NetBotz®

Rack Monitor 250

User's Guide

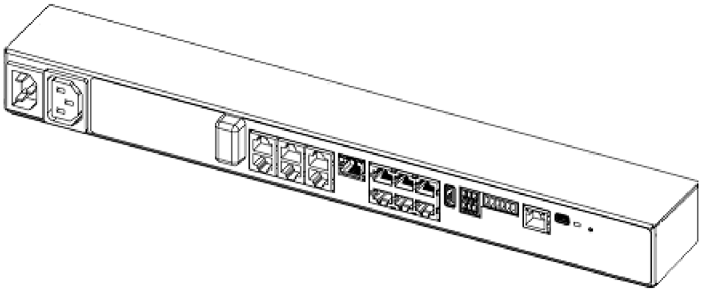
NBRK0250

NBACS0125

NBACS1356

990-9890A

Publication Date: March 2017



APC™ by Schneider Electric

Schneider Electric Legal Disclaimer

The information presented in this manual is not warranted 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, 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 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 SCHNEIDER ELECTRIC, OR ANY PARENT, AFFILIATE OR SUBSIDIARY COMPANY OF 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 SCHNEIDER ELECTRIC HAS BEEN EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. 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.

Table of Contents

Introduction

Product Features

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 six ports for connecting temperature and humidity sensors, and other sensors including fluid detection sensors and third-party dry contact sensors. Using other ports on the Rack Monitor 250, you can connect two door switch sensors, two rack door handles, a beacon, and temperature and humidity sensors with digital display.

To expand your system, you can 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, and use ports that provide power to or allow control of other devices.

NOTICE: The Rack Monitor 250 cannot be connected to or networked with any other NetBotz appliances. It uses unique software that is not compatible with other NetBotz products.

See the NetBotz Rack Monitor 250 Installation and Quick Configuration and manual for more information.

The NetBotz 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)

Getting Started

Initial Setup

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

- IP address of the NetBotz 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 NetBotz Rack Monitor 250 and that is usually running. The NetBotz 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 NetBotz 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 in PDF on www.apc.com.

Access

You can log on using the following methods:

1. Local access to the *Command Console* from a computer with a direct *serial* connection.

   NOTICE: 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 web site.
   More more information, see APC Knowledge Base article FA158350.
2. Telnet or *Secure SHell* (*SSH*) access to the *Command Console* from a remote computer.
3. Web access; either directly or through *StruxureWare Data Center Expert*

User Account Overview

The NetBotz Rack Monitor 250 is initially configured with three User Types, and associated User Names:

- *Super User* (User Name: *apc*)
- *Device* (User Name: *device*)
- *Read-Only* (User Name: *readonly*).

The default password for each of these is *apc*. All levels of access require user name and password permissions.

Both user name and password are case-sensitive, and have a 64 byte maximum, supporting up to 64 ASCII characters; less for multi-byte languages.

The *Super User* can define additional user accounts, and set other variables for the additional users. It is generally recommended that non-default user name and passwords be set.

NOTE: 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.

To manage User settings from the web browser (accessed by entering the NetBotz Rack Monitor 250 IP address into the address bar), navigate to **Configuration > Security > Local Users > Management**.

- Click **Add User**

The User types that can be added are:

- **Administrator:** Administrator users have full access just as the Super User does, but this user type can be deleted.

  NOTE: A Super User account must be enabled before all administrator accounts are deleted or disabled.

- **Device:** Device users have read-write access to the device-related menus only. An Administrator can enable or disable Device user accounts.
- **Read-Only:** Read-Only Users have read-only access through the Web interface to view status, but not to control a device or change any configured value. An Administrator can enable or disable Read-Only user accounts.
- **Network-Only:** Network-Only users have read-write access to the network-related menus only. An Administrator can enable or disable Network-Only user accounts.

See “Local Users” on page 63 for more information.

Recovering a Lost Password

Select a USB port at the local computer and disable any service that uses that port. Connect a local computer to the NetBotz Rack Monitor 250 to that USB port.

NOTICE: 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 web site. For more information, see APC Knowledge Base article FA158350.

1. Connect the included USB A - USB mini B configuration cable to the selected port on the computer and to the console port at the NetBotz Rack Monitor 250.
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
```

4. 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.

5. 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 is flashing to temporarily reset the user name and password to their default values (apc/apc).
6. Press ENTER as many times as necessary to redisplay the User Name prompt, then use the default, apc, for the user name and password.

   NOTE: If you take longer than 30 seconds to log on, after pressing the reset button for the second time, you must repeat step 5 and log on again.
7. At the *Command Console*, 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 no longer supported via the *Command Console*. If a user's user name needs to be changed, it must be deleted and re-created. The *Super User* will also have access now to log in and adjust any other user's password.
8. Type `quit`, `exit`, or `bye` to log off. Remember to reconnect any USB cable you may have disconnected, and to restart any service you may have disabled.

Watchdog Features

Overview

To detect internal problems and recover from unanticipated inputs, the NetBotz 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 NetBotz Rack Monitor 250 implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the NetBotz 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 NetBotz Rack Monitor 250 does not restart if the network is quiet for 9.5 minutes, the NetBotz Rack Monitor 250 attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the NetBotz 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 NetBotz Rack Monitor 250 from restarting.

Automatic Logout

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

You can adjust he default logout time through the web interface **Configuration > Security > Local Users > Management**.

– Click the user name hyperlink for the account you want to change.

– Under *Session Timeout,* modify the number of minutes.

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

Command Console Access

You can access the NetBotz Rack Monitor 250 *Command Console* locally using a USB A - USB mini B *serial* connection, or remotely using a secured *Telnet* or *SSH* connection. *Telnet* provides the basic security of a user name and password; *SSH* encrypts all transmitted data, including user name and password. *Telnet* is enabled by default.

More information about *Telnet* and *SSH* is provided in subsequent sections. Access to the *Command Console* always requires providing an authentic user name and password. User name and password are case-sensitive.

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.

Serial Port Access to the Command Console

1. Select a USB port at the local computer, and disable any service that uses that port.

   NOTICE: 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 web site. For more information, see APC Knowledge Base article FA158350.
2. Connect the USB A - USB mini B configuration cable to the console port on the NetBotz Rack Monitor 250 and to the USB port of the computer.
3. Run a terminal program (HyperTerminal, etc.), configure the port as follows, and press `ENTER`, repeatedly if needed.

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

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

Remote Access to the Command Console through Telnet

1. Access a computer on the same network as the NetBotz Rack Monitor 250.
2. Open a terminal program that provides telnet support or type "`telnet`" and the IP address of the NetBotz Rack Monitor 250 at a DOS or command prompt and press ENTER.

   Example:

   ```
   telnet 139.225.6.133
   ```

   NOTE: The NetBotz Rack Monitor 250 uses Telnet port 23 by default. If the NetBotz 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.
3. Enter user name and password.

Remote Access to the Command Console through SSH

The only way to securely access the *Command Console* remotely is to use the *Secure Shell*, or SSH. Data transmitted over *SSH* is encrypted using SSL (Secure Sockets Layer) encryption.

Using *SSH* is optional, and it is not enabled by default. A properly configured *SSH* client must be installed on your computer.

The interface, user accounts, and user access rights are the same whether you access the *Command Console* through *SSH* or *Telnet*.

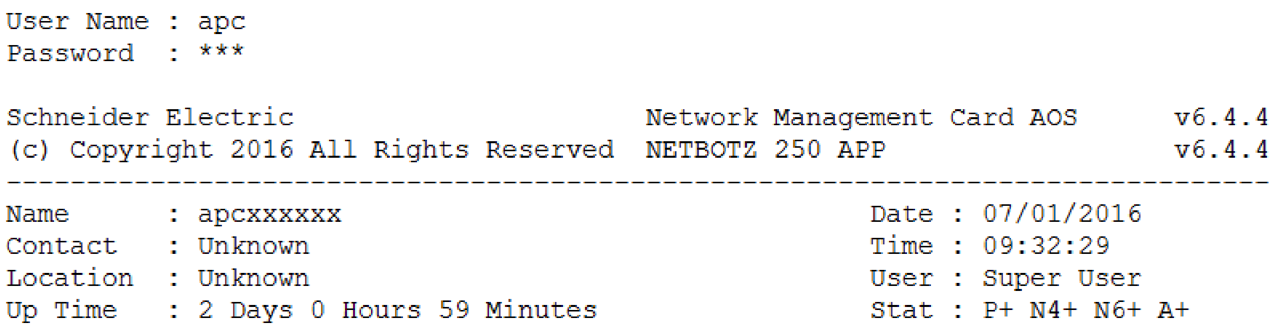
Command Line Interface (CLI)

Syntax and Implementation Overview

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 Command Console prompt.

CLI Prompt - The NetBotz Rack Monitor 250 CLI prompt is the fixed string “apc>” (apc<greater than>).

Example Login Screen



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

Schneider Electric                      Network Management Card AOS      v6.4.4
(c) Copyright 2016 All Rights Reserved  NETBOTZ 250 APP                  v6.4.4
-------------------------------------------------------------------------------
Name      : apcxxxxxx                                 Date : 07/01/2016
Contact   : Unknown                                   Time : 09:32:29
Location  : Unknown                                   User : Super User
Up Time   : 2 Days 0 Hours 59 Minutes                 Stat : P+ N4+ N6+ A+
```

- The operating system (Network Management Card AOS) and Application Module (NetBotz Rack Monitor 250 App) are the firmware versions of the device.

```
Network Management Card AOS      v6.4.4
NetBotz 250 APP                  v6.4.4
```

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

```
Name                  : apcxxxxxx
Contact               : Unknown
Location              : Unknown
```

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

```
Up Time  : 2 Days 0 Hours 59 Minutes
```

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

```
Date     : 07/01/2016
Time     : 09:32:29
```

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

```
User     : Super User
```

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

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

Alarm Status Field

The Stat field displays any active alarms for the NetBotz Rack Monitor 250 system.

`P+`	The operating system (AOS) is functioning properly.
`N4+` `N6+`	IPv4 AND IPv6 Network Status. The network is functioning properly.
`N4?` `N6?`	A BOOTP request cycle is in progress.
`N4-` `N6-`	The NetBotz Rack Monitor 250 failed to connect to the network.
`N4!` `N6!`	Another device is using the IP address of the NetBotz Rack Monitor 250.
`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 “Worldwide Customer Support” even if you can still access the NetBotz Rack Monitor 250.

Capitalization and Case Sensitivity

1. CLI commands and arguments ARE NOT case sensitive.
   Example:
   `portSpeed = PoRTsPeeD`

2. CLI options ARE case sensitive.
   Example:
   `-p ≠ -P`

Command Detection

If an entered command is not known, the following error message is displayed:

```
E101: Command Not Found.

Type “?” for a list of available commands. Type “<command> ?” for help
on a specific command.
```

CLI Login and Logout

When you first access the NetBotz Rack Monitor 250, you are always prompted to login. Enter your user name and password, each followed by a carriage return. If your user name and password are valid, you will be logged into the Command Console CLI.

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

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

Command Argument Syntax

Since each command varies in the number of arguments it supports, the following syntax is defined to indicate how arguments can be used.

Item	Description
-	Options are preceded by a hyphen
[...]	Square brackets […] denote optional arguments
<...>	greater/less than brackets <> denote user entered text
|	The “pipe symbol” denotes OR

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
```

Command Response Codes

Error Code Table

These response codes allow automated processes to detect error conditions without resorting to matching error text.

Code	Message	Notes
E000	Success	
E001	Successfully Issued	
E002	Success, Reboot Required	
E100	Command Failed	
E101	Command Not Found	
E102	Parameter Error	Reported when there is any problem with the arguments supplied to the command: too few, too many, wrong type, etc.
E103	Command Line Error	
E104	User Level Denial	
E105	Command Prefill	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 NetBotz Rack Monitor 250 has been lost
E200	Input error	Only reported when an error occurs during the execution of a command
E201	No Response	Reported when a sensor fails to respond
E202	User already exists	
E203	User does not exist	
E204	User does not have access to this command	
E205	Invalid target	User failed to input a target or target was out of range.

Prompting 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.

Command Editing

The <backspace> key deletes the last character of the command string you entered, and is the only editing function available to you during command entry.

History

The NetBotz Rack Monitor 250 CLI implements a command history buffer, recalling the 10 previous commands. You can navigate backwards and forwards through entered commands using the <up arrow> and <down arrow> keys respectively.

Auto Completion

The NetBotz Rack Monitor 250 CLI supports command auto-completion. If you enter a partial command, you can use the `<TAB>` key to complete the command to the first available matched command. If such a match exists, the command line shall be completed by the system.

Additional presses of the `<TAB>` key select the next available command match. Once you scroll through all available commands, the original partially entered command is displayed.

Delimiter

The NetBotz 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>
```

Command Console and CLI Response Format

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).

Response Format and Message Codes

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

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

See the Error Code Table on “Error Code Table” on page 11 for more information regarding Message Code Notes.

Example:

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

NetBotz Rack Monitor 250 System Command Descriptions

Interface Commands

Courier font is used to show the text output of the NetBotz Rack Monitor 250. Italicized Courier font is used to show user input to the NetBotz Rack Monitor 250. Text enclosed in '< >' is a variable name. The text '...' is used in several examples as a placeholder, shortening lengthy outputs. In these situations, the first two and last two lines of output is shown.

? 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>?
Network Management Card Commands:
---------------------------------------------------------------------
?           about       alarmcount  boot        cd          date
delete      dir         eventlog    exit        format      ftp
help        ping        portspeed   prompt      quit        radius
reboot      resetToDef  system      tcpip       user        web
xferINI     xferStatus
```

Example 2:

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

Error Message: `E000, E102`

about

Access: Super User, Administrator, Device User, Read Only, 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:        6/23/2016

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 NetBotz 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: Get/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 NetBotz Rack Monitor 250 turns on, resets, or restarts. See “TCP/IP” on page 68 for information about each boot mode setting.
-c	[<enable|disable>] (Require DHCP Cookie)	dhcp and dhcpBootp boot modes only. Enable or disable the requirement that the DHCP server provide the APC cookie.
-v	[<vendor class>]	Vendor Class is APC
-i	[<client id>]	The MAC address of the 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

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

Description: Exit the CLI

Parameters: None

Example:

```
apc>bye
Connection Closed - 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`

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 command line interface 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 command line interface.

Parameters:

Option	Argument	Description
-s	<enable | disable> (ssh)	Configure access to the command line interface, or use the `disable` command to prevent access. Enabling SSH also enables SCP and disables Telnet.
-t	<enable | disable>] (telnet)	
-pt	<telnet port n>	Define the Telnet port used to communicate with the NetBotz Rack Monitor 250 (23 by default).
-ps	<SSH port n>	Define the SSH port used to communicate with the NetBotz 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 command line interface, 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: 23
SSH Port:    22
Baud Rate:   9600
```

Error Message:

```
E000, E102
```

date

Access: Super User, Administrator

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

To configure an NTP server to define the date and time for the NetBotz Rack Monitor 250, see “Set the Date and Time” on page 90.

Parameters:

Option	Argument	Description
`-d`	`<“datestring”>`	Set the current date. The format must match the current `-f` setting.
`-t`	`<00:00:00>`	Configure the current time, in hours, minutes, and seconds. Use the 24-hour clock format.

`-f`	`mm/dd/yy |`
	`dd.mm.yyyy |`
	`mmm-dd-yy |`
	`dd-mmm-yy |`
	`yyyy-mm-dd`
		Select the numerical format in which to display all dates in this user interface. Each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.

`-z`	`<time zone offset>`	Set the difference with GMT 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, 2016, type:

```
date -d “2016-07-01”
```

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  2013 aos.bin

--wx-wx-wx  1 apc      apc      3145728 Jun 23 2013 app.bin

-rw-rw-rw-  1 apc      apc        45000 Jul 1 2016 config.ini

drwxrwxrwx  1 apc      apc            0 Mar 18 2013 ssl/

drwxrwxrwx  1 apc      apc            0 Mar 18 2013 ssh/

drwxrwxrwx  1 apc      apc            0 Mar 18 2013 logs/

drwxrwxrwx  1 apc      apc            0 Mar 18 2013 sec/

drwxrwxrwx  1 apc      apc            0 Mar 18 2013 dbg/

drwxrwxrwx  1 apc      apc            0 Mar 18 2013 fwl/

drwxrwxrwx  1 apc      apc            0 Mar 18 2013 rms/
```

. **Error Messages:** `E000`

dns

Access: Super User, Administrator, Network-Only User

Definition: 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:

```
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 NetBotz Rack Monitor 250, and the status of sensors connected to the NetBotz 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 command line interface.
ENTER	Update the log display. Use this command to view events that were recorded after you last retrieved and displayed the log.
SPACEBAR	View the next page of the event log.
B	View the preceding page of the event log. This command is not available at the main page of the event log.
D	Delete the event log. Follow the prompts to confirm or deny the deletion. Deleted events cannot be retrieved.

Example:

```
apc>eventlog
---- Event Log -----------------------------------------------------
     Date: 07/06/2016 Time: 13:22:26
     ------------------------------------
Date        Time      Event
     ---------------------------------------------------------------
     07/06/2016 13:17:22  System: Set Time.
     07/06/2016 13:16:57  System: Configuration change. Date format
                           preference.
     07/06/2016 13:16:49  System: Set Date.
     07/06/2016 13:16:35  System: Configuration change. Date format
                           preference.
     07/06/2016 13:16:08  System: Set Date.
     07/05/2016 13:15:30  System: Set Time.
     07/05/2016 13:15:00  System: Set Time.
     07/05/2016 13:13:58  System: Set Date.
     07/05/2016 13:12:22  System: Set Date.
     07/05/2016 13:12:08  System: Set Date.
     07/05/2016 13:11:41  System: Set Date.
<ESC>- Exit, <ENTER>- Refresh, <SPACE>- Next, <D>- Delete
```

Error Message: `E000, E100`

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

firewall

Access: Super User, Administrator

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

Parameters:

Parameters	Argument	Description
`-S`	`<enable | disable>`	Enable or disable the Firewall.
`-f`	`<file name to activate>`	Name of the firewall to activate.

`-t`	`<file name to test>`
	`<duration time in minutes>`
		Name of firewall to test and duration time in minutes.

`-fe`	No argument. List only	Shows active file errors.
`-te`	No argument. List only	Shows test file errors.
`-c`	No argument. List only	Cancel a firewall test.
`-r`	No argument. List only	Shows active firewall rules.
`-l`	No argument. List only	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, Device User, Read Only, 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> (valid ranges are: 21 and 5000-32768)`	Define the TCP/IP port that the FTP server uses to communicate with the NetBotz Rack Monitor 250 (21 by default). The FTP server uses both the specified port and the port one number lower than the specified port.
`-S`	`enable | disable`	Configure access to the FTP server.

Example:

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

```
apc>ftp -p 5001

E000: Success



apc>ftp

E000: Success


Service: Enabled

Ftp Port: 5001



apc>ftp -p 21

E000: Success
```

Error Message: `E000, E102`

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 `help`.

Parameters: None

Example 1:

To view a list of commands available to a Device User, type:

```
help
```

Example 2:

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

```
alarmcount help
```

Error Message: None

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 NetBotz 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: `logzip [-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, Device User, Read Only, 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, and 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:

<table>
<tr><th>Option</th><th>Arguments</th><th>Description</th></tr>
<tr><td>-s</td><td>auto | 10H | 10F | 100H | 100 F</td><td>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 70 for more information about the port speed settings.</td></tr>
<tr><td colspan="2">H = Half Duplex
F = Full Duplex</td><td>10 = 10 Meg Bits
100 = 100 Meg Bits</td></tr>
</table>

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

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 interface of the NetBotz Rack Monitor 250.

For a summary of RADIUS server configuration and a list of supported RADIUS servers, see “TCP/IP” on page 68.

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 NetBotz 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 NetBotz Rack Monitor 250.
`-t1` `-t2`	`<server timeout>`	The time in seconds that the NetBotz Rack Monitor 250 waits for a response from the primary or secondary RADIUS server.

Example 1:

To view existing RADIUS settings for the NetBotz 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 NetBotz 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 'YES' 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 NetBotz 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
session	[-d <session ID>] (Delete)
-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> [1]
-a	<enable | disable> (Authentication)
-u	<User Name>
-w	<Password>
-e	<none | ifavail | always | implicit> (Encryption)
-c	<enable | disable> (Require Certificate)
-i	<Certificate File Name>
[1] Port options are 25, 465, 587, 5000 to 32768	

Example:

```
apc>smtp
E000: Success
From:          address@example.com
Server:        mail.example.com
Port:          25
Auth:          disabled
User:          User
Password:      <not set>
Encryption:    none
Req. Cert:     disabled
Cert File:     <n/a>
```

Error Message: `E000, E102`

snmp

Access: Super User, Administrator,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 NetBotz 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]	<Crypth phrase>	Crypthphrase 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> [language code]
-t[n]	<Trap Type> [snmpV1 | snmpV3]]
-g[n]	<Generation> [enable | disable]
-a[n]	<Auth Trap> [enable | disable]
-u[n]	<profile1 | profile2 | profile3 | profile4> (User Name)
n=Trap receiver # = 1,2,3,4,5 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 "Syntax and Implementation Overview" on page 8 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 NetBotz 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>] (system-hostname sync)	Allow the host name to be synchronized with the system name so both fields automatically contain the same value. **NOTE:** When enabling this feature, the system name identifier can no longer contain a space character (since it will be synchronized to the host name field).

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 NetBotz Rack Monitor 250.

Parameters:

Option	Argument	Description
`-i`	`<IP address>`	Type the IP address of the NetBotz Rack Monitor 250 using the format *xxx.xxx.xxx.xxx*
`-s`	`<subnet mask>`	Type the subnet mask for the NetBotz 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 NetBotz Rack Monitor 250 will use.
`-S`	`enable | disable`	Enable or disable IPv4.

Example 1:

To view the network settings of the NetBotz 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 NetBotz 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 NetBotz 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 NetBotz Rack Monitor 250.
`-auto`	`enable | disable`	Enable the NetBotz Rack Monitor 250 to automatically configure the IPv6 address.
`-i`	`<IPv6 address>`	Set the IPv6 address of the NetBotz 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 NetBotz 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 NetBotz 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 “User Account Overview” on page 3.

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		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`

userdflt

Access: Super User, Administrator

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

- Determine 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> (Enable)`	By default, user will be enabled or disabled upon creation. Remove (Enable) from the end
`-pe`	`<Administrator | Device | Read-Only | Network-Only> (user permission)`	Specify the user's permission level and account type.
`-d`	`<user description>`	Provide a user description.
`-st`	`<session timeout> minute(s)`	Provide a default session timeout.
`-bl`	`<bad login attempts>`	Number of incorrect login attempts a user has before the system disables their account. Upon reaching this limit, a message is displayed informing the user the account has been locked. The Super User or an Administrator-level account is needed to re-enable the account to allow the user to log back in. **NOTE:** A Super User account cannot be locked out, but can be manually disabled if necessary.
`-el`	`<enable | disable> (Event Log Color Coding)`	Enable or disable event log color coding.
`-lf`	`<tab | csv> (Export Log Format)`	Specify the log export format, tab or CSV.
`-ts`	`<us | metrics> (Temperature Scale)`	Specify the user's temperature scale. This setting is also used by the system when a user preference is not available (for example, email notifications).
`-df`	`<mm/dd/yyyy | dd.mm.yyyy | mmm-dd-yy | dd-mmm-yy | yyyy-mm-dd> (Date Format)`	Specify the user's preferred date format.
`-lg`	`<language code (enUs, etc)>`	User language
`-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 interface 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 NetBotz 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 NetBotz Rack Monitor 250 (443 by default). The other available range is 5000–32768.

Example 1:

To prevent all access to the web interface, 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 command line interface through a serial connection. After the upload completes:

- If there are any system or network changes, the command line interface restarts and you must log on again.
- If you selected a baud rate for the file transfer that is not the same as the default baud rate for the NetBotz Rack Monitor 250, you must reset the baud rate to the default to reestablish communication with the NetBotz 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 “Verifying Upgrades” on page 111 for descriptions of the transfer result codes.

Parameters: None

Example:

```
apc>xferStatus

E000: Success

Result of last file transfer: Failure unknown
```

Error Message: `E000`

NetBotz Rack Monitor 250 Device Command Descriptions

The following NetBotz Rack Monitor 250 application CLI commands are available in this release:

modbus

Access: Super User, Administrator

Description:

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 hexidecimal.
-rDef		Restore default settings.
-tE	enable | disable	Enable or disable Modbus TCP.
-tP	<1 - 65535>	Specify 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`

Web Access

The web user interface provides options to view the status and manage the NetBotz Rack Monitor 250.

Supported Web Browsers

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

Getting Started

To access the NetBotz Rack Monitor 250 in a web browser, you must disable any *proxy server* services. Access to the NetBotz 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 NetBotz Rack Monitor 250 is not proxied.

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

- For an IP address of 139.225.6.133, when the NetBotz 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 NetBotz 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 NetBotz Rack Monitor 250 (Web1 in this example), enter:

  `http://Web1` if HTTP is your access mode.

  `https://Web1` if HTTPS is your access mode.

The Web Interface

When you log on to the NetBotz Rack Monitor 250 web interface, 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.

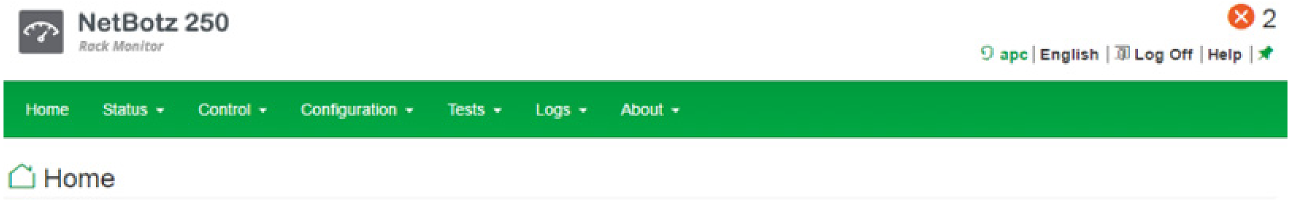
Limited Status Access

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.

Home

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.



The **Home** page 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.

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.

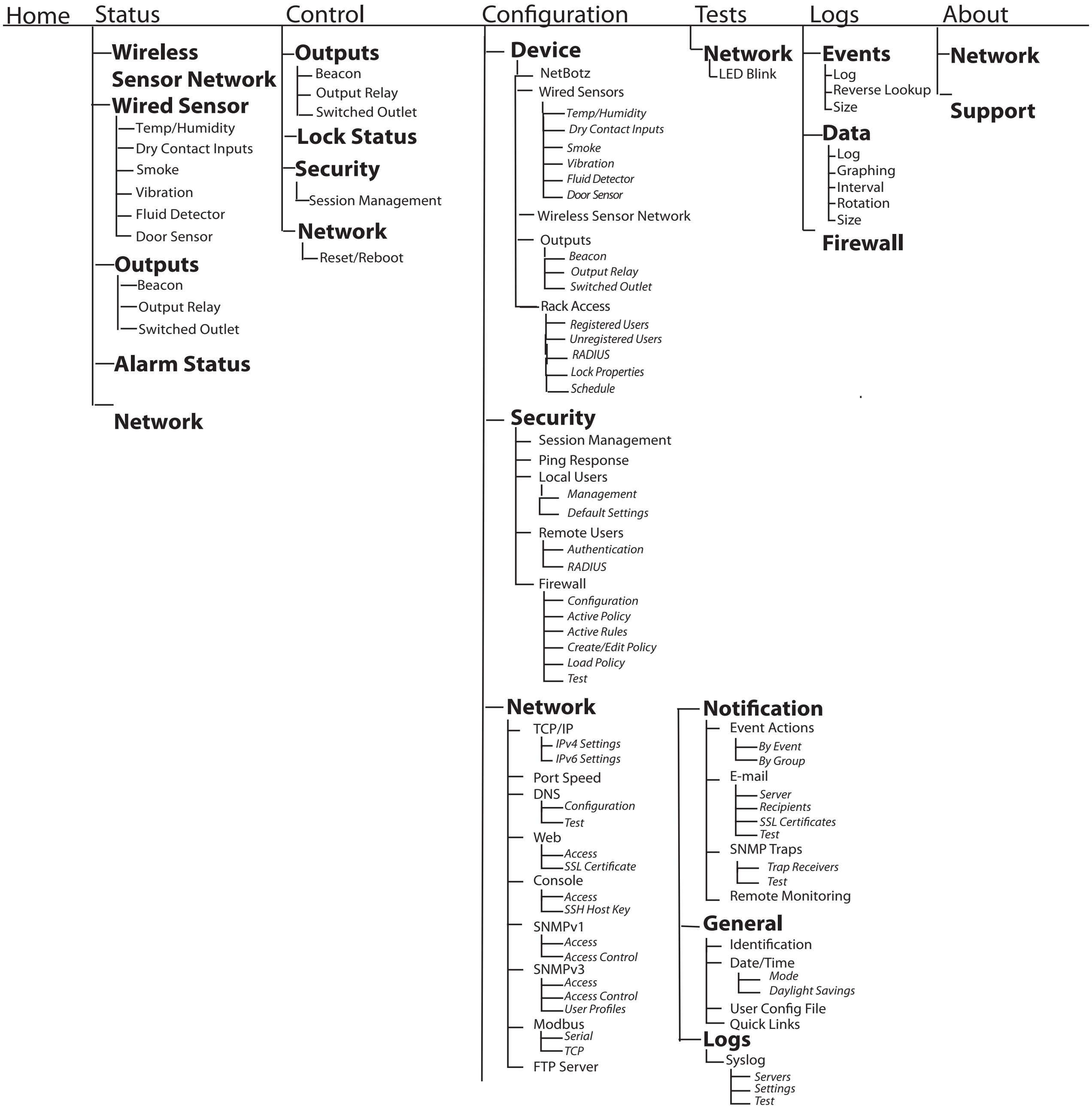
Quick Links

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 APC web-enabled products
- **Link 3:** Information on Schneider Electric Monitoring Services

Display Menu Tree

Edit the image below with application-specific and application-optional details.



Status

Wireless Sensor Network

Status > Wireless Sensor Network

View all connected wireless temperature and temperature/humidity sensors.

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 on 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.

Wired Sensors

Status > Wired Sensors

All wired sensors display the following status:

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 device name to configure the device.

Location

Location of the monitored device (up to 20 characters).

Module Name

Name of the module to which the sensor is connected, the NetBotz 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. Click the sensor name to configure its settings.

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 Temperature Scale.

Humidity

Relative humidity of the air surrounding the temperature/humidity 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

Outputs

Status > Outputs

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

All outputs display the following information:

Module Name

Name of Module to which the output is connected. Click to view all devices connected to the module.

Module Location

Location of Module to which the output is connected, the NetBotz 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.

Each output type displays additional status information:

Beacon

State

On (monitored device is in alarm state) or Off (no alarms).

Relay Output

State

Open or Closed

Switched Outlet

State

On or Off

Alarm Status

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).

Module Alarms

View alarms for modules. (This area appears only if a NetBotz Rack 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:

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.

Network

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.

Control

Session Management

Control > Security > Session Management

Lists all of the currently logged in users, the interface from which they are logged in, their IP address, 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.**

Network Reset/Reboot

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	• 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	Select one or more of the following options: **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 NetBotz Rack Monitor 250 to its default configuration. **User Configurations**: Resets all users to their default configuration.

Outputs

Control > Outputs

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

All outputs display the following information:

Module Name

Name of Module to which the output is connected. Click to view all devices connected to the module.

Module Location

Location of Module to which the output is connected, the NetBotz 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.

Each output type displays additional control information:

Beacon: Turn the beacon on and off.

Output Relay: Open and close the relay.

Switched Outlet: Turn the outlet on and off.

Lock Control

Control > Lock Control

Lock and unlock the rack access handle connected to the Door Handle 1 and Door Handle 2 ports.

Configuration

NetBotz

Configuration > Device > NetBotz

Click the module name, NetBotz or NBPod150, to configure its settings, and view and configure settings for its connected sensors.

NetBotz: Name and Location

NBPod 150: Name, Location, and Blink Identifier LED on the selected Sensor Pod 150 module for the number of minutes you specify.

View the module factory information, including the model number, serial number, hardware revision, and software revision.

Wired Sensor

Configuration > Device > Wired Sensor

Click the sensor name to configure its settings.

Temperature and Humidity

Name: Enter a name (up to 20 characters).

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.

Threshold Settings: Click to enter the minimum, low, high, maximum, and hysteresis values for temperature and humidity.

Temperature above any of these thresholds causes an alarm:

Maximum: Must be greater than High Temperature Threshold.

High: Must be greater than the sum of Low Temperature Threshold and Temperature Threshold Hysteresis.

Temperature below any of these thresholds causes an alarm:

Low: Must be greater than Minimum Temperature Threshold.

Minimum: The lowest temperature threshold.

Humidity above any of these thresholds causes an alarm:

Maximum: Must be greater than High Humidity Threshold.

High: Must be greater than the sum of Low Humidity Threshold and Humidity Threshold Hysteresis.

Humidity below any of these thresholds causes an alarm:

Low: Must be greater than Minimum Humidity Threshold.

Minimum: The lowest humidity threshold.

Hysteresis: The difference between the threshold violation and the clearing point.

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 Change Settings: Click to configure the acceptable short-term and long-term rate of change (increase and decrease in the time you specify). When the rate of change is exceeded, an alarm occurs. Once an increase or decrease no longer exceeds the limits you specify, the rate of change alarm clears.

Wireless Sensor Network

Configuration > Device > Wireless Sensor Network

Modify the settings for each wireless sensor, including name, extended address, location, alarm generation, and temperature, humidity, battery, and signal thresholds.

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 Thresholds: Set the thresholds for the temperature:

> **Maximum**: If the threshold for the maximum temperature for the sensor is exceeded, an alarm occurs.
>
> **High**: If the threshold for the high temperature for the sensor is exceeded, an alarm occurs.
>
> **Low**: If the temperature drops below its low threshold for the sensor, an alarm occurs.
>
> **Minimum**: If the temperature drops below its minimum threshold for the sensor, an alarm occurs.

Humidity Thresholds: Set the thresholds for the humidity:

> **Maximum**: If the threshold for the maximum humidity for the sensor is exceeded, an alarm occurs.
>
> **High**: If the threshold for the high humidity for the sensor is exceeded, an alarm occurs.
>
> **Low**: If the humidity drops below its low threshold for the sensor, an alarm occurs.
>
> **Minimum**: If the humidity drops below its minimum threshold for the sensor, an alarm occurs.

Battery Thresholds: Set the thresholds for the battery voltage:

> **Low**: If the battery voltage drops below its low threshold for the sensor, an alarm occurs.
>
> **Minimum**: If the battery voltage drops below its minimum threshold for the sensor, an alarm occurs.

Signal Thresholds: Set the thresholds for the signal strength:

> **Low**: If the signal strength drops below its low threshold for the sensor, an alarm occurs.
>
> **Minimum**: If the signal strength drops below its minimum threshold for the sensor, an alarm occurs.

Outputs

Configuration > Device > Outputs (Beacon, Output Relay, and Switched Outlet)

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

All outputs display the following information:

Module Name

Name of Module to which the output is connected. Click to view all devices connected to the module.

Module Location

Location of Module to which the output is connected, the NetBotz 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.

Each output type displays additional configuration information:

Name: Enter a name (up to 20 characters).

Location: Enter the location of the sensor (up to 20 characters).

Normal State: On/Off or Open/Closed (excluding the beacon)

Control: Turn On/Off or Open/Close

Alarm Mapping: The beacon, output relay and switched outlet can be activated by alarm states of sensors on the NetBotz module only.

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.

User Access

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.

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.

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:

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 exit without saving.

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.

Configuration > Device > Rack Access > RADIUS

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

Lock user authentication

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.

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

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.

Lock Properties

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.

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: Rack access supports eight access card formats. Choose the format of the card you are configuring:

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.

MIFAREC4: Mifare Classic 4 byte card.

MIFAREC7: Mifare Classic 7 byte.

MIFAREDF: Mifare DESfire.

MIFAREPL: Mifare Plus.

To register a new proximity card:

1. Check the box to enable the card reader. Specify the card type for the installed handle(s), the auto-relock time (10 - 60 seconds), and the time to wait before the door open alarm is activated for Door 1, Door 2, or both (1 - 120 minutes). Click Apply.
2. Hold the card in front of the proximity reader on the handle until you hear a beep.
3. Go to Configuration > Device > User Access > Unregistered Users.
4. Click the card ID number to specify the user name, door access (Door 1, Door 2, or both), the access schedule (24 x 7 by default), and enable account access.
5. Click Apply.

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

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

Configuration > Device > Rack Access > Schedule

Schedule a date and time to automatically unlock the enclosure doors.

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.

Security

Session Management

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 “Session Management” on page 53 for more information.

Ping Response

Configuration > Security > Ping Response

Control whether or not the NetBotz Rack Monitor 250 responds to a network ping. If enabled, and the NetBotz Rack Monitor 250 does not respond to an IPv4 ping, see “Unable to ping the NetBotz Rack Monitor 250” on page 112.

Local Users

Configuration > Security > Local Users > Management

Create and manage *Super User* and *General User* profiles on the NetBotz Rack Monitor 250. The initial view is a list of the current user profiles, separated by type. Click any *User Name or Add User* to navigate to the *User Configuration* page.

Your changes will take effect after you log off. For more information about *User Account types*, see “User Account Overview” on page 3“.

Access: Check the box to enable access to log into the NetBotz Rack Monitor 250. Uncheck 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: 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:

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 interface 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.

Default Settings

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.

Bad Login Attempts: Number of incorrect login attempts before the system disables the 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.

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: Configure whether new passwords created for user accounts require additional rules, such as at least one lowercase character, one uppercase character, one number, and one symbol.

Password Policy: Select the duration (in days) after which the user will be required to change their password. A value of 0 days disables this feature (by default).

Remote Users

Authentication

Configuration > Security > Remote Users > Authentication

Select how to administer remote access to the NetBotz 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**.

Schneider Electric supports the authentication and authorization functions of RADIUS (Remote Access Dial-In User Service).

- When a user accesses a NetBotz 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 NetBotz 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:

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 command line interface, 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 command line interface when RADIUS only is selected.

Configure the RADIUS Server

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.

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.

Configuration Procedure

You must configure your RADIUS server to work with the NetBotz 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 NetBotz 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

Configuration > Security > Firewall

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

Configuration: Enable or disable the overall firewall functionality

Active Policy: Select an active policy from the available firewall policies.

Active Rules: Lists the individual rules that are being enforced based on the current active policy.

Create/Edit Policy: Create a new policy or edit an existing one.

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

Test Policy: Temporarily enforce the rules of a chosen policy.

NOTE: The firewall is disabled by default.

Though the NetBotz 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 betested before it is applied to a production environment.

Network

TCP/IP

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 NetBotz 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.

BOOTP, DHCP

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 NetBotz Rack Monitor 250 requests a network assignment from any BOOTP server: • 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 NetBotz 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: • 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. **Vendor Cookie** Check to require vendor specific cookie to accept DHCP address (disabled by default). **NOTE:** The default values for these three settings generally do not need to be changed: • **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.

DHCP Configuration Advanced

You can use a RFC2131/RFC2132-compliant DHCP server to configure the TCP/IP settings for the NetBotz 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 APC Knowledge Base article ID **FA156110** at **www.apc.com/support**.

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

IPv6 Settings

Current IPv6 Settings

Type: Indicates the IP address is assigned Manually or Automatically.

IP Address: The IPv6 address of the device.

Prefix Length: Indicates thee number of bits used to identify the network.

IPv6 Configuration

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 NetBotz 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:

- **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 be used for any configuration settings.

Port Speed

Configuration > Network > Port Speed

The Port Speed setting defines the communication speed of the TCP/IP port. For Auto-negotiation (the default), Ethernet devices negotiate to transmit at the highest possible speed. If the supported speeds of two devices do not match, the slower speed is used.

You can also select 10 Mbps or 100 Mbps half-duplex (communication in only one direction at a time) or full-duplex (communication in both directions on the same channel simultaneously).

DNS

Configuration

Configuration > Network > DNS > Configuration

The NetBotz 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.

DNS Status

Active Primary DNS Server

Active Secondary DNS Server

Active Host Name

Active Domain Name (IPv4/IPv6)

Active Domain Name (IPv6)

Manual Domain Name System Settings

Override Manual DNS Settings: 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: 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) and **Domain Name (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).

DNS Network Test

Configuration > Network > DNS > Test

Test the DNS settings you specified.

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:

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

Configuration > Network > Web > Access

Option	Description
Access	Enable/disable access to the web interface. You must log out of the NetBotz Rack Monitor 250 web interface to activate your changes. You must use a computer with telnet access to re-enable web access. • **Enable HTTP:** Sets Hypertext Transfer Protocol (HTTP) as the means of access to the web interface. 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 interface. 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 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.

	NOTE: 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

Configuration > Network > Web > SSL Certificate

Option	Description
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. **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 NetBotz Rack Monitor 250. • **Valid certificate**: A valid certificate was installed or was generated by the NetBotz Rack Monitor 250. Click the link to view the certificate’s contents. • **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

Configuration > Network > Console

Option	Description
Access	Configure access to the *Command Console*. • **Disable:** Disables access to the Command Console. • **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 command line interface. For **SSH**, see your *SSH* client documentation to specify a non-default port in the command line that starts *SSH*.	
SSH Host Key	View the status of an installed *SSH* Host Key, and add, replace, or remove a Host Key. • **Status**: Indicates whether the current *SSH* Host Key is valid. • **Add or Replace Host Key**: 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. 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. **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.

Network Configuration SNMP

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 NetBotz Rack Monitor 250 on the public network of a StruxureWare system, you must have SNMP enabled in the NetBotz Rack Monitor 250 interface. Read access will allow StruxureWare to receive traps from a NetBotz Rack Monitor 250. Write access is required while you use the interface of the NetBotz Rack Monitor 250 to set StruxureWare as a trap receiver.

Configuration > Network > SNMPv1 > Access

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**

Configuration > Network > SNMPv1 > Access Control

Option	Description
Access Control	You can configure up to four access control entries to specify which NMS can have access to the NetBotz 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. **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: • 149.225.12.**255**: Access only by an NMS on the 149.225.12 segment. • 149.225.**255.255**: Access only by an NMS on the 149.225 segment. • 149.**255.255.255**: Access only by an NMS on the 149 segment. • 0.0.0.0 (the default setting) which can also be expressed as 255.255.255.255: Access by any NMS on any segment. **Access Type:** The actions an NMS can perform through the community. • Read: GETS only, at any time. • Write: GETs 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. • Disable: No GETS or SETS at any time.

SNMPv3 Configuration

Configuration > Network > SNMPv3

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

Access	SNMPv3 Access: Enables SNMPv3 as a method of communication with this device.
User Profiles	By default, lists the settings of four user profiles, configured with the user names “apc snmp profile1” through “apc snmp profile 4,” and no authentication and no privacy (no encryption of data). To edit the following settings for a user profile, click a user name in the list. **User Name:** The identifier of the user profile. SNMP version 3 maps GETs, SETs, and traps to a user profile by matching the user name of the profile to the user name in the data packet being transmitted. A user name can have up to 32 ASCII characters. **Authentication Passphrase:** A phrase up to 32 bytes, ASCII English 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 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	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. **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. • 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: • 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.

Enabling Modbus

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

Modbus - Serial (RTU) Access

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.

Modbus - TCP Access

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

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 NetBotz 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

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” on page 93.
  - Queries (SNMP GETs)
  - For more information, see “Network Configuration SNMP” on page 76. 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

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 or System Events categories. Or you can 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 92
- “E-mail Recipients” on page 87
- “SNMP Trap Receivers” on page 88

Configure 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 therecipients 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 84 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, 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

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

Configuration > Notification > E-mail > Server

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

- **Outgoing Mail Configuration**
  - **From Address:**
    - 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: If your mail server requires authentication, enter your user name and password here.

- **Advanced**
  – Use SSL/TLS: Select when encryption is used.
    - **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

Configuration > Notification > E-mail > Recipients

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

E-mail Recipient

- **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**
  - **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.
  - **Recipient:** This is the SMTP server of the recipient. The NetBotz 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.
  - **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.

Custom E-mail Server Settings

- See "Outgoing Mail Configuration" on page 85.

E-mail SSL Certificates

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

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 Traps Notifications

Configuration > Notification > SNMP Traps

SNMP Trap Receivers

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 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

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

Configuration > General > Identification

Define the values for:

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 the Remote Monitoring Service, 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 the Remote Monitoring Service, 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.

Services Used By	**Name**	**Contact**	**Physical Location**
sysName OID in the SNMP agent	●	●	●
Remote Monitoring Service	●		●
StruxureWare Data Center Expert	●	●	●

Set the Date and Time

Configuration > General > Date/Time > Mode

Set the time and date used by the NetBotz 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 NetBotz 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 NetBotz Rack Monitor 250.

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.
Time Zone	Select a time zone. The number of hours preceding each time zone in the list is the offset from Coordinated Universal Time (UTC), formerly Greenwich Mean Time.
Update Interval	Define how often, in hours, the NetBotz 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

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**.

Using a Configuration File (.ini)

Configuration > General > User Config File

See “Retrieve the .ini File Using the Web Interface” on page 103. for more information.

Configuring Links

Configuration > General > Quick Links

Quick Links provide quick access to useful Web sites, 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 interface pages. A **Name** to identify the link is required (up to 40 characters) 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

Configuration > Logs > Syslog

Servers

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 NetBotz 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. The NetBotz Rack Monitor 250 uses the default port 514 to send Syslog messages.

NOTE: To disable Syslog messages, See “Configure Event Actions” on page 83. In addition, Syslog messages can be disabled if the "Message Generation" option is not selected in *Syslog Settings*.

Language: Choose a language for any Syslog messages.

Protocol: Choose between UDP and TCP.

Settings

Configuration > Logs > Syslog > Settings

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.

These messages can be categorized in the drop-down list by an available Syslog priority. The local severity options are Critical, Warning, and Informational. In addition, Syslog supports Severity Mapping. Various system events can be prioritized and highlighted through the generation of a severity map.

Test

Configuration > Logs > Syslog > Test

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

LED Blink

Tests > Network > LED Blink

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

Logs

Creating a log is resource intensive. Depending on your device’s configuration, generating and downloading a log may require several minutes to complete. 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 the *Launch Log in New Window* button. The log entries can always be cleared, by clicking **Clear Log**.

NOTE: JavaScript must be enabled in your browser.

Event Log

Logs > Events > Log

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.

Event Log Color Coding

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**.

Event Log Filtering

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 box, 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

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

Logs > Events > Size

Specify the size of the event log by number of events. The minimum number of events is 25; 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

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.

Retrieve Data Log File Using Web Interface

Logs > Data > Log

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: See “Log Retrieval - General” on page 79.

Retrieve Data Log Files using FTP or SCP

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 interface. You can use SCP to retrieve the log file using encryption-based security protocols; retrieval by FTP is unencrypted. See “Log Retrieval - General” on page 79.

FTP Retrieval of 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 NetBotz 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 81 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
```

Retrieval of event.txt or data.txt by SCP

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
```

Graph the Data Log

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.

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 “Log Retrieval” in the Data: Log section for further FTP and SCP instructions.

Parameter	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 menu, 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.

Click *Apply* to view the graph, or click *Cancel* to discard the changes. Click *Launch Graph* in New Window to display the graph in a new browser window that provides a full-screen view.

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

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.

Configuring Data Log Rotation

Logs > Data > Rotation

There is a limited amount of solid state storage in the NetBotz 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.

Parameter	Description
Last Upload Result	Indicates whether the last upload of the data file to the FTP server succeeded or failed, or displays “None Available.”
Data Log Rotation	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: • 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

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.

Firewall Log

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 NetBotz Rack Monitor 250 reboots.

About the NetBotz Rack Monitor 250

Network

About > Network

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

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

Support

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 "Retrieving and Exporting the .ini File"), 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

Capabilities, Requirements, and Installation

How to use the Wizard to Configure TCP/IP Settings

The Device IP Configuration Wizard can discover NetBotz 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 NetBotz Rack Monitor 250 that already have a DHCP-assigned IP address.

NOTE: For detailed information on the Utility, see the Knowledge Base on the support page of the www.apc.com website and search for FA156064 (the ID of the relevant article).

NOTE: To use the DHCP Option 12, see Knowledge Base ID FA156110.

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.
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.

Configuration File (.ini) Settings

Retrieving and Exporting the .ini File

Summary of the Procedure

Configuring new devices, whether replacement devices, or when setting up essentially similar systems can be greatly simplified by re-using the configuration settings from an existing device with desired settings. An Administrator can retrieve the .ini file of a NetBotz Rack Monitor 250 and then export it to one or more NetBotz Rack Monitor 250s. Using a .ini file can also be useful for backup purposes, in case of a future device failure. The config.ini file can be retrieved in several ways.

1. Configure a NetBotz Rack Monitor 250 to have the settings you want to export.
2. Retrieve the .ini file from that NetBotz Rack Monitor 250
3. Customize the file to change at least the TCP/IP settings.
   NOTE: Retain the original customized file for future use. Each receiving NetBotz 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 NetBotz Rack Monitor 250 to transfer a copy to one or more other NetBotz Rack Monitor 250s. For a transfer to multiple NetBotz Rack Monitor 250s, use an FTP or SCP script or the .ini file utility.

Note: The .ini file utility is available for download from the APC Knowledge Base at **www.apc.com/support**, article **FA156117**.

Contents of the .ini file

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

Retrieve the .ini File Using the Web Interface

Configuration > General > User Config File

At the User Configuration File page of the web interface, the current config.ini file can be downloaded, or, a new config.ini file can be uploaded.

Retain the original customized file for future use. **The file that you retain is the only record of your comments.** Comments are ignored by the Rack Monitor 250 upon file import.

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 NetBotz Rack Monitor 250 can use it to set its own configuration.
Download	Prompts the user to download the config.ini file.

Retrieval of the .ini File Using FTP

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

1. If possible, use the interface of the NetBotz 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 NetBotz Rack Monitor 250:
   a. Open a connection to the NetBotz 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 NetBotz Rack Monitor 250’s settings:

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

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

Customizing

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.**

Transferring the File to a Single NetBotz Rack Monitor 250

- Select the Configuration tab, General on the top menu bar, and User Config File on the dropdown menu. Enter the full path of the file, or use Browse.
- Use any file transfer protocol supported by NetBotz Rack Monitor 250s, i.e., FTP, FTP Client, SCP, or TFTP. The following example uses FTP:
  - From the folder containing the copy of the customized .ini file, use FTP to log in to the NetBotz Rack Monitor 250 to which you are exporting the .ini file:

```
ftp> open ip_address
```

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

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

Exporting the File to Multiple NetBotz Rack Monitor 250

- You can export the file to multiple devices by using FTP or SCP with a script. The script would incorporate and repeat the steps used in exporting a single Configuration file

The Upload Event and Error Messages

After the NetBotz 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 NetBotz Rack Monitor 250 succeeds, and additional event text states the error.

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

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 102 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 NetBotz 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 NetBotz Rack Monitor 250s and configure other settings through their user interface. See **“Device IP Configuration Wizard” on page 101** 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 NetBotz 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
```

File Transfers

Upgrading Firmware

Keeping firmware versions current and consistent across your network allows for implementation of the latest features, performance improvements, as well as bug fixes. Regular upgrades also ensures that all NetBotz Rack Monitor 250s support the same features, in the same manner. Obtain the free, latest firmware version from **www.apc.com/tools/download**

Firmware consists of:

- Boot Monitor Module *(bootmon)*
- APC Operating System *(AOS)*
- Application Module *(APP Module)*

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.

Firmware Module Files

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

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

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

NOTE: When you transfer individual firmware modules, *Bootmon* must precede AOS, if *bootmon* update is required. The *AOS* module must be transferred to the NetBotz 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 NetBotz 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 NetBotz Rack Monitor 250s and export them to other NetBotz 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 NetBotz Rack Monitor 250. This method is also one which works with a NetBotz Rack Monitor 250 NOT on your network.

Using 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 NetBotz 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. See also “Using the Firmware Upgrade Utility for Multiple Upgrades on Windows” .

Using 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 NetBotz 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.

FTP to Upgrade NetBotz Rack Monitor 250

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

- The NetBotz 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 NetBotz Rack Monitor 250 see “FTP Server” .

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

1. The firmware module files must be extracted, see “To extract the firmware files:”
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 107.
3. Open an FTP client session:

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

4. Type `open` with the **IP address** of the NetBotz 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.

SCP to Upgrade NetBotz Rack Monitor 250

To use Secure CoPy (SCP) to upgrade firmware for the NetBotz 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 107..
2. Use an SCP command line to transfer the AOS firmware module to the NetBotz 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 NetBotz Rack Monitor 250. (Always upgrade the *AOS* before the *App Module*).

XMODEM to Upgrade NetBotz Rack Monitor 250

To use XMODEM to upgrade one NetBotz Rack Monitor 250 that is not on the network, you must extract the firmware files with the Firmware Upgrade Utility (see “To extract the firmware files:”).

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 NetBotz 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 NetBotz 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 NetBotz Rack Monitor 250’s network interface.

Using 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 NetBotz 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 UPS 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.

Verifying Upgrades

Verify the Success of the Transfer

To verify whether a firmware upgrade succeeded, you can use the `xferStatus` command in the command line interface 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.

Verify the Version Numbers of Installed Firmware

About > Network

Use the web user interface to verify the versions of the upgraded firmware modules. You could also use an SNMP GET to the MIB-2 *sysDescr* OID. In the command line interface, use the `about` command.

Troubleshooting

NetBotz 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 NetBotz Rack Monitor 250	The NetBotz Rack Monitor 250 supports the ability to disable IPv4 Ping Response for security reasons. This setting is located in the web UI under **Configuration > Security > Ping Response** or can be located in config.ini. Check this setting or verify other access methods such as HTTPS, FTP, Telnet, or SSH. If the NetBotz Rack Monitor 250's Status LED is green, try to ping another node on the same network segment as the NetBotz Rack Monitor 250. If that fails, it is not a problem with the NetBotz Rack Monitor 250. If the Status LED is not green, or if the ping test succeeds, perform the following checks: Verify all network connections. Verify the IP addresses of the NetBotz Rack Monitor 250 and the NMS. If the NMS is on a different physical network (or subnetwork) from the NetBotz Rack Monitor 250, verify the IP address of the default gateway (or router). Verify the number of subnet bits for the NetBotz Rack Monitor 250's subnet mask.
Cannot allocate the communications port through a terminal program	Before you can use a terminal program to configure the NetBotz Rack Monitor 250, you must shut down any application, service, or program using the communications port.
Cannot access the command console through a USB serial connection	Make sure a USB A-USB mini B cable is connected to the correct USB port. Make sure that the baud rate is configured correctly: 9600, 81N.
Cannot access the command console remotely	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. For *SSH*, the NetBotz Rack Monitor 250 may be creating a host key. The NetBotz Rack Monitor 250 takes several minutes to create the host key, and *SSH* is inaccessible during that time.

Problem	Solution
Cannot access the web interface	Verify that HTTP or HTTPS access is enabled. Check your browser’s proxy settings. Make sure the URL is consistent with the security system used by the NetBotz Rack Monitor 250. SSL requires https, not http, at the beginning of the URL. Verify that you can ping the NetBotz Rack Monitor 250. Verify that you are using a supported Web browser. If available, try a different web browser. See “Supported Web Browsers” on page 44. If the NetBotz Rack Monitor 250 has just restarted and SSL security is being set up, the NetBotz Rack Monitor 250 may be generating a server certificate. The NetBotz Rack Monitor 250 may take up to several minutes to create this certificate, and the SSL server is not available during that time.

SNMP Issues

Problem	Solution
Unable to perform a GET	Verify the read (GET) community name (SNMPv1) or the user profile configuration (SNMPv3). Use the Command Console or web interface to ensure that the NMS has access. See “Network Configuration SNMP” on page 76.
Unable to perform a SET	Verify the read/write (SET) community name(SNMPv1) or the user profile configuration (SNMPv3). Use the Command Console or the web interface 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 “Network Configuration SNMP” on page 76.
Unable to receive traps at the NMS	Make sure the trap type (SNMPv1 or SNMPv3) is correctly configured for the designated NMS as a trap receiver. 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. If either is not correct, use SETs to the mconfigTrapReceiverTable OIDs, or use the Command Console or web interface to correct the trap receiver definition. For SNMPv3, check the user profile configuration for the NMS, and run a trap test. See “Network Configuration SNMP” on page 76, “SNMP Trap Receivers” on page 88,“ and “Event Actions” on page 83.
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.

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:

   This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Worldwide Customer Support

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

- Visit the APC web site to access documents in the APC Knowledge Base and to submit customer support requests.
  - **www.apc.com**
    Connect to localized APC web sites for specific countries, each of which provides customer support information.
  - **www.apc.com/support/**
    Global support searching APC Knowledge Base and using e-support.
- Contact the Customer Care Center by telephone or e-mail.
  - Local, country-specific centers: go to **www.apc.com/support/contact** for contact information.

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