeat step 5 and step 6. In step 6, use the App Module file name.
8. Type `reset` or press the **Reset** button to restart the Rack Monitor 250’s network interface.

Use the Firmware Upgrade Utility for Multiple Upgrades on Windows

After downloading the Upgrade Utility from the Firmware downloads page on the www.apc.com website, double click on the .exe file to run the utility and follow these steps to upgrade your Rack Monitor 250 firmware:

1. In the utility dialog, type in an IP address, a user name, and a password, and choose the **Ping** button if you need to verify the IP address.
2. Choose the **Device List** button to open the `iplist.txt` file. Here you should type all devices to upgrade with the necessary information: IP, user name, and password.

Example:

```
SystemIP=192.168.0.1
SystemUserName=apc
SystemPassword=apc
AllowDowngrade=0
```

NOTE: You can use an existing `iplist.txt` file if it already exists. `AllowDowngrade=1` is also a valid value, in reference to the above example.

3. Select the **Upgrade From Device List** check box to use the `iplist.txt` file.
4. Choose the **Upgrade Now** button to start the firmware version upgrade(s).
5. Make sure to save the file after editing is complete. Choose **View Log** to verify any upgrade.

Verify Upgrades

Verify the Success of the Transfer

To verify whether a firmware upgrade succeeded, use the `xferStatus` command in the CLI to view the last transfer result.

Alternatively, you can 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.

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

Verify the Version Numbers of Installed Firmware

About > Network

Use the Web UI to verify the versions of the upgraded firmware modules. You could also use an SNMP GET to the MIB-2 `sysDescr` OID. In the CLI, use the `about` command.

Wireless Firmware Upgrades

1. Download the NetBotz Wireless Firmware Update Utility: go to **www.apc.com**, and select **Support > Resources & Tools > Software/Firmware**. Under **Filter by Software/Firmware**, select **Software Upgrades - Software for NetBotz appliances**.
2. Install the Utility as an administrator.
3. Remove the plastic cover over the Wireless port. Remove the coordinator and connect it to a USB port on the computer where you installed the Utility.
NOTE: The coordinator must remain within range of the wireless sensors to upgrade the sensors.
4. Record the MAC address of the Wireless Temperature Sensor that came with the Rack Monitor 250. Turn on the Wireless Temperature Sensor.
5. Run the Utility as an administrator.
NOTE: The Utility may not operate correctly if you do not select Run as Administrator.
NOTE: If you are unable to launch the utility, you may need to install a serial-to-USB virtual COM port driver on your computer. The required driver is available in the drivers folder of the Utility.
6. Enter the MAC address of the Wireless Temperature Sensor in the commission list field. If you have more than one wireless sensor, make sure they are all turned on, and add their MAC addresses also.
7. Click **OK** to start the utility.
8. Browse to the wireless firmware .zip file installed with the utility.
9. Click **Apply** to update the wireless sensor firmware.
10. When the firmware update is complete, reconnect the Coordinator to the Rack Monitor 250 Wireless port and replace the plastic cover. **DO NOT** connect the Coordinator to any other USB port on the appliance.

Troubleshooting

Rack Monitor 250 Access Problems

For problems that are not described here, or if the problem still persists, contact **Worldwide Customer Support**.

Problem	Solution
Unable to ping the Rack Monitor 250	<p>The Rack Monitor 250 supports the ability to disable IPv4 Ping Response for security reasons.</p> <p>This setting is located in the Web UI under Configuration > Security > Ping Response or can be located in config.ini. Check this setting or verify other access methods such as HTTPS, FTP, Telnet, or SSH.</p> <p>If the Rack Monitor 250's 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:</p> <p>Verify all network connections. Verify the IP addresses of the Rack Monitor 250 and the NMS.</p> <p>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).</p> <p>Verify the number of subnet bits for the Rack Monitor 250's subnet mask.</p>
Cannot allocate the communications port through a terminal program	<p>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.</p>
Cannot access the CLI through a USB serial connection	<p>Make sure a USB A-USB mini B cable is connected to the correct USB port.</p> <p>Make sure that the baud rate is configured correctly: 9600, 81N.</p>
Cannot access the CLI remotely	<p>Make sure you are using the correct access method, Telnet or Secure SHell (SSH). An Administrator can enable these access methods. By default, Telnet is enabled. SSH and Telnet can be enabled/disabled independently.</p> <p>For SSH, the Rack Monitor 250 may be creating a host key. The Rack Monitor 250 takes several minutes to create the host key, and SSH is inaccessible during that time.</p>
Cannot access the Web UI	<p>Verify that HTTP or HTTPS access is enabled. Check your browser's proxy settings.</p> <p>Make sure the URL is consistent with the security system used by the Rack Monitor 250. SSL requires https, not http, at the beginning of the URL.</p> <p>Verify that you can ping the Rack Monitor 250.</p> <p>Verify that you are using a supported Web browser. If available, try a different Web browser. See "Web User Interface" on page 56.</p> <p>If the Rack Monitor 250 has just restarted and SSL security is being set up, the Rack Monitor 250 may be generating a server certificate. The Rack Monitor 250 may take up to several minutes to create this certificate, and the SSL server is not available during that time.</p>

SNMP Issues

Problem	Solution
Unable to perform a GET	Verify the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3). Use the CLI or Web UI to ensure that the NMS has access. See “SNMPv1 configuration” on page 99 and “SNMPv3 configuration” on page 101.
Unable to perform a SET	Verify the read/write (SET) community name(SNMPv1) or the user profile configuration (SNMPv3). Use the CLI or the Web UI to ensure that the NMS has write (SET) access (SNMPv1) or is granted access to the target IP address through the access control list (SNMPv3). See “SNMPv1 configuration” on page 99 and “SNMPv3 configuration” on page 101.
Unable to receive traps at the NMS	<p>Make sure the trap type (SNMPv1 or SNMPv3) is correctly configured for the designated NMS as a trap receiver.</p> <p>For SNMP v1, query the mconfigTrapReceiverTable APC 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.</p> <p>If either is not correct, use SETs to the mconfigTrapReceiverTable OIDs, or use the CLI or Web UI to correct the trap receiver definition.</p> <p>For SNMPv3, check the user profile configuration for the NMS, and run a trap test.</p> <p>See See “SNMPv1 configuration” on page 99, “SNMPv3 configuration” on page 101, “SNMP trap receivers” on page 108”, and “Event actions” on page 104.</p>
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.

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. All advertising materials mentioning features or use of this software must display the following acknowledgment:
4. This product includes software developed by the University of California, Berkeley and its contributors.
5. 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.

Worldwide Customer Support

Customer support for this product is available at www.apc.com.³

© 2019 APC by Schneider Electric. All Rights Reserved. APC, the APC logo, NetBotz, and StruxureWare are trademarks owned by Schneider Electric Industries, S.A.S. All other trademarks are property of their respective owners.