USER'S GUIDE

NetBotz Rack Access PX

Contents

Introduction

Product Description

Features of the NetBotz Rack Access PX

The American Power Conversion (APC®) NetBotz® Rack Access PX provides electronic monitoring and access control of your enclosure. It uses a Network Management Card, which provides full management capabilities over a network using Telnet, HTTP, HTTPS, Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure CoPy (SCP), and SNMP. The Rack Access PX provides the following features:

- Electronic monitoring of the users who access the enclosure
- Customizable access schedules for each user
- Remote locking or unlocking of the enclosure doors
- Door-open alarms
- Scheduled unlocking events
- Beacon mapping
- Event log accessible by Telnet, FTP, SSH (Secure SHell), SCP, serial connection, or a Web browser
- SNMP traps and e-mail notifications sent based on the severity level of the events
- Syslog events sent to configured Syslog servers
- Security protocols for authentication and encryption

Initial setup

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

- IP address of the management card
- Subnet mask
- IP address of the default gateway

Never use the loopback address (127.0.0.1) as the default gateway address for the Rack Access PX. Doing so will disable the card and will require you to reset TCP/IP settings to their defaults using a local serial login.

To configure the TCP/IP settings, see the Rack Access PX *Installation* manual, provided in printed form, and in PDF on either the APC NetBotz Rack Access PX *Utility* CD or on the APC Web site, **www.apc.com**.

To use a DHCP server to configure the TCP/IP settings at a Rack Access PX, see TCP/IP settings (Administration>Network>TCP/IP).

Internal Management Features

Overview

The Rack Access PX has two user interfaces (control console and Web interface) which allow you to manage the Rack Access PX, depending on your preferences. You can also manage the Rack Access PX through the SNMP interface by using a SNMP browser with the PowerNet® MIB.

For more information about the Rack Access PX's user interfaces, see Control Console and Web Interface.

To use the PowerNet MIB with an SNMP browser, see the *PowerNet SNMP Management Information Base (MIB) Reference Guide*, which is provided on the APC NetBotz Rack Access PX *Utility* CD.

Login control

Only one user at a time can log on to the Rack Access PX to use its internal user interface features. The priority for access is as follows:

- Local access to the control console from a computer with a direct serial connection to the Rack Access PX always has the highest priority.
- Telnet or Secure SHell (SSH) access to the control console from a remote computer has the next highest priority.
- Web access, either directly or through the InfraStruXure Manager, has the lowest priority.

For information on how SNMP access to the Rack Access PX is controlled, see SNMP (Administration>Network>SNMP>options).

Types of user accounts

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

- An Administrator can use all of the management menus available in the control console and the Web interface. The Administrator's default user name and password are both **apc**.
- A Device-Only User can access the **Log** tab and use the **Rack Access** tab. The Device-Only User's default user name is **device**, and the default password is **apc**.
- A Read-Only User has the following restricted access:
  - Access through the Web interface only.
  - Access to the same menus as a Device-Only User, but without the capability to change configurations, control devices, or delete data. Links to configuration options may be visible but are disabled, and the event log displays no **Clear Log** button.

  The Read-Only User's default user name is **readonly**, and the default password is **apc**.

To set **User Name** and **Password** values for the Administrator, Device-Only User, and Read-Only accounts, see Setting user access (Administration>Security>Local Users>options). You must use the Web interface to configure values for the Read-Only User.

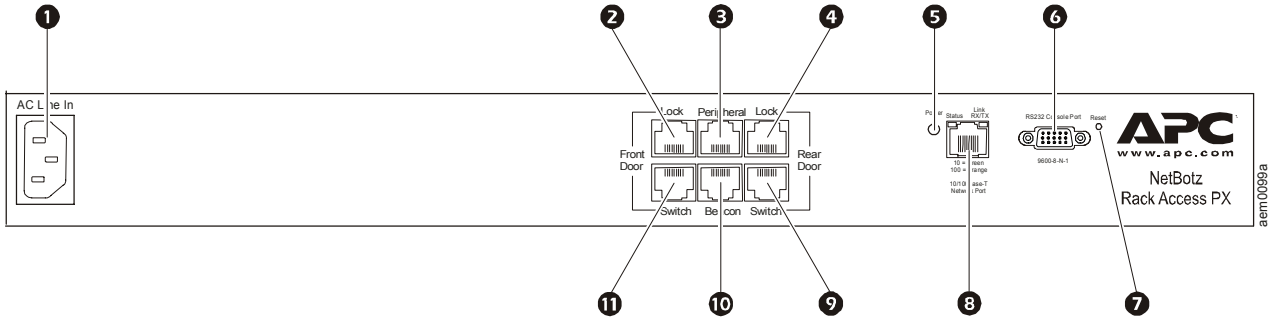
How to Recover from a Lost Password

Use a local computer, a computer that connects to the Rack Access PX or another device through the serial port, to access the control console.

1. Select a serial port at the local computer, and disable any service that uses that port.
2. Connect the APC null modem cable (APC part number 940-0103) to the selected port on the computer and to the serial port at the Rack Access PX.
3. Run a terminal program (such as HyperTerminal®) and configure the selected port as follows:
   - 9600 bps
   - 8 data bits
   - no parity
   - 1 stop bit
   - no flow control
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt. If you are unable to display the **User Name** prompt, verify the following:
   - The serial port is not in use by another application.
   - The terminal settings are correct as specified in step 3.
   - The correct cable is being used as specified in step 2.
5. Press the **Reset** button on the Rack Access PX. The Status LED will flash between orange and green. Immediately press the **Reset** button on the Rack Access PX a second time while the LED is flashing to reset the user name and password to their defaults temporarily.

6. Press ENTER as many times as necessary to redisplay the **User Name** prompt, then use the default, **apc,** for the user name and password. (If you take longer than 30 seconds to log on after the **User Name** prompt is redisplayed, you must repeat step 5 and log on again.)
7. From the **Control Console** menu, select **System**, then **User Manager**.
8. Select **Administrator**, and change the **User Name** and **Password** settings, both of which are now defined as **apc**. Select **Accept Changes** to store the new user name and password values.
9. Press CTRL-C, log off, reconnect any serial cable you disconnected, and restart any service you disabled.

Rear Panel



	Item	Description
❶	AC Line Inlet	Provides power to the Rack Access PX; see the APC NetBotz Rack Access PX *Installation* manual for voltage information.
❷	Front Door Lock port	Port used for communication with the front lock.
❸	Peripheral port	Reserved for future use.
❹	Rear Door Lock port	Port used for communication with the rear lock.
❺	Power LED	Indicates whether the unit is receiving power (green–receiving power; dark–not receiving power).
❻	RS-232 Console Port	Serial port used to configure initial network settings using the included configuration cable (APC part number 940-0103).
❼	Reset switch	Reset the Rack Access PX; this switch does not change configuration data.
❽	10/100 Base-T Network Port	Connect the Rack Access PX to the network. The Status and Link LEDs indicate network traffic. • Status LED: Blinks orange and green at startup; indicates the status of the network connection (solid green–IP address established; blinking green–attempting to obtain an IP address). • Link LED: Blinks to indicate network traffic (green–operating at 10 mbps; orange–operating at 100 mbps).
❾	Rear Door Switch port	Port used for communication with the rear door switch.
❿	Alarm beacon port	Connect an optional alarm beacon (AP9324).
⓫	Front Door Switch port	Port used for communication with the front door switch.

Link-RX/TX (10/100) LED

The Link-RX/TX LED on the front of the Rack Access PX indicates the network connection status of the card.

Condition	Description
Off	One of the following situations exist: • The Rack Access PX is not receiving input power. • The Rack Access PX is starting up. • The Rack Access PX is not operating properly. It may need to be repaired or replaced. Contact APC Worldwide Customer Support.
Solid Green	The device is connected to a network operating at 10 Megabits per second (Mbps).
Solid Orange	The device is connected to a network operating at 100 Megabits per second (Mbps).
Flashing Green	The device is receiving or transmitting data packets at 10 Megabits per second (Mbps).
Flashing Orange	The device is receiving or transmitting data packets at 100 Megabits per second (Mbps).

Status LED

This LED indicates the network status of the Rack Access PX.

Condition	Description
Off	The Rack Access PX has no power.
Solid Green	The Rack Access PX has valid TCP/IP settings.
Flashing Green	The Rack Access PX does not have valid TCP/IP settings.[1]
Solid Orange	A hardware failure has been detected in the Rack Access PX. Contact APC Worldwide Customer Support.
Flashing Orange	The Rack Access PX is making BOOTP[2] requests.
Alternately Flashing Green and Orange	The Rack Access PX is making DHCP[2] requests.

1 If you do not use a BOOTP server, see the Rack Access PX *Installation* manual provided in printed format and in PDF on the APC NetBotz Rack Access PX *Utility* CD to configure the TCP/IP settings.
2 To use a BOOTP or DHCP server, see TCP/IP settings (Administration>Network>TCP/IP).

Watchdog Features

Overview

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

Network interface watchdog mechanism

The Rack Access PX implements internal watchdog mechanisms to protect itself from becoming inaccessible over the network. For example, if the Rack Access PX does not receive any network traffic for 9.5 minutes (either direct traffic, such as SNMP, or broadcast traffic, such as an Address Resolution Protocol [ARP] request), it assumes that there is a problem with its network interface and restarts.

Resetting the network timer

To ensure that the Rack Access PX does not restart if the network is quiet for 9.5 minutes, the Rack Access PX attempts to contact the Default Gateway every 4.5 minutes. If the gateway is present, it responds to the Rack Access PX, and that response restarts the 9.5-minute timer. If your application does not require or have a gateway, specify the IP address of a computer that is running on the network most of the time and is on the same subnet. The network traffic of that computer will reset the 9.5-minute timer frequently enough to prevent the Rack Access PX from restarting.

Control Console

How to Log On

Overview

You can use either a local (serial) connection, or a remote (Telnet or SSH) connection, to access the control console.

Use case-sensitive user name and password entries to log on (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device-Only User). A Read-Only User cannot access the control console.

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

Remote access to the control console

You can access the control console through Telnet or Secure SHell (SSH), depending on which is enabled. (An Administrator can enable these access methods through the **Telnet/SSH** option of the **Network** menu.) By default, Telnet is enabled. Enabling SSH automatically disables Telnet.

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

1. At a command prompt, type **`telnet`** and the System IP address for the Rack Access PX (when the Rack Access PX uses the default Telnet port of 23), and press ENTER. For example:

   ```
   telnet 139.225.6.133
   ```

   If the Rack Access PX uses a non-default port number (between 5000 and 32768), you need to include a colon or a space (depending on your Telnet client) between the IP address and the port number.

2. Enter the user name and password (by default, **apc** and **apc** for an Administrator, or **device** and **apc** for a Device-Only User).

SSH for high-security access. If you use the high security of SSL for the Web interface, use Secure SHell (SSH) for access to the control console. SSH encrypts user names, passwords, and transmitted data.

The interface, user accounts, and user access rights are the same whether you access the control console through SSH or Telnet, but to use SSH, you must first configure SSH and have an SSH client program installed on your computer.

Local access to the control console

You can use a local computer that connects to the Rack Access PX through the serial port of the unit.

1. Select a serial port at the local computer, and disable any service which uses that port.
2. Use the supplied null modem cable (APC part number 940-0103) to connect the selected port to the serial port on the Rack Access PX.
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. Save the changes.
4. Press ENTER, repeatedly if necessary, to display the **User Name** prompt.
5. Enter the user name and password for the access desired (**Administrator** or **Device-Only User**).

Main Screen

Example main screen

The following is an example of the screen that appears when you log on to the control console at a Rack Access PX.

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


American Power Conversion               Network Management Card AOS vx.x.x
(c) Copyright 2005 All Rights Reserved  NetBotz Rack Access PX APP  vx.x.x
-------------------------------------------------------------------------------
Name      : Rack Access PX                            Date : 01/29/2006
Contact   : Bill Cooper                               Time : 10:16:58
Location  : Testing Lab                               User : Administrator
Up Time   : 0 Days 0 Hours 43 Minutes                 Stat : P+ N+ A+

NetBotz Rack Access PX Overview: No alarms present

Front Door Status: Locked, Handle Closed, Door Closed
Rear Door Status : Locked, Handle Closed, Door Closed
Beacon           : Normal

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

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

Information and status fields

Main screen information fields.

- Two fields identify the APC operating system (AOS) and application (APP) firmware versions. The application firmware name identifies the type of device that connects to the network. On the example main screen, the application firmware for the Rack Access PX is displayed.

```
Network Management Card AOS          vx.x.x
NetBotz Rack Access PX APP           vx.x.x
```

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

```
Name      : Rack Access PX
Contact   : Bill Cooper
Location  : Testing Lab
```

To set the **Name**, **Contact**, and **Location** values, see Information you configure (Administration>General>Identification).

- An **Up Time** field reports how long the Rack Access PX has been running since it was last reset or since power was applied.

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

- Two fields identify the date and time the last time the screen refreshed.

```
Date : 01/29/2006
Time : 10:16:58
```

- A **User** field identifies whether you logged on as Administrator or Device Manager (equivalent to Device-Only User in the Web interface).

```
User : Administrator
```

Main screen status fields.

- A **Stat** field reports the Rack Access PX status.

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

P+	The APC operating system (AOS) is functioning properly.
N+	The network is functioning properly.
N?	A BOOTP request cycle is in progress.
N–	The Rack Access PX failed to connect to the network.
N!	Another device is using the IP address of the Rack Access PX.
A+	The application is functioning properly.
A–	The application has a bad checksum.
A?	The application is initializing.
A!	The application is not compatible with the AOS.

If the AOS status is not P+, contact APC Worldwide Customer Support, even if you can still access the Rack Access PX.

Rack Access PX status field.

The **Status** field displays the status of the devices connected to the Rack Access PX. Under normal operation this field will read **No alarms present**.

```
NetBotz Rack Access PX Overview: No alarms present


Front Door Status: Locked, Handle Closed, Door Closed
Rear Door Status : Locked, Handle Closed, Door Closed
Beacon           : Normal
```

Control Console Menus

Menu structure

The menus in the control console list options by number and name. To use an option, type the option's number and press ENTER, then follow any on-screen instructions.

For menus that allow you to change a setting you must use the **Accept Changes** option to save the changes you made. Some changes may only take effect after you log off.

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

- Type **?** and press ENTER to access brief menu option descriptions (if the menu has help available).
- Press ENTER to refresh the menu.
- Press ESC to return to the menu from which you accessed the current menu.
- Press CTRL-C to return to the main (control console) menu.
- Press CTRL-L to access the event log.

For information about the event log, see Event log (Logs>Events>options).

Main menu

The main control console menu has options that provide access to the management features of the control console.

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

Device Manager option

This option accesses the **Device Manager** menu. Select the components you want to manage. For example:

```
1- User Access
2- Door Properties
3- Lock Control
4- Schedule
5- Beacon
```

Network option

Use this option to perform any of the following tasks:

- Configure the Rack Access PX's TCP/IP settings.
- Configure the settings for the type of server (DHCP or BOOTP) used to provide the TCP/IP settings to the Rack Access PX.
- Use the Ping utility.
- Define settings that affect the FTP, Telnet/SSH, Web/SSL/TLS, SNMP, E-mail, Syslog, and DNS features of the Rack Access PX.

System option

Use this option to perform any of the following tasks:

- Control **Administrator** and **Device Manager** access.
- Define the System **Name**, **Contact**, and **Location** values.
- Set the date and time used by the Rack Access PX.
- Restart the Rack Access PX interface.
- Reset control console settings to their default values.
- Access System information about the Rack Access PX.
- Define RADIUS access and set primary and secondary servers.

Web Interface

How to Log On

Overview

You can use a Rack Access PX's DNS name or System IP address for the URL address of the Web interface. Use your case-sensitive **User Name** and **Password** settings to log on. The default user name differs by account type:

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

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

If you are using HTTPS (SSL/TLS) as your access protocol, your login credentials are compared with information in a server certificate. If the certificate was created with the APC Security Wizard, and an IP address was specified as the common name in the certificate, you must use an IP address to log on to the Rack Access PX. If a DNS name was specified as the common name on the certificate, you must use a DNS name to log on.

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

Supported Web browsers

You can use Microsoft® Internet Explorer (IE) 5.5 and higher (on Windows operating systems only), Firefox, version1.*x*, by Mozilla Corporation (on all operating systems), or Netscape® 7.*x* and higher (on all operating systems) to access the Rack Access PX through its Web interface. Other commonly available browsers also may work but have not been fully tested by APC.

To use the Web interface, it is not required that you enable JavaScript® for your Web browser. It is recommended, however, for optimal functioning of the interface.

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

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

URL address formats

Type the DNS name or IP address of the Rack Access PX in the Web browser's URL address field and press ENTER. Except when you specify a non-default Web server port in Internet Explorer, **`http://`** or **`https://`** is automatically added by the browser.

If the notice "Someone is currently logged into the APC Management Web Server. Please try again later" occurs (Internet Explorer only), another user is logged on to the Web interface or control console. If the error "No Response" (Netscape) or "This page cannot be displayed" (Internet Explorer) occurs, Web access may be disabled, or the card may use a non-default Web-server port that you did not specify correctly in the address.

- For a DNS name of Web1, the entry would be one of the following:
  - **`http://Web1`** if HTTP is your access mode
  - **`https://Web1`** if HTTPS (SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133, when the Rack Access PX uses the default port (80) at the Web server, the entry would be one of the following:
  - **`http://139.225.6.133`** if HTTP is your access mode
  - **`https//139.225.6.133`** if HTTPS (SSL/TLS) is your access mode
- For a System IP address of 139.225.6.133, when the Rack Access PX uses a non-default port (5000, in this example) at the Web server, the entry would be one of the following:
  - **`http://139.225.6.133:5000`** if HTTP is your access mode
  - **`https://139.225.6.133:5000`** if HTTPS (SSL/TLS) is your access mode

Summary Page

When you log on to the Web interface at the Rack Access PX, navigation tabs are displayed at the top of the screen. Below the navigation tabs, a top menu bar lists options related to the selected tab. The status field displays information about the selected tab or top menu bar option.

Navigation tabs

Four tabs are displayed at the top of the screen:

- **Home**—view any active alarm or warning conditions and clear active alarms; this tab is displayed at login.
- **Rack Access**—view and configure users, remotely lock or unlock the enclosure, configure the beacon, and create scheduled unlock events.
- **Logs—**view and configure the event log.
- **Administration—**configure security, network connection, notification, and device settings.

The quick status tab is displayed in the upper right of every screen in the Web interface. The tab displays a warning of any alarms.

	Click the green “device operating normally” icon to return to the status screen where the status for attached devices is displayed.
	Click the “attention required” icon to return to the status screen where active warnings and alarms are displayed.
	Click the “alarm detected” icon to return to the status screen where active alarms are displayed.

Status

The status field displays one of three states (No alarms present, Warning, or Critical) for the front door, rear door, and beacon. The Recent Device Events table displays the five most recent device events, and the dates and times they took place. Click **More Events** at the bottom of the **Recent Device Events** table to see previous events

Help

Click **Help**, located in the upper right hand corner of the Web interface, to view context-sensitive information.

Select a tab to perform a task

To do the following, see Rack Access PX Operation:

- View and configure user access permissions.
- Delete user permissions.
- Enable or disable the access card reader.
- Configure door-open alarms.
- Remotely lock or unlock enclosure doors.
- View the status of the beacon.
- Configure an automatic unlock event.

To do the following, see Administration: Notification and Logging:

- Access the event log.
- Configure the actions to be taken based on an event's severity level.
- Configure SNMP Trap Receiver settings for sending event-based traps.
- Define who will receive e-mail notifications of events.
- Test e-mail settings.

To do the following, see Administration: Network Features:

- Configure new TCP/IP settings for the Rack Access PX.
- Identify the Domain Name System (DNS) Server and test the network connection to that server.
- Define settings for the FTP server, Telnet/SSH, SNMP, e-mail, Syslog, and Web/SSL.

To do the following, see Administration: General Options:

- Control **Administrator**, **Device-Only User**, and **Read-Only** user access.
- Configure RADIUS access, servers, and server secret.
- Define the System **Name**, **Contact**, and **Location** values.
- Set the date and time used by the Rack Access PX.
- Restart the user interface of the Rack Access PX.
- Reset network interface settings to their default settings.
- Remove all registered and unregistered users.
- Reset lost communication alarms.
- Upload a user configuration file.
- Define the URL addresses of the user links and APC logo links in the Web interface.

Rack Access PX Operation

User Access

The left navigation menu option **User Access**, selected by default when you choose **Rack Access** on the top menu bar, displays information about registered and unregistered users.

View registered and unregistered users

Registered Users. View the configured settings of each registered user, including the user's name and contact information, the doors the user can open, and the status of the user's time schedule (granted or not configured). Click the user's name to edit name, contact information, and access permissions.

Unregistered Users. View the card identification number and the most recent access attempt of each unregistered user.

Register a user

To add a card ID number to the list of **Unregistered Users**, close and lock the enclosure doors, then hold the card in front of the Rack Access PX lock until the Rack Access PX beeps once.

Unregistered cards cause the Rack Access PX to beep once for approximately three seconds. Registered cards cause it to beep twice.

To register a user, click the card ID number in the **Unregistered Users** list, and configure the following settings. (The card ID itself is not configurable.)

- **Name**: Enter a name (up to 20 characters) for this user.
- **Contact**: Enter the contact information (up to 20 characters) for this user.
- **Account Access**: Mark this checkbox to activate the card. To temporarily disable this registered user's access permissions, unmark this checkbox.
- **Door Access**: Assign the doors the configured access card will open: **Front**, **Back**, or **Both**.
- **Granted Access Schedule**: Enable the card user's access for specific days of the week and for a period of time on each of those days. Until the access schedule is configured, this user cannot unlock enclosure doors.
  - To enable access on a day, mark the checkbox next to the day.
  - To specify the time period during which the card can unlock the rack on a selected day, enter the time in hours and minutes. Valid times are 00:00 to 23:59.

Click **Register User** to save your changes, or **Cancel** to exit without saving.

Delete access card settings

To remove an access card from the list of registered users, click the user name from the **Registered Users** list. The user access configuration page appears; click **Delete User**.

If you hold an access card in front of the lock after its settings are deleted, its card ID number appears in the list of unregistered users.

Door Properties

Select the **Rack Access** tab, then select the left navigation menu option **Door Properties** to configure the door lock properties.

Enable or disable the access card reader

By default, the access card reader is disabled. To enable the card reader, mark the **Card Reader** checkbox. When this setting is disabled, you must use a key or the Web interface to access the enclosure.

Configure auto-relock settings

Configure the door to lock if it is not opened within the period of time you specify in the **Auto-Relock** field. Valid values are 10–60 seconds.

Configure door open alarms

If a door is open for a period of time that is greater than the amount of time specified in its enabled **Door Open Alarm** field, an alarm is generated. To enable the alarm, mark the checkbox next to the door, and specify the time limit, in minutes. Valid values are 10–120 minutes.

Click **Apply** to save your changes, or **Cancel** to exit without saving.

Lock Control

Select the **Rack Access** tab, then select the left navigation menu option **Lock Control** to use the interface to lock or unlock the doors remotely. Mark the checkbox of the door to lock or unlock, then select **Next>>**. Select **Apply** to change the state of the lock, or select **Cancel** to leave the lock in its current state.

Beacon

Select the **Rack Access** tab, then select the left navigation menu option **Beacon** to view the current state of the beacon and configure the following settings:

- **Name**: Enter a name (up to 20 characters) for the beacon.
- **Location**: Enter the location (up to 20 characters) of the beacon.
- **Alarm Status**: View the current status of the beacon, **Normal** or **Abnormal State**.
- **State**: View the current state of the beacon, **On** or **Off**.
- **Control**: Mark this checkbox to change the state of the beacon manually.
- **Mapping**: Choose the alarms that will change the state of the beacon:
  - **Door Open Alarm**: The door has been open for a greater amount of time than the configured **Door Open Alarm** limit in the **Door Properties** menu.
  - **Key Override**: The door was opened with a key.
  - **Forced Entry**: The door was opened in an unauthorized manner, without a key, access card, scheduled unlock, or command from a user interface.
  - **Hardware Error**: A hardware error has been detected. Contact APC Worldwide Customer Support.

Click **Apply** to save your changes, or **Cancel** to exit without saving.

Schedule

Select the **Rack Access** tab, then select the left navigation menu option **Schedule** to schedule a date and time to unlock one or both enclosure doors automatically. Configure the following settings:

- **One-time Schedule**: Mark the checkbox to enable the scheduled unlock.
- **Date**: Designate the date the doors will unlock.
- **Time**: Enter the time, in hours and minutes, when the doors will unlock. Valid values are 00:00 to 23:59.
- **Unlock Doors**: Specify which doors to unlock—the front door, back door, or both doors.
- **Remain Unlock for**: 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 duration**: Mark the checkbox to prevent the door from locking if it is closed during the scheduled unlock.

Click **Apply** to save your changes, or **Cancel** to exit without saving.

Administration: Security

Local Users

Permission levels

Before you configure user access, be sure you understand the capabilities of each account type (Administrator, Device-Only User, and Read-Only User) to use menus, view information, and change settings.

For information on user permission levels for each account type (Administrator, Device-Only User, and Read-Only User), see Types of user accounts.

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

You set the user name and password for each of the account types in the same manner.

User name. The case-sensitive user name (maximum of 10 characters) is used by Administrator and Device-Only Users to log on at the control console or Web interface and by the Read-Only User to log on at the Web interface. Default values are **apc** for Administrator, **device** for Device-Only Users, and **readonly** for the Read-Only User.

Password. The case-sensitive password (maximum of 10 characters) is used to log on to the Web interface or (except for the Read-Only User) the control console. The default setting for **Password** is **apc** for Administrators, Device-Only Users, and Read-Only Users.

Remote Users

Authentication (Administration>Security>Remote Users>Authentication)

Use this option to select how to administer remote access to the Rack Access PX:

For information about local authentication (authentication that can be administered without the centralized authentication provided by a RADIUS server), see the *Security Handbook* provided on the *Utility* CD and available on the APC Web site at **www.apc.com**.

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

- When a user accesses the Rack Access PX or other network-enabled device that has RADIUS enabled, an authentication request is sent to the RADIUS server to determine the user's permission level.
- RADIUS user names used with the Rack Access PX are limited to 32 characters.

Select one of the following:

- **Local Device Only**: RADIUS is disabled. Local authentication is enabled.
- **RADIUS, then Local Device**: RADIUS is enabled, and local authentication is enabled. Authentication is requested from the RADIUS server first; local authentication is used only if RADIUS authentication fails.
- **RADIUS Only**: RADIUS is enabled. Local authentication is disabled.

If **RADIUS Only** is selected, the only way to recover if the RADIUS server is unavailable, improperly identified, or improperly configured is to use a serial connection to the control console and change the **Access** setting to **Local Device Only** or **RADIUS, then Local Device**.

RADIUS (Administration>Security>Remote Users>RADIUS)

Use this option to do the following:

- Display a list of RADIUS servers identified as being available to the Rack Access PX and the time-out period for each server (the number of seconds the Rack Access PX will wait for a reply from the server before the request fails).
- Add a server to the list of identified RADIUS servers. Click **Add Server**, and configure the following parameters for authentication by the new server:

RADIUS Setting	Definition
RADIUS Server	The server name or IP address of the RADIUS server. **NOTE:** RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.
Secret	The shared secret between the RADIUS server and the Rack Access PX.
Timeout	The time in seconds that the Rack Access PX waits for a response from the RADIUS server.
Test Settings	Enter the Administrator user name and password to test the RADIUS server path that you have configured.
Skip Test and Apply	Do not test the RADIUS server path.

Configuring the RADIUS Server

You must configure your RADIUS server to work with the Rack Access PX. The following procedure summarizes the steps to perform.

For examples of the file entries needed to configure a RADIUS server for use with a Rack Access PX, see the *Security Handbook*, available on the *Utility* CD or from the APC Web site, **www.apc.com**.

Summary of the configuration procedure

1. Add the IP address of the Rack Access PX to the RADIUS server client list (file).

   RADIUS servers use port 1812 by default to authenticate users. To use a different port, add a colon followed by the new port number to the end of the RADIUS server name or IP address.

2. The users must be configured with Service-Type attributes unless Vendor Specific Attributes (VSAs) are defined instead. If no Service-Type attribute is configured, the user will have read-only access (on the Web interface only).

   See your RADIUS server documentation for information about the RADIUS users file, and see the APC *Security Handbook* for an example.

3. Vendor Specific Attributes (VSA) can be used instead of the Service-Type attributes provided by your RADIUS server. This method requires a dictionary entry and a RADIUS users file. In the dictionary file, you can define the names for the ATTRIBUTE and VALUE keywords, but not the numeric values. If you change the numeric values, RADIUS authentication and authorization will not work correctly. VSAs take precedence over standard RADIUS attributes.

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

Configuring a RADIUS server on UNIX®, with shadow passwords

If UNIX shadow password files are used (/etc/passwd) in conjunction 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-Only Users, change the APC-Service-Type to **`Device`**.

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

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

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

Supported RADIUS servers

APC supports FreeRADIUS, Microsoft Windows 2000 Server, and Microsoft Windows 2000 RADIUS Server. Other commonly available RADIUS applications may work but have not been fully tested by APC.

Inactivity Timeout (Administration>Security>Auto Log Off)

Use this option to configure the time (3 minutes by default) that the system waits before logging off an inactive user.

Administration: Network Features

TCP/IP and communication settings

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

The **TCP/IP** option on the left navigation menu, selected by default when you choose **Network** on the top menu bar, displays the current TCP/IP settings of the Rack Access PX (its IP address, subnet mask, default gateway, and MAC address).

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

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

Setting	Description
Manual	The IP address, subnet mask, and default gateway must be configured manually. (The MAC address is not configurable.) Click **Next>>**, and enter the new values.
BOOTP	A BOOTP server provides the TCP/IP settings. At 32-second intervals, the Rack Access PX requests network assignment from any BOOTP server: • If it receives a valid response, it starts the network services. • If it finds a BOOTP server, but the request to that server fails or times out, the Rack Access PX stops requesting network settings until it is restarted. • By default, if previously configured network settings exist, and it receives no valid response to five requests (the original and four retries), it uses the previously configured settings so that it remains accessible if a BOOTP server is no longer available. Click **Next>>** to access the BOOTP Configuration page to change the number of retries or the action to take if all retries fail to find a BOOTP server [1]: • **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries. • **If retries fail**: Select either **Use prior settings** (the default) or **Stop BOOTP request**.

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

Setting	Description
DHCP	At 32-second intervals, the Rack Access PX requests network assignment from any DHCP server. By default, the number of retries is unlimited. • If it receives a valid response, by default it requires the APC cookie from the DHCP server in order to accept the lease and start the network services. • If it finds a DHCP server, but the request to that server fails or times out, it stops requesting network settings until it is restarted. • If a DHCP server responds with an invalid offer (for example, the offer does not contain the APC Cookie), the Rack Access PX accepts the lease from that server on the last request of the sequence and then immediately releases that lease. This prevents the DHCP server from reserving the IP Address associated with its invalid offer.  For more information on what a valid response requires, see DHCP response options To specify values other than the defaults, click **Next>>** to access the **DHCP Configuration** page[1]: • **Require vendor specific cookie to accept DHCP Address**: To disable the requirement that the DHCP server provide the APC cookie, unmark this check-box. • **Maximum retries**: Enter the number of retries that will occur when no valid response is received, or zero (0) for an unlimited number of retries.

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

Setting	Description
DHCP & BOOTP	The default setting. The Rack Access PX tries to obtain its TCP/IP settings from a BOOTP server first, and then, if it cannot discover a BOOTP server, from a DHCP server. If it obtains its TCP/IP settings from either server, it switches this setting from the default to **BOOTP** or **DHCP**, depending on the type of server that supplied the TCP/IP settings to the Rack Access PX. Click **Next>>** to access and configure the same settings that are available on the **BOOTP Configuration** and **DHCP Configuration** pages[1] and to specify that the **DHCP and BOOTP** setting be retained after either type of server provides the TCP/IP values.

1 The default values for these three settings on the configuration pages generally do not need to be changed:

- **Vendor Class**: APC
- **Client ID**: The MAC address of the Rack Access PX, which uniquely identifies it on the local area network (LAN)
- **User Class**: The name of the application firmware module

DHCP response options

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

Vendor Specific Information (option 43). The Rack Access PX uses this option in a DHCP response to determine whether the DHCP response is valid. This option contains up to two APC-specific options in a TAG/LEN/DATA format: the APC Cookie and the Boot Mode Transition.

- **APC Cookie. Tag 1, Len 4, Data "1APC"**
  Option 43 communicates to the Rack Access PX that a DHCP server is configured to service APC devices. By default, this DHCP response option must contain the APC Cookie for the Rack Access PX to accept the lease.

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

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

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

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

Access PX accepts the DHCP response. Whenever the Rack Access PX reboots, it will request its network assignment from a DHCP server only.

Following, in hexadecimal format, is an example of a Vendor Specific Information option that contains the APC cookie and the disable Boot Mode Transition setting:

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

TCP/IP options. The Rack Access PX uses the following options within a valid DHCP response to define its TCP/IP settings. All of these options except the first are described in **RFC2132**.

- **IP Address** (from the **yiaddr** field of the DHCP response, described in **RFC2131)**: The IP address that the DHCP server is leasing to the Rack Access PX.
- **Subnet Mask** (option 1): The Subnet Mask value that the Rack Access PX needs to operate on the network.
- **Router,** i.e., Default Gateway (option 3): The default gateway address that the Rack Access PX needs to operate on the network.
- **IP Address Lease Time** (option 51): The time duration for the lease of the IP Address to the Rack Access PX.
- **Renewal Time, T1** (option 58): The time that the Rack Access PX must wait after an IP address lease is assigned before it can request a renewal of that lease.
- **Rebinding Time, T2** (option 59): The time that the Rack Access PX must wait after an IP address lease is assigned before it can seek to rebind that lease.

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

- **Network Time Protocol Servers** (option 42): Up to two NTP servers (primary and secondary) that the Rack Access PX can use.
- **Time Offset** (option 2): The offset of the Rack Access PX's subnet, in seconds, from Coordinated Universal Time (UTC).
- **Domain Name Server** (option 6): Up to two Domain Name System (DNS) servers (primary and secondary) that the Rack Access PX can use.
- **Host Name** (option 12): The host name that the Rack Access PX will use (32-character maximum length).
- **Domain Name** (option 15): The domain name that the Rack Access PX will use (64-character maximum length).
- **Boot File Name** (from the **file** field of the DHCP response, described in **RFC2131**): The fully qualified directory-path to an APC user configuration file (.ini file) to download. The **siaddr** field of the DHCP response specifies the IP address of the server from which the Rack Access PX will download the .ini file. After the download, the Rack Access PX uses the .ini file as a boot file to reconfigure its settings.

Port Speed (Administration>Network>Port Speed)

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

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

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

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

- Select **servers** to specify the IP addresses of the primary and optional secondary Domain Name System server. The Rack Access PX cannot send any e-mail messages unless at least the IP address of the primary DNS server is defined.
  - The Rack Access PX waits a maximum of 15 seconds for a response from the primary DNS server or the secondary DNS server (if a secondary DNS server is specified). If the Rack Access PX does not receive a response within that time, e-mail cannot be sent. Therefore, use DNS servers on the same segment as the Rack Access PX or on a nearby segment (but not across a wide-area network [WAN]).
  - After you define the IP addresses of the DNS servers, verify that DNS is working correctly by entering the DNS name of a computer on your network to look up the IP address for that computer.
- Select **naming** to define the host name and domain name of the Rack Access PX:
  - **Host Name**: When an Administrator configures a host name here and a domain name in the **Domain Name** field, users can then enter a host name in any field in the Rack Access PX interface (except e-mail addresses) that accepts a domain name as input.
  - **Domain Name**: An Administrator must configure the domain name here only. In all other fields in the Rack Access PX interface (except e-mail addresses) that accept domain names, the Rack Access PX adds this domain name when only a host name is entered.

- To override all instances of the expansion of a specified host name by the addition of the domain name, set the domain name field to its default, `example.com`, or to `0.0.0.0`.
- To override the expansion of a specific host name entry — for example when defining a trap receiver — include a trailing period. The Rack Access PX recognizes a host name with a trailing period (such as *`mySnmpServer.`*) as if it were a fully qualified domain name and does not append the domain name.

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

– As **Query Type**, select the method to use for the DNS query:

- **by Host**: the URL name of the server
- **by FQDN**: the fully qualified domain name
- **by IP**: the IP address of the server
- **by MX**: the Mail Exchange used by the server

– In the **Query Question** field, identify the value to be used for the selected query type:

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

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

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

Use the options under **Web** on the left navigation menu to configure the following:

Option	Description

access	To activate changes to any of the following access selections, log off from and back on to the Rack Access PX:
	• **Disable**: Disables all access to the Web interface. (You must use the control console to re-enable access to the Web interface. Select **Network** and **Web/SSL/TLS**. Then for HTTP access, select **Access** and **Enabled**, and for HTTPS access, also select **Web/SSL** and **Enabled**.)
	• **Enable HTTP** (the default): Enables Hypertext Transfer Protocol (HTTP), which provides Web access by user name and password, but does not encrypt user names, passwords, and data during transmission.
	• **Enable HTTPS**: Enables Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) to provide Web access. Secure Sockets Layer (SSL) encrypts user names, passwords, and data during transmission, and provides authentication of the Rack Access PX by digital certificate.
	 
	See also
	See "Creating and Installing Digital Certificates" in the *Security Handbook* on the APC NetBotz Rack Access PX *Utility* CD to choose among the several methods for using digital certificates.
	When HTTPS is enabled, your browser displays a lock icon, usually at the bottom of the screen: 
	HTTP Port: Identifies the TCP/IP port used for communication by HTTP with the Rack Access PX. The default is 80.
	HTTPS Port: Identifies the TCP/IP port used for communications by HTTPS with the Rack Access PX. The default is 443.
	You can change either port setting to the number of any unused port from 5000 to 32768 to enhance the protection provided by User Name and Password settings. You must then use a colon (:) in the address field of the browser to specify the non-default port number. For example, for port 5000 and the Rack Access PX IP address of 152.214.12.114, you would use one of these Web addresses:
	`http://152.214.12.114:5000`
	`https://152.214.12.114:5000`

Option	Description
ssl cipher suites	Enable or disable any of the SSL encryption ciphers and hash algorithms: • **DES**: A block cipher that provides authentication by Secure Hash Algorithm. • **RC4_MD5** (enabled by default): A stream cipher, providing authentication by MD5 hash algorithm. • **RC4_SHA** (enabled by default): a stream cipher that provides authentication by Secure Hash Algorithm. • **3DES**: A block cipher that provides authentication by Secure Hash Algorithm.
ssl certificate	Add, replace, or remove a security certificate. **Status**: • **Not installed**: A certificate is not installed, or a certificate was installed by FTP or SCP to an incorrect location. Using **Add or Replace Certificate File** installs the certificate to the correct location, **/sec** on the Rack Access PX. • **Generating**: The Rack Access PX is generating a certificate because no valid certificate was found. • **Loading**: A certificate is being activated on the Rack Access PX. • **Valid certificate**: A valid certificate was installed or was generated by the Rack Access PX. Click on this link to view the certificate's contents. **If you install an invalid certificate, or if no certificate is loaded when you enable SSL, the Rack Access PX generates a default certificate, a process which delays access to the interface for up to five minutes.** You can use the default certificate for basic encryption-based security, but a security alert message displays whenever you log on. **Add or Replace Certificate File**: Enter or browse to the certificate file created with the Security Wizard.  See also See "Creating and Installing Digital Certificates" in the *Security Handbook* on the APC NetBotz Rack Access PX *Utility* CD to choose a method for using digital certificates, including certificates created by the Security Wizard or generated by the Rack Access PX. **Remove**: Delete the current certificate.

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

Use the options under **Console** on the left navigation menu to configure the following:

Option	Description

access	Choose one of the following:
	• **Disable**: Disables all access to the control console.
	• **Enable Telnet** (the default setting): Telnet transmits user names, passwords, and data without encryption.
	• **Enable SSH v1/v2**: Do not enable both versions 1 and 2 of Secure SHell (SSH) unless you require that both be activated at the same time. (Security protocols use extensive processing power.)
	• **Enable SSH v1 only**: Secure SHell (SSH) version 1 transmits user names, passwords, and data in encrypted form. There is little or no delay as you log on.
	• **Enable SSH v2 only**: Secure SHell (SSH) version 2 transmits user names, passwords, and data in encrypted form with somewhat more protection than version 1 from attempts to intercept, forge, or alter data during transmission. There is a noticeable delay as you log on.
	
	Identify the TCP/IP port used for communications with the Rack Access PX by Telnet and Secure SHell (SSH)
	• **Telnet Port**: The default is 23.
	• **SSH Port**: The default is 22.
	
	You can change the Port setting to the number of any unused port from 5000 to 32768 to enhance the protection provided by User Name and Password settings.
	• For Telnet, you must use either a colon (:) or a space in the command line, according to the requirements of your Telnet client program, to specify the non-default port number. For example, for a port number of 5000 and the Rack Access PX IP address of 152.214.12.114, your Telnet client requires one of the following commands:
	`telnet 152.214.12.114:5000`
	`telnet 152.214.12.114 5000`
	• For SSH, see the documentation for your SSH client for the command line format required to specify a non-default port when starting SSH.

Option	Description
ssh encryption	Enable or disable encryption algorithms (block ciphers) compatible with SSH version 1 or version 2 clients: SSH v1 algorithms: • **DES** • **Blowfish**: If your SSH client cannot use Blowfish, which is always enabled, you must also enable DES. SSH v2 algorithms: • **3DES**: (enabled by default) • **Blowfish**: (enabled by default) • **AES 128** • **AES 256** Your version 2 SSH client selects the enabled algorithm that provides the highest security. If your SSH client cannot use the default algorithms, you must enable an AES algorithm that it can use.

Option	Description
ssh host key	**Status** indicates the status of the host key (private key): • **SSH Disabled: No host key in use:** SSH is disabled and is not using a host key even if one is loaded. • **Generating**: The Rack Access PX is creating a host key because no valid host key was found. • **Loading**: A host key is being activated on the Rack Access PX. • **Valid**: One of the following valid host keys is in the **/sec** directory (the required location on the Rack Access PX: •A 1024-bit host key created by the APC Security Wizard •A 768-bit RSA host key generated by the Rack Access PX **Add or Replace**: Upload a host key file created by the APC Security Wizard to the **/sec** directory: 1. Click **Browse**. 2. Locate the file. 3. Click **Apply**. If you use FTP or Secure CoPy (SCP) instead to transfer the host key file, you must specify the **/sec** directory as the target location in the command.  See also To use the APC Security Wizard, see the *Security Handbook* on the APC NetBotz Rack Access PX *Utility* CD. **NOTE:** To reduce the time required to enable SSH, create and upload a host key in advance. **If you enable SSH with no host key loaded, the Rack Access PX takes up to 5 minutes to create a host key, and the SSH server is not accessible during that time.** **Remove**: Remove the current host key.


Note

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

SNMP (Administration>Network>SNMP>*options*)

Use the options under **SNMP** on the left navigation menu to configure the following:

Option	Description
access	Enable or disable SNMP. With SNMP enabled (the default), the a**ccess control** option controls how each of the four available SNMP channels is used. To define up to four Network Management Systems (NMSs) as trap receivers, see Trap Receivers (Administration>Notification>SNMP Traps>trap receivers).  To use SNMP to manage the Rack Access PX, see the *PowerNet Management Information Base (MIB) Reference Guide* on the APC NetBotz Rack Access PX *Utility* CD **NOTE:** All user names, passwords, and community names for SNMP are transferred over the network as plain text. If your network requires the higher security of the encryption-based options available, disable SNMP access or set the access type for each channel to Read. (Read access allows you to receive status information and to use SNMP traps.)
access control	**Community Name**: The password (maximum of 15 characters) that an NMS defined by the **NMS IP/Host Name** setting uses to access the channel. **NMS IP/Host Name**: Access is granted only to the Network Management System (NMS) specified by the host name or only to the NMSs specified by one of the IP address formats in the following examples: • 159.215.12.1: Only the NMS at the IP address 159.215.12.1. • 159.215.12.255: Any NMS on the 159.215.12 segment. • 159.215.255.255: Any NMS on the 159.215 segment. • 159.255.255.255: Any NMS on the 159 segment. • 0.0.0.0 or 255.255.255.255: Any NMS. **Access Type**: Define how any NMS specified by **NMS IP/Host Name** and using the correct community name can access the channel. • **Read**: The NMS can use GETs at any time, but it can never use SETs. • **Write**: The NMS can use GETs at any time and can use SETs when no one is logged on to the Rack Access PX. • **Disabled**: The NMS cannot use GETs or SETs. • **Write+**: The NMS can use GETs and SETs at any time, even when someone is logged on to the Rack Access PX.

FTP Server (Administration>Network>FTP Server)

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

You can change the **Port** setting to the number of any unused port from 5001 to 32768 to enhance the protection provided by User Name and Password settings. You must then use a colon (:) in the command line to specify the non-default port number. For example, for a port number of 5001 and the Rack Access PX IP address of 152.214.12.114, you would use this command:

```
ftp 152.214.12.114:5001
```

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

Related topics

See these related topics:

- Console (Administration>Network>Console>options) to configure SSH.
- How to use FTP or SCP to retrieve the event log to obtain a text version of the event log.

Administration: Notification and Logging

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

Types of notification

You can configure event actions to occur in response to an event or a 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

To set up additional methods of active notification that are not included in the **Event Action** options, see Configure door open alarms.

- Indirect notification through the event log. If none of the direct notification methods are configured, users must check the log to determine which events have occurred.

Another method of indirect notification, not included in the **Event Action** options, is the use of informational queries. See access, under SNMP (Administration>Network>SNMP>options), for a description of SNMP access types that enable a Network Management System (NMS) to perform informational queries. Configuring the most restrictive SNMP access type, READ, enables informational queries without the risk of allowing remote configuration changes.

Configuring event actions

You can configure event actions for individual events or for pre-defined groups of events.

Configuring by event. To define event actions for an individual event:

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu.
2. Follow the on-screen instructions to list events by severity, either by main category or sub-category.
3. In the list of events, check the marked columns to see whether the action you want is already configured for the event. (By default, logging is configured for all events.)
4. For details of the current configuration, such as the recipients to be notified by e-mail or the Network Management Systems (NMSs) to be notified by SNMP traps, click on the event name.
5. Add to or change the event configuration.

A Syslog server must be configured before you can display or use the Syslog option, and at least one e-mail recipient or trap receiver must be configured before you can display or use the detailed e-mail and trap notification options.

   – Mark the check-boxes to enable (or unmark them to disable) event logging or Syslog for this event.
   – Click on any e-mail recipient or trap receiver, and specify any value up to three digits to configure the following detailed options.
      • How long, in seconds or minutes, the Rack Access PX waits after the event occurs before sending e-mail to the selected e-mail recipient or a trap to the selected trap receiver. If the event clears during this delay period, no notification is sent. To configure a delay longer than 999 seconds (16 minutes, 39 seconds), use minutes.

- How frequently to send e-mail to the selected e-mail recipient or a trap to the selected trap receiver. E-mail or a trap repeats at the time interval specified here in seconds, minutes, or hours, unless the event has cleared.
- The number of times to send e-mail to the selected e-mail recipient or a trap to the selected trap receiver. Choose to send e-mail or a trap a specified number of times or to repeat the notification an unlimited number of times. In either case, notification stops if the event clears.

When configuring events, you can enable or disable notification to configured e-mail recipients, Syslog message recipients, or trap receivers, but you cannot add or remove any recipients or receivers. To add or remove recipients or receivers, see Identifying Syslog Servers (Logs>Syslog>servers), E-mail recipients (Administration>Notification>E-mail>recipients), and Trap Receivers (Administration>Notification>SNMP Traps>trap receivers).

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

1. Select the **Administration** tab, **Notification** on the top menu bar, and **by group** under **Event Actions** on the left navigation menu.
2. Choose how you want events to be grouped for configuration:
   – If you choose **Grouped by severity**, you can then select all events of one or more severity types.

When configuring events by severity, you must use their existing severity. You cannot change the severity of an event.

   – If you choose **Grouped by category**, you can then select all events in one or more pre-defined categories.
3. Select event actions for all events in the group.

Note

A Syslog server must be configured in order to display or use the Syslog option, and at least one e-mail recipient (for e-mail notification) or at least one trap receiver (for notification by SNMP traps) must be configured in order to display the detailed e-mail and trap receiver notification options.

– Click the **Logging** button to choose logging for all events in the group. Click **Next>>**, and then mark the check-boxes to enable (or unmark them to disable) event logging or Syslog for these events.

– Click the **E-mail Recipients** or **Trap Receivers** button, click **Next>>**, and select an e-mail recipient or trap receiver. Then specify any value up to three digits to configure the following detailed options.

  • How long, in seconds or minutes, the Rack Access PX waits after one of these events occurs before sending e-mail to the selected e-mail recipient or a trap to the selected trap receiver. If the event clears during this delay period, no notification is sent. To configure a delay longer than 999 seconds (16 minutes, 39 seconds), use minutes.

  • How frequently to send e-mail to the selected e-mail recipient or a trap to the selected trap receiver. E-mail or a trap repeats at the time interval specified here in seconds, minutes, or hours, unless the event has cleared.

  • The number of times to send e-mail to the selected e-mail recipient or a trap to the selected trap receiver. Choose to send e-mail or a trap a specified number of times or to repeat the notification an unlimited number of times. In either case, notification stops if the event clears.

To add or remove recipients or receivers, see E-mail recipients (Administration>Notification>E-mail>recipients) or Trap Receivers (Administration>Notification>SNMP Traps>trap receivers).

4. Click **Next>>**, and then click **Apply** to confirm the displayed selections.

Active, Automatic, Direct Notification

E-mail notification

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

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

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

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

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

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

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

  To configure recipients, see E-mail recipients (Administration>Notification>E-mail>recipients).

You can use the **To Address** setting of the **recipients** option to send e-mail to a text-based pager.

SMTP (Administration>Notification>E-mail>server). Use this option to define the following settings:

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

E-mail recipients (Administration>Notification>E-mail>recipients). Use this option to identify up to four e-mail recipients.

Setting	Description
To Address	Defines the user and domain names of the recipient. To use e-mail for paging, use the e-mail address for that recipient's pager gateway account (for example, **myacct100@skytel.com**). The pager gateway will generate the page. You can bypass the DNS lookup of the mail server's IP address by using the IP address in brackets instead of the e-mail domain name. For example, use jsmith@[xxx.xxx.x.xxx] instead of jsmith@company.com. This is useful when DNS lookups are not working correctly. **NOTE:** The recipient's pager must be able to use text-based messaging.

SMTP Server	Selects one of the following methods for routing e-mail:
	• **Local**: Through the Rack Access PX's SMTP server (the recommended setting). This option ensures that the e-mail is sent before the Rack Access PX's 20-second time-out, and, if necessary, is retried several times. Also do one of the following:
	  • Enable forwarding at the Rack Access PX's SMTP server so that it can route e-mail to external SMTP servers. Typically, SMTP servers are not configured to forward e-mail. Always check with the administrator of your SMTP server before changing its configuration to allow forwarding.
	  • Set up a special e-mail account for the Rack Access PX to forward e-mail to an external mail account.
	• **Recipient**: Directly to the recipient's SMTP server. On a busy remote SMTP server, the time-out may prevent some e-mail from being sent because, with this option, the Rack Access PX tries to send the e-mail only once.
	
	When the recipient uses the Rack Access PX's SMTP server, this setting has no effect.

E-mail Generation	Enables (by default) or disables sending e-mail to the recipient.

E-mail test (Administration>Notification>E-mail>test). Use this option to send a test message to a configured recipient.

SNMP Traps

Trap Receivers (Administration>Notification>SNMP Traps>trap receivers). Use this option to define the **Trap Receiver** settings that determine which Network Management Systems (NMSs) receive traps.

Item	Definition
Community Name	The password (maximum of 15 characters) used when traps are sent to the NMS identified by the **NMS IP/Host Name** setting.
NMS IP/Host Name	The IP address or host name of the NMS that will receive traps. **0.0.0.0** (the default value) causes traps not to be sent to any NMS.
Trap Generation	Enables (by default) or disables the sending of any traps to the NMS identified by the **NMS IP/Host Name** setting.
Authentication Traps	Enables or disables the sending of authentication traps to the NMS identified by the **NMS IP/Host Name** setting.

SNMP Trap Test (Administration>Notification>SNMP Traps>test). Use this option to test the sending of a trap to a configured trap receiver.

Syslog (Logs>Syslog>*options*)

By default, the Rack Access PX can send messages to up to four Syslog servers whenever events occur. The Syslog servers, which must be specifically identified by their IP addresses or host names, record the events that occur at network devices in a log that provides a centralized record of events.

This user's guide does not describe Syslog or its configuration values in detail. For more information about Syslog, see RFC3164, at **www.ietf.org/rfc/rfc3164.txt?number=3164**.

Identifying Syslog Servers (Logs>Syslog>servers). Use this option to identify one or more Syslog servers that will receive Syslog messages and to specify a port for each.

Setting	Definition
Syslog Server	Uses specific IP addresses or host names to identify up to four servers that will receive Syslog messages sent by the Rack Access PX. **NOTE:** To use the Syslog feature, at least **Syslog Server** must be defined for at least one server.
Port	Identifies the user datagram protocol (UDP) port that the Rack Access PX will use to send Syslog messages. The default is **514**, the number of the UDP port assigned to Syslog.

Syslog Settings (Logs>Syslog>settings). Leave the Syslog settings, except the **Server IP** settings, set to their defaults unless otherwise specified by the Syslog network or system administrator.

Setting	Definition
Message Generation	Enables (by default) or disables the Syslog feature.
Facility Code	Selects the facility code assigned to the Rack Access PX's Syslog messages (**User**, by default). **NOTE: User** is the selection that best defines the Syslog messages sent by the Rack Access PX. Do not change this selection unless advised to do so by the Syslog network or system administrator.
Severity Mapping	Maps each of the severity levels assigned to Rack Access PX events to the available Syslog priorities. You should not need to change the default mappings. The following definitions are from RFC3164: • **Emergency**: The system is unusable • **Alert**: Action must be taken immediately • **Critical**: Critical conditions • **Error**: Error conditions • **Warning**: Warning conditions • **Notice**: Normal but significant conditions • **Informational**: Informational messages • **Debug**: Debug-level messages Following are the default settings for the four **Local Priority** settings: • **Severe** is mapped to **Critical** • **Warning** is mapped to **Warning** • **Informational** is mapped to **Info** • **None** (for events that have no severity level assigned) is mapped to **Info** **NOTE:** To disable sending Syslog messages for **Severe**, **Warning**, or **Informational** events, see Configuring event actions.

Syslog Test and Format Example (Logs>Syslog>test). Use this option to send a test message to the Syslog servers configured through the **servers** option (**Logs>Syslog>servers**):

1. Select a severity to assign to the test message.
2. Define the test message, using any text that is formatted according to the required message (MSG) fields. The message fields, which you format, are one of the three parts of the Syslog message that will be sent. For example, **`APC: Test Syslog`**, meets the formatting requirements.
   - The priority (PRI) identifies the Syslog priority assigned to the message's event and the facility code assigned to messages sent by the Rack Access PX.
   - The Header includes a time stamp and the IP address of the Rack Access PX.
   - The message (MSG) part has two fields:
     - A TAG field, which is followed by a colon and a space, identifies the event type.
     - A CONTENT field provides the event text, followed (optionally) by a space and the event code.

Indirect Notification through Logs or Queries

Event log (Logs>Events>*options*)

Displaying and using the event log (Logs>Events>log). Use this option to view or delete the contents of the event log. The event log displays all events recorded since the log was last deleted or since the log reached its maximum capacity and the older half was deleted automatically. Events are in reverse chronological order. By default, all events are logged:

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

  Alternatively, you can use FTP or Secure CoPy (SCP) to view the event log. See How to use FTP or SCP to retrieve the event log.

- To delete all events recorded in the log, click **Clear Event Log** on the Web page that displays the log. Deleted events cannot be retrieved.

To disable the logging of events based on their assigned severity level or their event category, configure event actions by group.

See Configuring by group.

To access lists of all configurable events and how they are currently configured, select the **Administration** tab, **Notification** on the top menu bar, and **by event** under **Event Actions** on the left navigation menu, and then click, in turn, on each major category of event

See Configuring by event.

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

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

How to use FTP or SCP to retrieve the event log

If you are an Administrator or Device-Only User, you can use FTP or SCP to retrieve a tab-delineated event log file (*event.txt*) that you can import into a spreadsheet application.

- The file reports all of the events recorded since the log was last deleted.
- The file includes information that the event log does not display.
  - The version of the file format (first field)
  - The date and time the file was retrieved
  - The **Name**, **Contact**, and **Location** values and IP address of the Rack Access PX
  - The unique **Event Code** for each recorded event

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

If you are using the encryption-based security protocols for your system, use Secure CoPy (SCP) to retrieve the log file. (You should have FTP disabled.)

If you are using unencrypted authentication methods for the security of your system, use FTP to retrieve the log file.

See the *Security Handbook*, available on the APC NetBotz Rack Access PX *Utility* CD and on the APC Web site (**www.apc.com**) for information on the available protocols and methods for setting up the type of security appropriate for your needs.

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

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

To use FTP to retrieve the file. To use FTP to retrieve the *event.txt* file:

1. At a command prompt, type **ftp** and the Rack Access PX's IP address, and press ENTER.

   If the **Port** setting for the **FTP Server** option (which you select on the **Network** menu of the **Administration** tab) has been changed from its default value (**21**), you must use the non-default value in the FTP command. For Windows FTP clients, use the following command, including spaces. (For some FTP clients, you must use a colon instead of a space between the IP address and the port number.)

   ```
   ftp>open ip_address port_number
   ```

   To set a non-default port value to enhance security for the FTP Server, see FTP Server (Administration>Network>FTP Server). You can specify any port from 5001 to 32768.

2. Use the case-sensitive **User Name** and **Password** for either an Administrator or a Device-Only User to log on.
   - For Administrator, **apc** is the default for **User Name** and **Password**.
   - For the Device-Only User, **device** is the default for **User Name**, and **apc** is the default for **Password**.

3. Use the **get** command to transmit the text-version of the event log to your local drive.

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

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

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

   – You will not be asked to confirm the deletion.

   – If you clear the event log, a new *event.txt* file is created to record the deleted-log event.

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

Queries (SNMP GETs)

For a description of SNMP access types that enable a Network Management System (NMS) to perform informational queries, see access, under SNMP (Administration>Network>SNMP>options). Configuring the most restrictive SNMP access type, READ, enables informational queries without the risk of allowing remote configuration changes.

Administration: General Options

Information about the Rack Access PX

Information you configure (Administration>General>Identification)

Use this option to define the System **Name**, **Location**, and **Contact** values used by the Rack Access PX's SNMP agent. The option's settings provide the values used for the MIB-II **sysName**, **sysContact**, and **sysLocation** Object Identifications (OIDs).

For example, you might configure **Name** as Test Lab, **Location** as Building 3, and **Contact** (whom to contact about the device) as Donald Adams.

For more information about the MIB-II OIDs, see the *PowerNet*® *SNMP Management Information Base (MIB) Reference Guide* provided on the APC NetBotz Rack Access PX *Utility* CD and on the APC Web site, **www.apc.com**.

Hardware and firmware information (Administration>General>Factory Info)

The hardware information is especially useful to APC Customer Support in helping to troubleshoot problems with your Rack Access PX. The serial number and MAC address accessible through the **Factory Info** menu option are also available on the Rack Access PX itself.

Firmware information, listed under Application Module and APC OS (AOS), indicates the name, firmware version number, and the date and time each firmware module was created. This information may also be useful in troubleshooting and enables you to determine quickly if updated firmware is available to download from the APC Web site.

Date and Time

Date and time (Administration>General>Date & Time>*options*)

How date and time will be set (Administration>General>Date & Time>mode). Use this option to set the time and date used by the Rack Access PX. The option displays the current settings, and allows you to change those settings manually, or through a Network Time Protocol (NTP) Server.

- **Manual**: Use this selection to do one of the following:
  - Enter the date and time for the Rack Access PX.
  - Mark the checkbox **Apply Local Computer Time** to match the date and time settings of the computer you are using, and click **Apply**.
- **Synchronize with NTP Server**: Use this selection to have an NTP Server define the date and time for the Rack Access PX.

Setting	Definition
Primary NTP Server	Enter the IP address or domain name of the primary NTP server.
Secondary NTP Server	Enter the IP address or domain name of the secondary NTP server, when a secondary server is available.
Time Zone	Select a time zone. The number of hours preceding each time zone in the list is the offset from UTC (Coordinated Universal Time, Temps Universel Coordonné, formerly Greenwich Mean Time), the international time standard.
Update Interval	Define how often, in hours, the Rack Access PX accesses the NTP Server for an update. The minimum is 1 hour; the maximum is 8760 hours (1 year).
Update Using NTP Now	Mark this check-box and click **Apply** to Initiate an immediate update of the date and time by the NTP Server.

Enabling and configuring Daylight Saving Time (Administration>General>Date & Time>daylight saving). Use this option to enable either traditional United States Daylight Saving Time (DST) or to enable and configure a customized daylight saving time, with starting and ending dates and time that you specify to match how Daylight Saving Time is implemented in your local area. DST is disabled by default.

When customizing Daylight Saving Time:

- If the local Daylight Saving Time always starts or ends on the 4th occurrence of a specific weekday of a month (for example, the 4th Sunday), choose Fourth/Last. If a 5th Sunday occurs in that month in a subsequent year, the time setting will still change to or from Daylight Saving Time on the 4th Sunday.
- If the local Daylight Saving Time always starts or ends on the last occurrence of a specific weekday of a month, such as the last Sunday of that month, regardless of whether that last Sunday is the 4th or the 5th Sunday, choose Fifth/Last.

Selecting a date format (Administration>General>Date & Time>date format). Select the numerical format in which to display all dates in this User Interface. In the selections, each letter m (for month), d (for day), and y (for year) represents one digit. Single-digit days and months are displayed with a leading zero.

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

Use this option to perform any of the following actions:

Action	Definition
Reboot Management Interface	Restarts the interface of the Rack Access PX.
Reset All	Resets configuration settings as follows: Mark the **Include TCP/IP** checkbox to include the setting that determines how this device must obtain its TCP/IP settings. That setting will be reset to its default, DHCP & BOOTP. **NOTE:** Do not mark the **Include TCP/IP** checkbox to reset all settings except the TCP/IP settings of this device.
Reset Only	You can choose one or more of the following options by marking their check-boxes: **TCP/IP**: Resets only the setting that determines how this device must obtain its TCP/IP settings. That setting will be reset to its default, DHCP & BOOTP. **Event Configuration**: Resets only events to their default configuration. Any configuration changes, by event or by group, will revert to their default settings. **Lost Comm Alarms**: Resets alarms caused when devices are removed from the system. **User Configurations**: Erases all registered and unregistered user information.

Configuring Links (Administration>General>Quick Links)

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

By default, these links access the following Web pages:

- **APC's Web Site**: The APC home page.
- **Testdrive Demo**: A demonstration page where you can use samples of APC Web-enabled products.
- **APC Monitoring**: The home page of the APC Remote Monitoring Service.

To reconfigure a link, click on that link in the **Display** column, and change any of the following:

- **Display**: The short link name displayed on each interface page
- **Name**: A name that fully identifies the target or purpose of the link
- **Address**: Any URL—for example, the URL of another device and server

APC Device IP Configuration Wizard

Purpose and Requirements

Purpose: configure basic TCP/IP settings

You can use the APC Device IP Configuration Wizard to configure the basic TCP/IP settings (IP address, subnet mask, and default gateway) of the following:

- Network Management Cards
- Network-enabled devices (devices that contain embedded Network Management Cards)

Using the Wizard, you can configure the basic TCP/IP settings of installed or embedded Network Management Cards in either of the following ways:

- Automatically discover and configure unconfigured Network Management Cards or network-enabled devices remotely over your TCP/IP network.
- Configure or reconfigure a Network Management Card or network-enabled device through a direct connection from the serial port of your computer to the device that contains the card.

The Wizard can discover and configure Network Management Cards or devices only if they are on the same network segment as the computer that is running the Wizard.
Most software firewalls must be temporarily disabled for the Wizard to discover unconfigured Network Management Cards or other devices.

System requirements

The Wizard runs on Windows 2000, Windows 2003, and Windows XP workstations.

Install the Wizard

Automated installation

If autorun is enabled on your CD-ROM drive, the installation program starts automatically when you insert the CD.

Manual installation

If autorun is not enabled on your CD-ROM drive, run **setup.exe** in the Wizard directory on the CD, and follow the on-screen instructions.

You can also download the latest version of the APC Device IP Configuration Wizard from the APC web site, **www.apc.com** and run **setup.exe** from the folder to which you downloaded it.

Use the Wizard

Launch the Wizard

The installation creates a shortcut link in the **Start** menu that you can use to launch the Wizard.

Configure the basic TCP/IP settings remotely

Prepare to configure the settings. Before you run the Wizard, be sure that you have the information you will need during the configuration procedure:

1. Contact your network administrator to obtain valid TCP/IP settings.
2. If you are configuring multiple unconfigured Network Management Cards or network-enabled devices, obtain the MAC address of each one so that you can identify each Network Management Card or device that the Wizard discovers. (The Wizard displays the MAC address for a discovered card or device on the same screen on which you then enter the TCP/IP settings.)
   - For Network Management Cards that you install, the MAC address is on a label on the bottom of the card.
   - For a network-enabled device (with an embedded Network Management Card), the MAC address is on a label on the device — for example, usually on the side of a device that you mount in a rack.

   You can also obtain the MAC address from the Quality Assurance slip that came with the Network Management Card or device.

Run the Wizard to perform the configuration. To discover and configure, over the network, Network Management Cards or network-enabled devices that are not configured:

1. From the **Start** menu, launch the Wizard. The Wizard automatically detects the first Network Management Card or network-enabled device that is not configured.
2. Select **Remotely (over the network)**, and click **Next >**.
3. Enter the TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway**) for the unconfigured Network Management Card or network-enabled device identified by the MAC address at the top of the screen. Then click **Next >**.

   On the **Transmit Current Settings Remotely** screen, if you check-mark **Start a Web browser when finished**, the default Web browser connects to the Network Management Card or device after you transmit the settings.
4. Click **Finish** to transmit the TCP/IP settings. If the IP address you entered is in use on the network, the Wizard prompts you to enter an IP address that is not in use. Enter a correct IP address, and click **Finish**.
5. The Wizard searches for another unconfigured Network Management Card or device. If it finds one, it displays the screen with data entry boxes for the TCP/IP settings of that card or device.
   - To skip configuring the Network Management Card or device whose MAC address is currently displayed, click **Cancel**.
   - To configure the TCP/IP settings of the next card, repeat this procedure beginning at step 3.

Configure or reconfigure the TCP/IP settings locally

To configure a single Network Management Card or network-enabled device through a serial connection:

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

How to Export Configuration Settings

Retrieving and Exporting the .ini File

The enclosure must be secure when an .ini file upload is in progress. To secure the enclosure, close the front and rear doors, close both handles, and ensure that both locks are in the locked position.

Summary of the procedure

As an Administrator, you can retrieve a dynamically generated .ini file of the current configuration of the Rack Access PX and export that file to another Rack Access PX or to multiple Rack Access PXs.

1. Configure the Rack Access PX to have the settings you want to export.
2. Retrieve the .ini file from that Rack Access PX.
3. Customize the .ini file (to change at least the TCP/IP settings) and make a copy to export.
4. Use any of the file transfer protocols supported by the Rack Access PX to transfer the copied file to one or more additional Rack Access PXs. (To transfer the file to multiple Rack Access PXs simultaneously, write an FTP or SCP script that repeats the steps for transferring the file to a single Rack Access PX.)
5. Each receiving Rack Access PX stores the file temporarily in its flash memory, uses it to reconfigure its own settings, and then deletes the file.

To create batch files and use an APC utility to retrieve configuration settings from multiple Rack Access PXs and export them to other Rack Access PXs, see *Release Notes: ini File Utility, version 1.0* on the APC NetBotz Rack Access PX *Utility* CD.

Contents of the .ini file

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

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

  Note: Only section headings and keywords supported for the specific device (in this case the Rack Access PX) from which you retrieve the file are included.

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

    See Customizing for configuration guidelines for date and time settings.

Detailed procedures

Use the following procedures to retrieve the settings of the Rack Access PX and export them to one or more Rack Access PXs.

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

1. Configure the Rack Access PX with the settings you want to export.

   To avoid errors, configure the Rack Access PX by using its user interface whenever possible. Directly editing the .ini file risks introducing errors.

2. Use FTP to retrieve the file config.ini from the Rack Access PX you configured:
   a. Open a connection to the Rack Access PX, using its IP Address. For example:

      ```
      ftp> open 158.165.2.132
      ```

   b. Log on, using the Administrator user name and password configured for the Rack Access PX.
   c. Retrieve the config.ini file containing the Rack Access PX's current settings:

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

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

To create batch files and use an APC utility to retrieve configuration settings from multiple Rack Access PXs and export them to other Rack Access PXs, see *Release Notes: ini File Utility, version 1.0* on the APC NetBotz Rack Access PX *Utility* CD.

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

1. Use a text editor to customize the file.
   - Section headings, keywords, and pre-defined values are not case-sensitive, but string values that you define are case-sensitive.
   - Use adjacent quotation marks to indicate no value. For example, **`LinkURL1=""`** indicates that the URL is intentionally undefined.
   - To define values, opening and closing quotation marks are optional, except to enclose values that contain leading or trailing spaces or values which are already enclosed in quotation marks. (Leading or trailing spaces not within the opening and closing quotation marks are ignored.)
   - To export a specific system date and time or any scheduled events, you must configure the values directly in the .ini file.
     - To export a specific system time, export only the configured **`[SystemDate/Time]`** section as a separate .ini file. (The time necessary to export a large file would cause the configured time to be significantly inaccurate.)
     - For greater accuracy, if the Rack Access PXs receiving the file can access a Network Time Protocol (NTP) Server, set the value for the **`NTPEnable`** keyword as follows:

       `NTPEnable=enabled`
   - Add comments about changes that you made. The first printable character of a comment line must be a semicolon (`;`).
2. Copy the customized file to another file name in the same folder:
   - The copy, which you will export to the Rack Access PXs, can have any file name up to 64 characters and must have the .ini file suffix.
   - Retain the original customized file for future use. **The file that you retain is the only record of your comments.** They are removed automatically from the file that you export.

Transferring the file to a single Rack Access PX. To transfer the .ini file to one other Rack Access PX, do either of the following:

- From the Web interface of the receiving Rack Access PX, select the **Administration** tab, **General** on the top menu bar, and **User Config File** on the left navigation menu. Enter the full path of the .ini file to transfer or use the **Browse** button to identify the location of the .ini file.
- Use any of the file transfer protocols supported by Rack Access PXs (including FTP, FTP Client, SCP, and TFTP). The following example uses FTP:

  a. From the folder containing the customized .ini file and its copy, use FTP to log in to the Rack Access PX to which you are exporting the .ini file. For example:

  ```
  ftp> open 158.165.4.135
  ```

  b. Export the copy of the customized .ini file. The receiving Rack Access PX accepts any file name that has the .ini suffix, is no more than 64 characters in length, and is exported to its root directory.

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

Exporting the file to multiple Rack Access PXs. To export the .ini file to the multiple Rack Access PXs:

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

To create the batch file and use the utility, see *Release Notes: ini File Utility, version 1.0* on the APC NetBotz Rack Access PX *Utility* CD.

The Upload Event and Error Messages

The event and its error messages

The following event occurs when the receiving Rack Access PX completes using the .ini file to update its settings.

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

If a keyword, section name, or value is invalid, the event text is extended to include notification of the following errors.

The export to and the subsequent upload by the receiving Rack Access PX succeeds even if there are errors.

Event text	Description
Configuration file warning: Invalid keyword on line *number*. Configuration file warning: Invalid value on line *number*.	A line with an invalid keyword or value is ignored.
Configuration file warning: Invalid section on line *number.*	If a section name is invalid, all keyword/value pairs in that section are ignored.
Configuration file warning: Keyword found outside of a section on line *number*.	A keyword entered at the beginning of the file (i.e., before any section headings) is ignored.
Configuration file warning: Configuration file exceeds maximum size.	If the file is too large, the Rack Access PX stores and processes what it can, but ignores what it cannot. Reduce the size of the file, or divide it into two files, and try uploading again.

Messages in config.ini

The Rack Access PX from which you transfer the config.ini file must be discovered successfully in order for its configuration to be included. If the Rack Access PX is not present or, for some other reason, is not discovered, the config.ini file contains an error message under the appropriate section name, instead of keywords and values.

Errors generated by overridden values

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

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

The overridden values are device-specific and not appropriate to export to the other Rack Access PXs. Therefore, you can ignore these error messages. To prevent these error messages from occurring, 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.

Using the APC Device IP Configuration Wizard

On Windows operating systems, instead of using the preceding procedure for transferring .ini files, you can choose to update the basic TCP/IP settings of the Rack Access PX by using the APC Device IP Configuration Wizard.

See APC Device IP Configuration Wizard for a detailed description of how to discover and configure the basic TCP/IP settings of unconfigured Rack Access PXs remotely over your TCP/IP network or configure or reconfigure the one Rack Access PX through a direct connection from the serial port of your computer to the Rack Access PX.

File Transfers

Overview

The Rack Access PX automatically recognizes binary firmware files. Each of these files contains a header and one or more Cyclical Redundancy Checks (CRCs) to ensure that the data contained in the file is not corrupted before or during the transfer operation.

When new firmware is transmitted to the Rack Access PX, the program code is updated and new features become available.

This chapter describes how to transfer firmware files to the Rack Access PX.

To transfer a firmware file to a Rack Access PX, see Upgrading Firmware.

To verify a file transfer, see Verifying Upgrades and Updates.

Upgrading Firmware

Benefits of upgrading firmware

Upgrading the firmware on the Rack Access PX has the following benefits:

- New firmware has the latest bug fixes and performance improvements.
- New features become available for immediate use.
- Keeping the firmware versions consistent across your network ensures that all Rack Access PXs support the same features in the same manner.

Firmware files (Rack Access PX)

A firmware version consists of two modules: An APC Operating System (AOS) module and an application module.

The APC Operating System (AOS) and application module files used with the Rack Access PX share the same basic format:

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

- **`apc`**: Indicates that this is an APC file.
- *`hardware-version`*: **`hw0`***`x`* identifies the version of the hardware on which you can use this binary file.
- *`type`*: **`aos`** if the file is the APC Operating System (AOS) module, or **`accpx`** if the file is the application module for the Rack Access PX.
- *`version`*: The version number of the application file.
- **`bin`**: Indicates that this is a binary file.

Obtain the latest firmware version

Automated upgrade tool for Microsoft Windows systems. An automated self-extracting executable tool combines the firmware modules that you need to automate your upgrades on any supported Windows operating system. You can obtain the latest firmware version of the tool at no cost. At the support section of the APC web site **www.apc.com/tools/download**, find the latest firmware release for your APC product (in this case, your Rack Access PX) and download the automated tool, not the individual firmware modules.

Each upgrade tool is specific to an APC product type. Do not use the tool from one product CD to upgrade firmware of a different APC product. If you use a version of the tool from the APC Web site, make sure that you use the upgrade tool that corresponds with your APC product type.

Manual upgrades, primarily for Linux systems. If all computers on your network are running Linux, you must upgrade the firmware of the Rack Access PX manually, i.e., by using the separate APC firmware modules (AOS module and application module).

If you have a networked computer running a supported Microsoft Windows operating system on your network, you can use the tool described in Automated upgrade tool for Microsoft Windows systems to upgrade the firmware of the Rack Access PX automatically over the network. This tool automates the entire upgrade process.

You can obtain the individual firmware modules you need for a manual firmware upgrade from the support section of the APC Web site **www.apc.com/tools/download**.

Firmware file transfer methods

To upgrade the firmware of the Rack Access PX:

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

When you transfer individual firmware modules and do not use the automated firmware upgrade tool to upgrade the firmware for the Rack Access PX, you must transfer the APC Operating System (AOS) module to the Rack Access PX before you transfer the application module.

For more information about the firmware modules, see Firmware files (Rack Access PX).

Use FTP or SCP to upgrade one Rack Access PX

Instructions for using FTP. For you to be able to use FTP to upgrade a single Rack Access PX over the network:

- The Rack Access PX must be connected to the network.
- The FTP server must be enabled at the Rack Access PX.
- The Rack Access PX must have its TCP/IP settings (**System IP**, **Subnet Mask**, and **Default Gateway** addresses) configured.

To use FTP to upgrade the Rack Access PX:

1. Open an MS-DOS command prompt window on a computer that is connected to the network. Go to the directory that contains the firmware upgrade files, and list the files. For the directory **`C:\apc`**, the commands would be those shown in **bold**:

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

   Files listed for the Rack Access PX, for example, might be the following (with *xxx* representing the version number of each file):

   - **apc_hw03_aos_***xxx***.bin**
   - **apc_hw03_accpx_***xxx***.bin**

2. Open an FTP client session:

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

3. Type **open** and the Rack Access PX's IP address, and press ENTER. If the **port** setting for the FTP Server (accessible through the **Administration** tab, **Network** on the top menu bar, and **FTP Server** on the left navigation menu) has changed from its default of **21**, you must use the non-default value in the FTP command.
   a. For some FTP clients, use a colon to add the port number to the end of the IP address.
   b. For Windows FTP clients, separate the port number from the IP address by a space. For example, if the Rack Access PX's **FTP Server Port** setting has been changed from its default of **21**, such as to **21000**, you would use the following command for a Windows FTP client transferring a file to the Rack Access PX with an IP address of 150.250.6.10.
   ```
   ftp> open 150.250.6.10 21000
   ```
4. Log on using the Administrator user name and password. (**apc** is the default for both.)
5. Upgrade the AOS. (In the **put** command in the following example, *xxx* is the firmware version number, with no periods separating the digits:
   ```
   ftp> bin
   ftp> put apc_hw03_aos_xxx.bin
   ```
6. When FTP confirms the transfer, type **quit** to close the session.
7. Wait 20 seconds, and then repeat step 2 through step 5, but in step 5, use the application module file name instead of the AOS module.

Instructions for using SCP. To use Secure CoPy (SCP) to upgrade the firmware for one Rack Access PX:

1. Identify and locate the firmware modules described in the preceding instructions for FTP.
2. Use an SCP command line to transfer the AOS firmware module to the Rack Access PX. The following example assumes a Rack Access PX IP address of 158.205.6.185, and an AOS module of **apc_hw03_aos_*xxx*.bin**. (with **xxx** representing the version number of the AOS module, with no periods separating the digits).
   `scp apc_hw03_aos_xxx.bin apc@158.205.6.185:apc_hw03_aos_xxx.bin`
3. Use a similar SCP command line, with the name of the application module instead of the AOS module, to transfer the application module to the Rack Access PX.

Upgrade multiple Rack Access PXs

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

See *Release Notes: ini File Utility, version 1.0* on the APC NetBotz Rack Access PX *Utility* CD.

Use FTP or SCP to upgrade multiple Rack Access PXs. To upgrade multiple Rack Access PXs using an FTP client or using SCP, write a script which automatically performs the procedure. For FTP, use the steps in Use FTP or SCP to upgrade one Rack Access PX in the script.

Use XMODEM to upgrade one Rack Access PX

To use XMODEM to upgrade the firmware for a single Rack Access PX that is not on the network:

1. Obtain the individual firmware modules (the AOS module and the application module) from **www.apc.com/tools/download**.
2. Select a serial port at the local computer and disable any service which uses that port.
3. Connect the null modem cable (APC part number 940-0103) that came with the Rack Access PX to the selected port and to the serial port at the Rack Access PX.
4. Run a terminal program (such as HyperTerminal), and configure the selected port for 9600 bps, 8 data bits, no parity, 1 stop bit, and no flow control, and save the changes.
5. Press ENTER twice to display the **User Name** prompt.
6. Enter the Administrator user name and password (**apc** by default for both).
7. From the **Control Console** menu, select **System**, then **Tools**, then **File Transfer**, then **XMODEM**; and type **Yes** at the prompt to continue.
8. At the prompt for the baud rate, enter an appropriate baud rate for the terminal program to use for the transfer. A higher baud rate causes faster firmware upgrades.

   Allowed values are 2400, 9600, 19200, and 38400. To choose a baud rate different from your current connection, disconnect the null modem cable from the Rack Access PX before you change the terminal program's baud rate to match your selection, and reconnect the cable immediately afterwards.

   Press ENTER. The screen displays uppercase C, indicating transfer mode.

9. From the terminal program's menu, select the binary AOS file to transfer via XMODEM-CRC. After the XMODEM transfer is complete, set the baud rate to 9600 (if you selected a different rate in step 8). The Rack Access PX automatically restarts.
10. Repeat step 4 through step 9 to install the application module. In step 9, use the application module file name, not the AOS module file name.

For information about the file name format used for application modules, see Firmware files (Rack Access PX).

Verifying Upgrades and Updates

Overview

To verify that the firmware upgrade was successful, see the **Last Transfer Result** message, available through the **FTP Server** option of the **Network** menu (in the control console only), or use an SNMP GET to the **mfiletransferStatusLastTransferResult** OID.

Last Transfer Result codes

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

Use the Web interface to verify the versions of the upgraded APC Operating System (AOS) and application modules by selecting the **Administration** tab, **General** on the top menu bar, and **Factory Info** on the left navigation menu, or use an SNMP GET to the MIB II **sysDescr** OID.

Index

E

F

H

I

K

L

M

N

O

P

Q

R

S

T

U

W

X

APC Worldwide Customer Support

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

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

Direct InfraStruXure Customer Support Line	(1)(877)537-0607 (toll free)
APC headquarters U.S., Canada	(1)(800)800-4272 (toll free)
Latin America	(1)(401)789-5735 (USA)
Europe, Middle East, Africa	(353)(91)702000 (Ireland)
Japan	(0) 35434-2021
Australia, New Zealand, South Pacific area	(61) (2) 9955 9366 (Australia)

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

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

Copyright

990-2772 **03/2006**