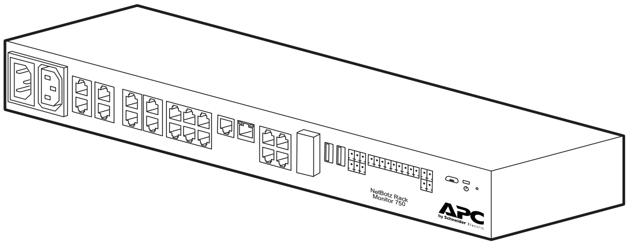
NetBotz 5.x

User Guide

NBRK0750

990-5934B-001
Release date: 02/2019



Legal Information

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

As standards, specifications, and designs change from time to time, please ask for confirmation of the information given in this publication.

Table of Contents

Preface

US Government Restricted Rights

Restricted rights legend. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software- Restricted Rights clause at CFR 52.227-19, as applicable.

Improper Use of Audio/Visual Recording Capabilities

Attention: THE EQUIPMENT CONTAINS, AND THE SOFTWARE ENABLES, AUDIO/VISUAL AND RECORDING CAPABILITIES, THE IMPROPER USE OF WHICH MAY SUBJECT YOU TO CIVIL AND CRIMINAL PENALTIES. APPLICABLE LAWS REGARDING THE USE OF SUCH CAPABILITIES VARY BETWEEN JURISDICTIONS AND MAY REQUIRE AMONG OTHER THINGS EXPRESS WRITTEN CONSENT FROM RECORDED SUBJECTS. YOU ARE SOLELY RESPONSIBLE FOR ENSURING STRICT COMPLIANCE WITH SUCH LAWS AND FOR STRICT ADHERENCE TO ANY/ALL RIGHTS OF PRIVACY AND PERSONALTY. USE OF THIS SOFTWARE FOR ILLEGAL SURVEILLANCE OR MONITORING SHALL BE DEEMED UNAUTHORIZED USE IN VIOLATION OF THE END USER SOFTWARE AGREEMENT AND RESULT IN THE IMMEDIATE TERMINATION OF YOUR LICENSE RIGHTS THEREUNDER.

Introduction

The APC by Schneider Electric NetBotz™ Rack Monitor 750 is a rack-mountable central hardware appliance for an environmental monitoring and control system. Once the system is installed, you can monitor and control your system using the Web User Interface (Web UI). This manual describes how to use the Web UI of a NetBotz Rack Monitor 750 (NBRK0750) to configure settings on your appliance, and how to use your appliance to monitor the environment and attached sensors and devices. (See the *Installation and Quick Configuration Manual* on *www.apc.com* for information on supported devices.)

The NetBotz Rack Monitor 750 has these additional features:

- Various levels of access: Super User and Administrator. (These are protected by user name and password requirements.)
- Configurable alarm thresholds that provide network and visual alarms to help avoid and address environmental risks.
- E-mail notifications for system events.
- SNMP traps, Syslog messages, and e-mail notifications based on the severity level of system events.
- Multiple user logon feature which allows up to four users to access the appliance simultaneously.
- Event logging.
- Security protocols for authentication and encryption.

Security Recommendations

NetBotz Appliances are not configured with the security infrastructure to be placed on the Web or on a public network. It is recommended that you take the following steps to protect your appliance:

- Connect your appliance to a private network with an appropriate level of access for authorized users.
- Connect your appliance to a subnetwork that is partitioned from your company's corporate network.
- Place a firewall between the appliance's LAN and your company's corporate network.
- Require authorized personnel to use a VPN when connecting to the network the appliance is on.
- Place the appliance in a physical environment where only authorized personnel have access to it.
- If you allow a customer support representative to make changes to your appliance, it is recommended that you create a temporary account for the support representative and remove the account when it is no longer needed.

Types of User Accounts

The appliance has three types of user accounts:

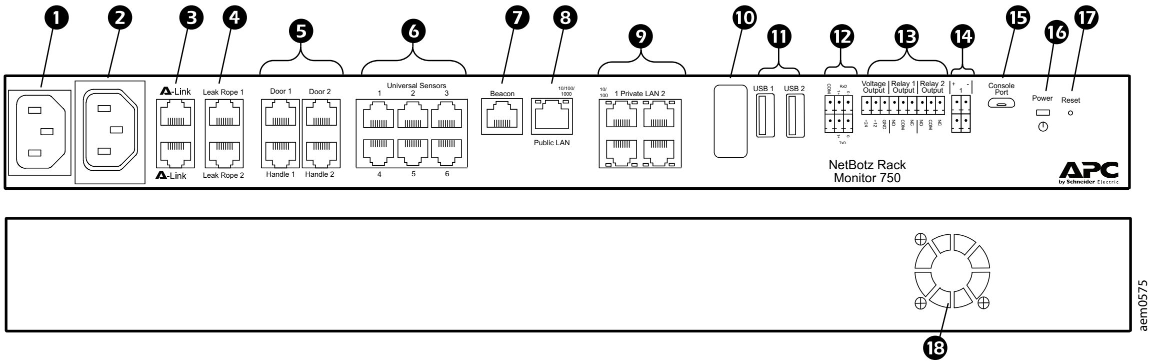
- Use the **Super User** account to log on to the Web UI after initial configuration. The super user can create, edit, or delete administrators.

  The default user name and password for this account are both **superuser**. The Super User is required to change the Super User password the first time they log on.

- **Administrators** (**admins**) are required to change their passwords when they first log on to the appliance. Admins can not create or edit other accounts.

- Use the **Root** account for procedures that require using the Console Port, e.g., when you use a terminal emulator to specify network settings. You set the default password the first time you log on. You can not change the default user name (**root**).

Physical Description



Item		Description
❶	AC line inlet	Input power connection.
❷	Switched Outlet	Provides power to a device at a maximum of 10 A. Activates a connected device when configured events occur. (For example, a fan may be connected to this outlet, and the outlet may be configured to turn on when certain alarms are generated.)
❸	A-Link ports	Provide communications and power to connected devices (sensor pods, rack access pods, and temperature/humidity sensors with digital displays) over standard CAT-5 cabling with straight-through wiring. For instructions to cascade devices, see the *Installation and Quick Configuration Manual* on *www.apc.com*.
❹	Leak Rope port	Used for connecting a NetBotz Leak Rope Sensor (NBES0308).
❺	Rack Access Ports*	Ports for the door switch sensors (NBES0302 or NBES0303) and handle sensors (NBHN125 or NBHN1356).
❻	Universal Sensor ports	Used to connect APC by Schneider Electric sensors, third-party dry-contact sensors, and standard, third-party 0–5 V sensors. Third-party, dry-contact state sensors require the NetBotz Dry Contact Cable (NBES0304), and third party, 0–5 V sensors require the NetBotz 0–5 V sensor cable (NBES0305).
❼	Beacon port	Used for connecting an Alarm Beacon (AP9324).
❽	10/100/1000 Network port	Provides a connection to the network. Status and link Light-emitting Diodes (LEDs) indicate network traffic. See *Link (10/100/1000) LED, page 9* and *Status LED, page 9* for details.
❾	Private LAN	Provides a 10/100/1000 connection to a private local area network and 48 VDC to an attached device.
❿	Wireless Sensor Coordinator	USB Port with Wireless NetBotz USB Coordinator (NBWC100U) installed. Used with wireless sensors.
⓫	USB Type A ports	Reserved for future use.
⓬	Modbus RS485 port	Reserved for future use.
⓭	Voltage Output	Provides 12 VDC or 24 VDC (75 mA) to one connected device.
	Relay Output ports 1, 2	Used for connecting relay-controlled external devices. Relay Outputs can only be connected to Class 2 circuits.
⓮	4–20 mA Inputs	Inputs for industry standard 4–20 mA sensors.
⓯	Console port	Provides a serial connection to the appliance.
⓰	Power LED	Illuminates when the unit is receiving power.
⓱	Reset switch	Reboots the appliance.
⓲	Exhaust fan	Exhausts hot air from the appliance.

*Not supported on firmware version 5.0.1. Update the firmware to access these features. See *Update the Appliance Firmware, page 41* for instructions to update the firmware.

Link (10/100/1000) LED

The LED on the right of any network port indicates the network status.

Condition	Description
Off	One or more of the following situations exist: • The appliance is not receiving input power. • The cable that connects the appliance to the network is disconnected or not functioning properly. • The appliance is turned off or not operating correctly. It may need to be repaired or replaced. Contact Customer Support at *www.apc.com/support*.
Solid green	The appliance is connected to a network operating at 100 Megabits (Mb) per second or 1000 Mb/1Gigabit (Gb) per second.
Solid orange	The appliance is connected to a network operating at 10 Mb per second.
Flashing green	The appliance is receiving or transmitting data packets at 1 Gb per second.
Flashing orange	The appliance is receiving or transmitting data packets at 10 Mb or 100 Mb per second.

Status LED

The LED on the left side of any network port indicates the status of the appliance.

Condition	Description
Off	One of the following situations exists: • The appliance is not receiving input power. • The appliance is not operating properly. It may need to be repaired or replaced. Contact Customer Support at *www.apc.com/support*.
Alternately flashing green and amber	The appliance ist waiting for a DHCP server to assign a valid IP address.
Solid green	The appliance is on and has a valid IP address.

Getting Started

To start using your NetBotz appliance,

1. Install and apply power to the appliance using the *Installation and Quick Configuration Manual* shipped with your appliance. (You can also find the *Installation and Quick Configuration Manual* on *www.apc.com*.)
2. Establish network settings.
3. Access the Web UI of the appliance.

Establish Network Settings

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

- IP address of the appliance
- Subnet mask
- Default gateway
- At least one IP address for a Domain Name System (DNS) server

You can use DHCP to configure network settings automatically, or use a terminal emulator to configure network settings manually.

Use DHCP to Establish Network Settings

By default, your appliance uses Dynamic Host Configuration Protocol (DHCP) to configure network settings. When you apply power to the appliance, it automatically attempts to contact a DHCP server.

Use a Terminal Emulator to Establish Network Settings

1. Connect a USB-A to Micro USB-B cable to the Console Port on the NetBotz appliance and a USB port on your computer.
2. Plug the power cord provided with your appliance into a wall outlet, and then connect it to the AC line inlet.

   The green Power LED illuminates. The appliance can take up to two minutes to initialize, depending on configuration settings.
3. Open a serial connection on your terminal emulator using port settings 115,200 baud, 8 data bits, no parity, 1 stop bit, and 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.
   - The Silicon Labs CP210x driver is installed on your computer. (You can find the driver on *www.silabs.com*.)
5. Log on with the Root account user name (**root**) and password (you set the password on first use).
6. Configure your appliance to use network settings assigned by a DHCP server, or provide an IP address, subnet mask, gateway address, and at least one IP address for a DNS server.
7. Save your configuration settings, and close the terminal emulator.
8. Test the IP connection of the appliance: start your Web browser and type the IP address of the appliance into the URL address bar. Press **Enter**. If the appliance is online and properly configured, the Web UI displays in the browser window.

Access the Web User Interface (Web UI)

NOTE: The Web UI takes about six minutes to become available after start-up.

After the network settings are configured, you can access the appliance through the Web UI. The Web UI provides a real-time overview of alerts and device details, including sensor readings and images captured by cameras. You can use Microsoft Internet Explorer (IE) 11, Google Chrome 67, or Mozilla Firefox 62 (or later versions of these Web browsers) on Windows 7 and 10 operating systems to access the appliance through its Web UI. Other commonly available browsers and operating systems may work but have not been fully tested.

1. Enter the host name or IP address of the appliance in the Web browser's URL address bar. (If you used DHCP to automatically obtain the IP address of the appliance, you can use a terminal emulator to view your current IP address. Follow steps 1–5 of *Use a Terminal Emulator to Establish Network Settings, page 10*.) You may receive a message that the Web page is not secure. This is normal when using self-signed certificates, and you can continue to the Web UI.

   Your appliance comes with a self-signed certificate installed. Browsers generate a security warning because they do not recognize the authority who signed the certificate. You can prevent the warning message by installing a certificate signed by a Certificate Authority (CA) the Web browser recognizes (see *Configure Certificates for Inbound Connections, page 38* for more information). You can also direct the browser to accept the certificate to prevent the warning.

2. Use your user name and case-sensitive password to log on. The default user name and password for the Super User are both superuser. For Administrators, there is no default user name or password. The Super User must define the user name and password for Administrators.

   Both the Super User and Administrators must change their passwords at first log on. Use strong passwords that comply with your company's password requirements.

Reset a Lost Root Account Password

1. Connect a USB-A to Micro USB-B cable to the Console Port on the NetBotz appliance and a USB port on your computer.

2. Disconnect and reconnect power to the appliance. Immediately press any key on your computer. If you do not press a key within five seconds after you connect power to the appliance, the appliance will restart normally.

3. Enter the following three commands:

   ```
   env set resetpwd true
   env save
   boot
   ```

   Wait for the system to restart.

4. Log on as the Root user. When prompted, reset the Root account password.

5. Disconnect and reconnect power to the appliance. Immediately press any key on your computer. If you do not press a key within 5 seconds after you connect power to the appliance, the appliance will restart normally.

6. Enter the following three commands:

   ```
   env set resetpwd false
   env save
   boot
   ```

   Wait for the system to restart.

NOTE: If you do not complete steps 5 and 6, the root password will be reset every time the appliance restarts.

Reset a Lost Super User Password

1. Connect to the appliance with SSH or through the console port on your computer. Log on with the root account user name and password, then press **Shift + x Enter** within 5 seconds of logging on.
2. Navigate to `/netbotz_app` and enter the following command:

   ```
   ./restart.sh stop startApp startClubber resetsupwd
   ```

   The appliance restarts.
3. Log on to the appliance as the Super User (both the user name and password are **superuser**).
4. Change the default password.

Reset to Defaults

This procedure reboots the appliance and resets all system settings (including passwords) to factory defaults.

> **NOTE:** This procedure causes the appliance IP address to be reset. In some cases, you may lose access to the appliance and may need to use a local connection to reset or rediscover the IP address.

1. Log into the Web UI as the Super User.
2. Open a new browser page, type `<`*`your appliance's IP address`*`>/rest/appliance/resetconfig` in the URL address bar, the press **Enter**.

   Example: `10.218.123.234/rest/appliance/resetconfig`

   > **NOTE:** For firmware v5.0.1, type `<`*`your appliance's IP address`*`>/rest/settings/appliance/recondition`.

   The appliance takes about six minutes to restart completely. Until the restart is complete, the Web UI is not available.
3. If needed, use a terminal emulator to view or reset the IP address of the appliance. See *Use a Terminal Emulator to Establish Network Settings, page 10* for instructions.

The next time you log on to the appliance, you must reset the Super User password.

Network Management with Other Applications

You can also manage the appliance with the following applications:

- StruxureWare Data Center Expert® (DCE): Provide enterprise-level power management and management of agents, Rack PDUs, and environmental monitors.

  > **NOTE:** You must enable and configure Simple Network Management Protocol (SNMP) before DCE can discover the appliance. See *Configure SNMP Settings, page 37* for instructions.

Web UI Features

The following features can be found throughout the Web UI.

Tabs

The following tabs are available:

- **Overview:**The default tab when you log on. View all devices attached to the appliance.
- **Alarms:** View detailed information about alarms. Filter information by alarm and status.
- **Cameras:** View detailed information for all camera pods and camera discoveries. Add or remove camera pods, and configure camera pod settings.
- **Rack Access:** View detailed information for rack access devices and register individual rack access users.

  NOTE: This tab is not available in firmware v5.0.1. Update the firmware to enable rack access.
- **Wireless:** View detailed information for all wireless devices, add or remove a wireless sensor, and update the wireless sensor network.
- **Settings:** Configure appliance settings including notifications, alarms, network settings, and user accounts. Update the firmware and create backup files.

Quick Status Icons and the Quick Status Area

Quick status icons indicate the severity of alarms. They appear next to alarms, sensors that generate alarms, and in the Quick Status area.

ℹ Information

⚠ Warning

✖ Critical

The Quick Status area (in the upper left of the Web UI) displays the number and severity of active alarms. Click any icon in the Quick Status area to go to the **Alarms** tab.

For more information on alarms, see *Alarms Tab, page 18* or *Configure Alarms, page 30*.

Quick Links

Three links appear in the upper right corner:

- **Help:** Links to the EcoStructure IT Help site, *help.ecostruxureit.com*, where you can ask questions or download additional documentation.
- **Logs:** Allows you to download information from the appliance log. Customer support can use this information for troubleshooting.
- **Logout:** Select this link to log out of the appliance.

Details Windows

Select any device connected to your appliance to see the details window for that device. Details provided vary by device.

Detail	Description
Label	A customizable name for each device. To change the label for any device, open the details window and click Edit ✎.
General information	Depending on the device, this may include hardware information (for example, the model or manufacturer of a device), network information (for example, the MAC address or IP address of a wireless sensor), or alarm status. See *Configure Alarms, page 30* for instructions to create alarms for individual devices.
Sensor details	For some NetBotz sensors, graphs show up to 96 hours of sensor history. Click any graph to open a graph window, where you can do any of the following: • Select **Table** to view the sensor history as a table. • Click Download ⤓ to save a comma separated values (CSV) file of the sensor history to your computer. • Hover over the graph to see sensor measurements from an exact time. State sensors do not show graph information, though you can click the sensor information to view a table or download a CSV file with up to 96 hours of sensor history. This is because state sensors detect a single condition (for example, the presence of smoke) instead of a range of values (for example, the temperature).
Camera details	View a live feed from the camera, or edit camera settings. See *Configure the Camera Pod Settings, page 16* for instructions to configure settings.
Outlet-controlled device detials	Details windows for outlet-controlled devices show whether the device is **Active** or **Inactive**, and provide an option to change this setting manually.
Commissioned/ Decommissioned status	Wireless devices only. **Commissioned** devices are connected to the wireless sensor network and report data to the appliance. **Decommissioned** devices are not connected to the wireless sensor network and do not report data to the appliance. You must commission a wireless devices for it to report data to the appliance. You must decommission a wireless device before you can remove it. You can change this status by clicking Commission🔗 or Decommission ⛓. See *Wireless Tab, page 25* for more information on the wireless sensor network and instructions to add or remove a wireless sensor.
Mode	This setting is exclusive to wireless devices. The **Mode** indicates what role a wireless device plays on the wireless sensor network. See *The Wireless Sensor Network, page 26* for more information.
Zigbee channel	This setting is exclusive to the coordinator for the wireless sensor network. Customer support can use it to help you trouble shoot the wireless sensor network.
Card reader	This setting is exclusive to rack access devices.
Video capture	You can configure alarms so that attached camera pods record video while the alarm is active (see *Configure Alarms, page 30*). If a connected device triggers an alarm with this feature enabled, the video recording appears at the bottom of the details window for that device. The appliance can store up to 96 hours of video per camera at a resolution of 1920x1080 pixels and a frame rate of 30 frames per second (f/s). Video capture is automatically deleted after 96 hours.

Overview Tab

The **Overview** tab displays feedback from cameras, sensors, and other devices connected to the appliance or the wireless sensor network. You can also use this tab to view detailed sensor information, customize 4–20 mA sensors, control devices by outlet, configure camera settings, and remove any sensor or device from the appliance.

There are three default tables on the **Overview** tab:

- **Appliance:** This table includes two outputs, one switched outlet, and two current inputs. These correspond to your appliance's relay outputs ports, voltage output port, and sensor input ports, respectively.
- **Appliance Rack Access** (**Enclosure** in firmware v5.0.1): This empty table can be populated with rack access handles and door sensors on firmware v5.1.0 and higher.
- **Wireless:** This table automatically includes the wireless coordinator attached to your appliance. If you add more wireless sensors to your wireless sensor network, they will appear here.

Most devices will automatically appear in the default tables as you connect them to the appliance. Sensor pods attached to the A-Link ports will appear as separate overview tables with attached and internal sensors listed as table items.

> **NOTE:** You can select the name of any non-wireless table to view information for that table and edit its title.

Information	**Description**
Alarm status	If there is an active alarm for any device, a quick status icon appears to the left of the device.
Port	A port icon indicates the port the device is connected to. If the port is numbered, the port number is also shown. Beacon 4–20 mA input Switched outlet Universal, USB, or Voltage output Rack Access (Available in firmware v5.1.0 or higher) Leak rope Wireless
Label	To edit the label for any device, select the device to open its details window, then click Edit.
Status information	Up to two sets of status information or sensor feedback are shown for each connected device. If a sensor provides more than two kinds of feedback, you can select the sensor to view all feedback in the details window.

Customize 4–20 mA Sensors

Select the sensor, then select **Customize**.

Setting	Description
Sensor type	Determines what units are measured.
Minimum input value	A value in milliamperes (mA) that corresponds to the **Minimum mapped value**.
Maximum input value	A value in mA that corresponds to the **Maximum mapped value**.
Minimum mapped value	The minimum value measured by the sensor.
Maximum mapped value	The maximum value measured by the sensor.

NOTE: Wait a few seconds for the sensor to configure itself.

Control Devices by Outlet

Outlet-controlled devices include devices connected to the beacon port, switched outlet, or relay output ports. You can select an outlet-controlled device to view its current status, or manually change the status of the device (from **inactive** to **active** or from **active** to **inactive**).

You can also configure alarms that will change the state of an outlet. See *Configure Alarms, page 30* for instructions.

Configure the Camera Pod Settings

Select any camera feed to open the details window. Under **Live Feed**, a **Motion** or **No Motion** label tells you whether the camera pod detects motion within your configured parameters. To edit those parameters, select **Settings**, and configure any of the camera pod settings.

Setting	Description
Motion Masking	To detect motion, cameras compare image capture frames for differences in pixels. Configure **Motion Masking** settings so that the camera only compares pixels in specific parts of the frame. Click and drag your mouse to draw one or more motion masking boxes on the view pane. The camera will not detect motion inside the masking boxes. To remove the motion masks, click **CLEAR ALL**. **NOTE: Motion Masking** is available on firmware v5.1.0 and higher.
Sensitivity	Specify how much change (in percent of pixels) between image captures is considered movement. Only pixels outside the masking box are measured. Lower values indicate higher sensitivity. **NOTE:** The **Sensitivity** setting is available on firmware v5.1.0 and higher.
Framerate	Select how many images (or frames) are recorded per second.
Resolution	Select the pixel resolution used for the images captured by the camera.

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

NOTE: See *Add a Camera Pod, page 19* to connect a Camera Pod 165.

NOTE: You can configure alarms that are generated by motion-detection settings in firmware v5.1.0 and higher. See *Configure Alarms, page 30* for details.

Remove a Wired Device

NOTE: When a device is removed, history and alarms for that device are deleted.

1. Disconnect the device from your appliance. Wait for the device to show as **Disconnected** 🔌 in the Web UI.
2. In the Web UI, select the device. In the details window, click Remove 🗑.
3. In the **Confirm** window, click **YES** to remove the device or **NO** to keep the device.

Remove a Camera Pod

NOTE: When a camera pod is removed, history and alarms for that camera pod are deleted.

Local camera pods (which are connected directly to the appliance) say **Auto** next to the label. Remote camera pods (which are connected to the appliance wirelessly) say **Manual** after the label.

To remove a local camera pod,

1. Disconnect the camera pod from your appliance. Wait for the device to show as **Disconnected** in the Web UI.
2. In the Web UI, select the camera pod. In the details window, click Remove 🗑.
3. In the **Confirm** window, click **YES** to remove the camera pod or **NO** to keep the camera pod.

To remove a remote camera pod,

1. Select the camera pod in the Web UI, then click Remove 🗑.
2. In the **Confirm** window, click **YES** to remove the camera pod or **NO** to keep the camera pod.

Remove a Wireless Sensor

NOTE: When a sensor is removed, history and alarms for that sensor are deleted.

1. Select the sensor. In the details window, click Decommission 🔗, then click **APPLY**.
2. In the **Confirm** window, click **YES**.
3. Select the sensor again, then click Remove 🗑.

Alarms Tab

You can use the **Alarms** tab to view all alarms. To view alarms, select parameters that define which alarms you want to view. Each alarm that fits the selected parameters appears with a quick status icon to show the severity of the alarm, a description of what caused the alarm, and the time and date the alarm was activated.

Parameter	Description
Critical	Show critical alarms.
Warning	Show warning alarms.
Informational	Show informational alarms.
All	Show active and resolved alarms.
Active	Show any alarm for which the cause of the alarm still exists.
Resolved	Show any alarm for which the cause of the alarm no longer exists.

> **NOTE:** Resolved alarms are stored for 96 hours. The appliance deletes alarms when the devices that generate the alarms are disconnected or removed from the wireless sensor network.

Select an alarm to view whether the relevant device is connected, graphical information (if applicable), and the time the alarm was resolved (if applicable). If the alarm is resolved, select the date or the quick status icon to view this information.

Clip Capture

The **Clip Capture** feature records video when an alarm is active. Once an alarm with **Clip Capture** is activated, a camera button appears next to the alarm. You can select the alarm to view the video recording in the details window.

To configure alarm settings or to enable **Clip Capture**, see *Configure Alarms, page 30*. To configure **Clip Capture** settings, see *Configure Video Capture Settings, page 40*.

Pagination

In firmware v5.1.0, up to 25 alarms are displayed per page. Click **FIRST**, **PREVIOUS**, **NEXT**, and **LAST** to navigate alarm pages.

The **Alarms** tab is not automatically updated while you view it. Select ⟳ **Refresh** to check for new alarms.

Cameras Tab

The **Cameras** tab displays thumbnail views and identification information for all Camera Pods monitored by the appliance. You can use the **Cameras** tab to add up to four Camera Pod 165 units to the appliance and configure their settings (see *Configure the Camera Pod Settings, page 16*).

Camera pods can be local or remote. Local camera pods are connected to the private network (Private LAN ports) and are discovered automatically. Remote camera pods must be discovered manually (see *Add a Camera Pod, page 19*).

The **Camera Discoveries** list records local cameras and information events for each discovered camera, which can be used for troubleshooting. To see information events for a camera, select the camera discovery, then select **Details**. To remove a camera discovery, click Delete ✖. It may take a few seconds for the discovery to be removed.

Add a Camera Pod

The appliance supports up to four Camera Pod 165 (NBPD0165) units.

> **NOTE:** The appliance counts disconnected and decommissioned camera pods as supported units. Remove disconnected or decommissioned camera pods before replacing them with new ones.

Add a Local Camera Pod

Connect the Camera Pod to a Private LAN port. On the **Cameras** tab, the camera pod appears under **Camera Discoveries**.

> **NOTE:** If the camera pod has previously been connected remotely, reset the camera after you connect it to the appliance. If you do not reset the camera, it may take hours or days to appear in the Web UI (the time depends on your company’s DHCP configuration).

Add a Remote Camera Pod

Click **+ADD**, and type the following information into the appropriate fields:

- **Hostname:** the host name or IP address of the camera pod
- **Username:** enter **apc** (the user name to log on to the camera pod)
- **Password:** enter **apc** (the password to log on to the camera pod)

You can use the **NetBotz Device Search** program to discover the IP address of your Camera Pod 165, or to assign a static IP address.

> **NOTE:** Camera streams from remote cameras are always transmitted using HTTP, not HTTPS.

Discover the IP address of your Camera Pod 165

1. Connect your computer to the same subnet as the Camera Pod 165.
2. Go to the Camera Pod 165 product page on *www.apc.com*. Download and open the **NetBotz Device Search** executable file.
3. In the **NetBotz Device Search** window, select **All NetCard** from the **Local Broadcast** drop down list, then click **Device Search**. Wait for the search to finish. You can identify your Camera Pod by the MAC address on the back of the unit.

Set the IP Address of your Camera Pod 165

1. Follow the instructions to Discover the IP address of your Camera Pod 165.
2. In the **Device Search** window, right-click the Camera Pod 165 and select **Network Setup** to open the **Network Setup** window.
3. Select **Static IP**, and enter the static **IP address**, default gateway (**Gateway**), Subnet Mask (**Netmask**), and Domain Name System server (**DNS**) for your Camera Pod 165.

Configure the Camera Pod Settings

Select any camera feed to open the details window. Under **Live Feed**, a **Motion** or **No Motion** label tells you whether the camera pod detects motion within your configured parameters. To edit those parameters, select **Settings**, and configure any of the camera pod settings.

Setting	Description
Motion Masking	To detect motion, cameras compare image capture frames for differences in pixels. Configure **Motion Masking** settings so that the camera only compares pixels in specific parts of the frame. Click and drag your mouse to draw one or more motion masking boxes on the view pane. The camera will not detect motion inside the masking boxes. To remove the motion masks, click **CLEAR ALL**. **NOTE: Motion Masking** is available on firmware v5.1.0 and higher.
Sensitivity	Specify how much change (in percent of pixels) between image captures is considered movement. Only pixels outside the masking box are measured. Lower values indicate higher sensitivity. **NOTE:** The **Sensitivity** setting is available on firmware v5.1.0 and higher.
Framerate	Select how many images (or frames) are recorded per second.
Resolution	Select the pixel resolution used for the images captured by the camera.

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

NOTE: See *Add a Camera Pod, page 19* to connect a Camera Pod 165.

NOTE: You can configure alarms that are generated by motion-detection settings in firmware v5.1.0 and higher. See *Configure Alarms, page 30* for details.

Remove a Camera Pod

> **NOTE:** When a camera pod is removed, history and alarms for that camera pod are deleted.

Local camera pods (which are connected directly to the appliance) say **Auto** next to the label. Remote camera pods (which are connected to the appliance wirelessly) say **Manual** after the label.

To remove a local camera pod,

1. Disconnect the camera pod from your appliance. Wait for the device to show as **Disconnected** in the Web UI.
2. In the Web UI, select the camera pod. In the details window, click Remove 🗑.
3. In the **Confirm** window, click **YES** to remove the camera pod or **NO** to keep the camera pod.

To remove a remote camera pod,

1. Select the camera pod in the Web UI, then click Remove 🗑.
2. In the **Confirm** window, click **YES** to remove the camera pod or **NO** to keep the camera pod.

Rack Access Tab

NOTE: Rack Access supported on firmware v5.1.0 and higher. See *Update the Appliance Firmware, page 41* for instructions to update the firmware.

NOTE: If you plan to use an authentication server to control rack access, configure the server first. (See *Configure LDAP Settings for Rack Access, page 39* for instructions to configure the authentication server.)

You can use the **Rack Access** tab to register proximity cards and schedule rack access. You can register one card at a time. Your rack access handles determine what kind of cards you can use.

Handle	Supported card types
Rack Access Pod 170 (NBPD0171 or NBPD0172)	• H10301—Standard 26 bit: An access card with a 26-bit card ID number and a facility code. • H10302—37 bit w/o facility code: An access card with a 37-bit card ID number and no facility code. • H10304—37 bit w/ facility code: An access card with a 37-bit card ID number and a facility code. • Corporate 1000 (CORP-1000) 35-bit: An access card with a 35-bit card ID number and a unique company ID code.. • Corporate 1000 (CORP-1000) 48-bit: An access card with a 48-bit card ID number and a unique company ID code.
NetBotz 125 kHz Handle Kit (NBHN0125)	• H10301 26-bit • H10302 37-bit • H10304 37-bit with facility code • CORP-1000 35-bit
NetBotz 13.56 MHz Handle Kit (NBHN1356)	• MIFARE Classic 4-byte UID • MIFARE Classic 7-byte UID • MIFARE DESFIRE • MIFARE PLUS • iClass

The **Audit** table shows rack access events in the last 96 hours. If there are too many events for one page, you can click **FIRST**, **PREVIOUS**, **NEXT**, or **LAST** to navigate between the pages. The **Audit** table is not automatically updated. Select ⟳ **Refresh** to update the **Audit** table.

Register a Proximity Card

Follow this procedure to register a new rack access card, or to re-register a deleted card. Registered cards can be associated with local users or LDAP users.

Local users have information that is stored directly on the appliance.

LDAP users have information stored on your company's LDAP server. When a proximity card is registered, or when a user tries to access a rack, the appliance retrieves and stores user information from your company's LDAP server. This information is used to verify the existence of the user. The appliance uses the stored information if the same user tries to access a rack within the next 10 minutes, or if the LDAP server is unavailable. Otherwise, the appliance retrieves new information every time a user tries to access a rack.

> **NOTE:** If a user is deactivated, they will still be able to access the rack. To remove a user, delete them from the LDAP server.

> **NOTE:** If a user is deleted on the LDAP server and the server becomes unavailable, the user may be able to access the racks using stored information until the server becomes available again.

1. Swipe the proximity card at a rack access handle. The card appears in the **Unregistered Cards** list.

2. If the card user is not stored on your company's authentication server, or if you want to provide the user with permission to access the rack when the LDAP server is unavailable, select **Local User**. If the card user is stored on your company's authentication server, you can select **LDAP**.

   Local User: Enter the card owner's name in the **User** field, then click **Register**.

   LDAP: Click **SEARCH LDAP**. In the **LDAP Search** window, click **ADD FILTER** and select at least one of the following attributes. Then click **SEARCH.**

Attribute	Description
Common Name	Typically the user's full name (first and last name).
UID	Typically the user's company ID. This is often, but not always, the first letter of the user's first name and the users last name.
Given Name	Typically the user's first name.
Surname	Typically the user's family name.
Sam Account Name	For Microsoft Active Directory® users, this is the name used to log on to Windows™.

   You can add more filters to narrow the search, or click delete 🗑 to remove a filter.

   > **NOTE:** The search will only return results for attributes that have been configured for the user on the company's LDAP server. Users and attributes can not be configured on the NetBotz appliance. New LDAP users and user attributes must be configured through the company's LDAP server.

   Select the user. Click **SELECT** to choose that user, then select **REGISTER**.

3. Select at least one door the card user can open from the drop-down list. (If you do not select a door, the card owner can not access the rack.) Click **+ADD** to add the selected door, or **+ADD ALL** to add all available doors.

   > **NOTE:** If a door switch sensor is not connected to the appliance, no doors are available to select.

Click **OK** to save your changes or **CANCEL** to discard them.

Schedule Rack Access

NOTE: The proximity card must be registered and assigned to a door before rack access can be scheduled. Complete the procedure to *Register a Proximity Card, page 23* and click **OK** before you schedule rack access.

Select **Edit**, then click schedule 📅.

Setting	Description
Schedule	By default, the card user is allowed access at all times. Click to disable access during any 15-minute increment. Click again to re-enable access. You can select column headings to disable access during any day of the week, or you can select row headings to disable access during a specific time of the day.
Access	Set **Long Access** and **Auto Lock Timeout** for individual doors. The **Global Door Auto Lock Timeout** setting still applies to all doors and cannot be disabled (see *Set Global Auto Lock Timeout, page 36*).
Long Access	When enabled, this setting disables **Auto Lock Timeout** and allows the cardholder unlimited access to the door. When this setting is deselected, **Auto Lock Timeout** resumes.
Auto Lock Timeout	This value determines the number of seconds before an unlocked handle re-locks. (This only applies to closed handles on closed doors — open handles and open doors will not re-lock). The default value is 10 seconds.

Click **APPLY** to save your changes.

Wireless Tab

You can use the **Wireless** tab to view detailed information about the wireless sensor network, add and remove sensors on the network, and update sensor firmware.

Sensor information		Description
Name		Also called the **Label**. You can edit this in the details window. (See *Details Windows, page 14*.)
MAC Address		The MAC address of each wireless device is a unique identifier assigned to the network interfaces for communication. While most networks use traditional 48 bit MAC addresses, the ZigBee technology used in the NetBotz wireless network requires 64 bit addresses. Valid MAC address forms include the following: • XXXXXXXXXXXXXXXX (for example, 282986FFFE123456) • XX:XX:XX:XX:XX:XX:XX:XX (for example, 28:29:86:FF:FE:12:34:56) • XX-XX-XX-XX-XX-XX-XX-XX (for example, 28-29-86-FF-FE-12-34-56)
Model		The part number for the unit. Because coordinators and routers all have the same part number (NBWC100U), **-C** is used to set the coordinator apart (**NBWC100U-C**).
Status		**Disconnected:**The device is setting up communication with your appliance. For an end device, this process may take up to one hour. If an end device does not set up communication with your appliance within an hour, the end device will wait for six hours before trying to set up communication again. You can restart the end device to force it to retry communication setup immediately. For a router, this process may take up to seven minutes. If the router does not set up communication with your appliance within seven minutes, it will retry communication setup again in five minutes. You can restart the router to force it to retry communication setup immediately. **Pending update:** New firmware is available. **Updating:** New firmware is being loaded to the wireless device. **Updated:** New firmware has been loaded to the wireless device. **Error:** New firmware could not be loaded to the wireless device. **Decommissioned:** The sensor is not connected to the wireless sensor network and does not send information to the host appliance. **Connected:** The sensor is connected to your wireless sensor network and can send information to the host appliance.
Battery		The current battery voltage reading from the wireless device. Firmware updates may not be successful if the battery voltage drops below 2.8 V.
RSSI		Received Signal Strength Indication in decibels (dB).
Versions	**Current**	The current firmware version used by the wireless device.
	Staging	Firmware that has been loaded to the wireless devices but is not yet active. If the **Staging** firmware version does not match the **Current** firmware version, click **APPLY**. If the **Staging** firmware version does not match the **Target** firmware version, update the firmware (see *Update the Wireless Sensor Network, page 28*).
	Target	The latest wireless firmware available. This is automatically populated when you update the firmware on your appliance. If the **Target** firmware version does not match the **Staging** firmware version, update the firmware (see *Update the Wireless Sensor Network, page 28*).

The Wireless Sensor Network

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

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

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

Devices on the Wireless Sensor Network

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

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

Connect the Wireless Sensor Network

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

1. Select the coordinator and routers: If a USB Coordinator and Router (NBWC100U) comes pre-installed on your appliance, then the pre-installed USB Coordinator and Router will act as you coordinator. Note the extended address of the coordinator. If necessary, choose one or more USB Coordinator & Routers to become routers.
2. Choose the locations for the routers and end devices. Do not power the routers or end devices at this time.
3. Power the coordinator first: On appliances with a USB Coordinator and Router installed, the coordinator is powered when you power the appliance. Otherwise, connect one USB Coordinator & Router to a USB Type A port on the NetBotz appliance.
4. Use an AC-USB adapter to apply power to each router. Routers are not directly connected to the NetBotz appliance.
5. Apply power to the end devices after the coordinator and the routers are powered. This helps to preserve battery life.
6. Add end devices (wireless sensors) to the wireless sensor network. See *Add Sensors to the Wireless Sensor Network, page 27* for instructions.

Add Sensors to the Wireless Sensor Network

Follow the instructions to *Connect the Wireless Sensor Network, page 27*. Then, in the **Wireless** tab, click **ADD**, and select one of the following.

Add Detected Sensors

1. Select any automatically detected device, or use the **Search** field to find the MAC address for a specific end device. You can enter a name for any selected sensor in the **Name** field.
2. Click **ADD** to add all selected sensors to the wireless sensor network, or click **CANCEL** to close the window.

Add Sensors Manually

1. Click **Choose File** to navigate to a CSV file saved on your computer, or type the MAC address of the device in the **MAC Address** field. You can enter a name for any selected sensor in the **Name** field. If you do not give the sensor a name, its MAC address is used as the name.

   NOTE: The CSV format for each sensor should be *`MAC address, optional name`*.

2. Select **Add another** to add more than one sensor, or click Remove 🗑 to remove a sensor from the list. You can enter the name or MAC address of a specific sensor in the **Search** field to highlight it.
3. Click **ADD** to add all listed sensors to the wireless sensor network, or click **CANCEL** to close the window.

Update the Wireless Sensor Network

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

1. Select **UPDATE**, then click **YES**. The target firmware is loaded to your wireless devices, but not implemented.
2. When the update has completed, click **APPLY**. This instructs your wireless devices to implement the new firmware.

Remove a Wireless Sensor

NOTE: When a sensor is removed, history and alarms for that sensor are deleted.

1. Select the sensor. In the details window, click Decommission 🔗, then click **APPLY**.
2. In the **Confirm** window, click **YES**.
3. Select the sensor again, then click Remove 🗑.

Settings Tab

You can use the **Settings** tab to view and edit settings for notifications, alarm configurations, system preferences, user accounts, firmware updates, backup processes, and general information about your appliance.

Configure Notification Policies

Path: Settings > Notification

Configure notifications to be sent when alarms are generated. Notifications can be sent via email and Simple Mail Transfer Protocol (SMTP), or via Simple Network Management Protocol (SNMP) traps. You can create new email notification policies or edit existing policies. To configure notifications by SNMP trap, you must edit the **Default Trap Policy**.

> **NOTE:** You must configure an SMTP server for email notifications to work. (See *Configure an SMTP Server, page 36* for details.) You must configure a remote trap receiver for trap notifications to work. (See *Configure SNMP Settings, page 37*.)

Click **ADD** to create a notification policy, or select **Edit** ✏ to change an existing policy. Then configure the notification policy settings.

Setting	Description
Name	This will appear under **Name** in the **Notification** page and in the header of a notification email.
Send to email addresses	Enter e-mail addresses for anyone who will receive the notification. To send emails to multiple recipients, separate the email addresses with commas or enter a distribution list.
Notify for severities	Select alarm severities that will cause the notification to be generated.
Units	Select the system used to show measurements in the notification: **Metric** or **Imperial**.
Time format	Select the system used to show time in the notification: **12 hour** or **24 hour**.

Click **OK** to save your policy, or **CANCEL** to discard it.

Configure Alarms

Path: Settings > Alarm Configuration

The appliance comes with default alarms pre-configured for its internal sensors (outlet, switched outlet, and current input). The appliance also creates default alarms when new sensors are connected. For example, if you connect a temperature sensor to the appliance, three **Default Temperature** alarms (**High**, **Low**, and **Too High**) are automatically created for that sensor.

When you connect additional sensors to the appliance, the appliance automatically applies the appropriate default alarms to those sensors. For example, if you connect three more temperature sensors to the appliance, the default temperature alarms are automatically applied to all three sensors. Unless you change these settings, any temperature sensor can set off any temperature alarm.

Sensor type	Name	Operation	Value	Severity	Description
Beacon	**Default Beacon**	Equals	Active	Informational	If the beacon is activated, generate an informational alarm.
Motion	**Default Motion**	Equals	Motion Detected	Informational	If motion is detected, generate an informational alarm.
Leak rope	**Default Leakrope**	Equals	Leak Detected	Informational	If a leak is detected, generate an informational alarm.
Smoke	**Default Smoke**	Less than	Smoke Detected	Informational	If smoke is detected, generate an informational alarm.
Battery	**Default Battery (Too Low)**	Less than	2.4 V	Critical	If the battery voltage falls below 2.4 V, generate a critical alarm named “Too Low.”
	Default Battery (Low)	Less than	2.65 V	Warning	If the battery voltage falls below 2.65 V, generate a warning alarm named “Low.”
Temperature	**Default Temperature (Low)**	Less than	18°C (64.4°F)	Warning	If the temperature falls below 18°C (64.4°F), generate a warning alarm named “Low.”
	Default Temperature (High)	Greater than	27°C (80.6°F)	Warning	If the temperature rises above 27°C (80.6°F), generate a warning alarm named “High.”
	Default Temperature (Too high)	Greater than	32°C (89.6°F)	Critical	If the temperature rises above 32°C (89.6°F), generate a warning alarm named “Too High.”
Relative Humidity (RH)	**Default Humidity (High)**	Greater than	80% RH	Warning	If the humidity rises above 80%, generate a warning alarm named “High.”
	Default Humidity (Low)	Less than	20% RH	Warning	If the humidity falls below 20%, generate a warning alarm named “Low.”
State Door Contact	**Default State** **Default Door** **Default Contact**	Equals	Open	Info	If a State, Door, or Contact sensor is switched to **Open**, generate an informational alarm.
Vibration	**Default Vibration**	Equals	Vibration Detected	Info	If vibration is detected, generate an informational alarm.
Spot leak	**Default Spot Leak**	Equals	Leak Detected	Info	If a leak is detected, generate an informational alarm.
Putlet Relay output Switched Outlet Switch	**Default Outlet** **Default Output** **Relay Default** **Switched Outlet** **Default Switch**	Equals	Relay Active	Info	If the status of an Outlet, Relay output, Switched outlet, or Switch is set to **Active**, generate an informational alarm.
External relay	**Default External Relay**	Equals	Relay On	Info	If the status of an external relay is set to **On**, generate an informational alarm.
Airflow	**Default Airflow (Low)**	Less than	8 ft/sec	Warning	If airflow falls below eight (8) feet per second, generate a warning alarm named “Low.”

You can use the **Alarm Configuration** page to edit the default alarms, create new alarms, or delete alarms. If you create new alarms, you must add sensors to the new alarms manually. Select **Edit** ✎ to change an existing alarm configuration, or click **ADD** and select the sensor type to create a new alarm. Then configure the alarm settings.

Setting	Description
Name	The name of the alarm. This appears on the alarm configuration page, the **Alarms** tab, and the relevant sensor details window when the alarm is generated.
Operation	**Greater than:** If the device returns a value greater than the **Value** field, the alarm is generated. **Less than:** If the device returns a value less than the **Value** field, the alarm is generated. **Equals:** If the device returns a value equal to the **Value** field, the alarm is generated.
Value	The alarm is based on this value. Available values depend on the selected type of device. **0V-5V:** Enter a value in Volts (V). **4mA-20mA:** Enter a value in milliamperes (mA). **Air Flow:** Enter a value in feet per second (ft/sec). **Air Flow (speed):** Enter a value in feet per minute (ft/min). **Beacon:** Select **Active** or **Inactive**. **Humidity:** Enter a percent value. **Motion:** Select **No Motion** or **Motion Detected**. **Output Relay:** Select **Active** or **Inactive**. **RSSI:** Enter a value in decibels (dB). **State:** Select **Open** or **Closed**. **Switched Outlet:** Select **Active** or **Inactive**. **Temperature:** Enter a value in degrees Fahrenheit or Celsius. The temperature scale is determined in your user settings (see *View and Edit User Accounts, page 40*.
Severity	Select the severity of the alarm: **Critical**, **Warning**, or **Informational**. You can also use the severity to configure notification policies. See *Configure Notification Policies, page 29* for more information.
Sensors	Select any sensors that can cause the alarm to be generated.
Clip Capture	This feature is optional. Select a camera to capture video when the alarm is generated. The captured video will appear in the details window for any device that causes an alarm. See *Configure Video Capture Settings, page 40* to set the duration and resolution of video captures for alarms.
Control	This feature is optional. Determine how other connected devices are affected by the alarm. Under **Name**, select devices the alarm will control. Under **On alarm active** and **On alarm clear**, select what will happen when the alarm activates and is cleared (respectively). For example, if you select **Beacon at appliance**, the beacon attached to your appliance will be controlled by the alarm. If you select **On** under **On alarm active** and select **Off** under **On alarm clear**, the beacon turns on when the alarm is generated and turns off when the alarm is cleared.
Schedule	This feature is optional in firmware v5.1.0 and above. Select **Schedule** , then select times during which the alarm can be generated. The alarm can not be generated during times that are not selected.

Click **OK** to save the alarm configuration, or **CANCEL** to discard it.

To delete an alarm, select 🗑 Delete.

Configure System Settings

Use this page to view and set preferences for any of the following:

- **Date and Time**
- **IP Filter** (restricted access — only available in firmware v5.0.1)
- **Identification**
- **Logging** (event log)
- **Network**
- **Proxy Settings**
- **Rack Access** (global auto lock timeout — available in firmware v5.1.0 and above)
- **SMTP Server**
- **SNMP**
- **SSL Certificate** (for inbound connections)
- **Trust Store** (certificates for outbound connections)
- **User Store** (LDAP settings for Rack Access — available in firmware v5.1.0 and above)
- **Video Capture**
- **Web server** (only available in firmware v5.0.1)
- **Wireless** (wireless update settings)

Configure Date and Time Settings

Path: Settings > System > Date and Time

NTP: Synchronize the time of the Web UI to the time of the specified Network Time Protocol (NTP) server. The default time is Coordinated Universal Time (UTC).

Setting	Description
Primary Server	Type the hostname or IP address of the NTP server.
Secondary Server	Optional: Type the hostname or IP address of a second NTP server. If the Primary Server fails, the appliance will synchronize with this server.
Tertiary Server	Optional: Type the hostname or IP address of a third NTP server. If the Secondary server fails, the appliance will synchronize with this server.
Timezone	Select your time zone from the drop-down list.

Manual: Configure the date and time yourself. Select the **Date**, **Time**, and your **Timezone** from the drop-down lists.

Click **APPLY** to save your changes or **RESET** to discard your changes.

Restrict Access to the Appliance

Path: Settings > System > IP Filter

NOTE: This feature is only available in firmware v5.0.1.

By default, users can access your appliance from any IP address. Use the IP Filter to create a white list so that users can only connect to the appliance from specified IP addresses or IP address ranges. This helps to increases security.

To create an IP Filter,

1. Select **Enable IP Filters**. Once the IP filter is enabled, only IP addresses or address ranges in the **White List** can connect to your appliance.
2. Click **ADD** to create a new entry, and enter the following information. You can use the arrow buttons to change the order of your white list entries.

IP address Enter an IP address to give it access to the appliance. If desired, use **Mask** to define a range of IP addresses.

Port The port the IP address will connect to. Enter a port number between 1 and 65536. The following ports are reserved for various protocols:

- 22 (SSH)
- 68 (DHCP)
- 80 (HTTP)

The default ports for SNMP and HTTPS are 161 and 443, respectively. Both defaults can be reconfigured.

Mask Use a subnet mask to define a range of IP addresses. Define a number of bits that must match the entered IP address. The remaining bits at the end of the address can be any number.

For example, if you enter 192.168.2.81 in the **IP address** field and 30 in the **Mask** field, every address that matches the first 30 bits of the IP address will be added to the filter. In binary, 192.168.2.81 is

11000000.10101000.00000010.01010**0**01 (the 30th bit is bolded and underlined)

so the IP address 11000000.10101000.00000010.01010**0**10 (192.168.2.82) would be included in the filter because the first 30 bits of this IP address match the first 30 bits of 192.168.2.81.

11000000.10101000.00000010.01010**1**00 (192.168.2.84) would not be included in the filter because the first 30 bits of this IP address do not match the first 30 bits of 192.168.2.81.

Protocol Specify which protocol can be used to access the appliance from this IP address:

- **TCP:** used for reliable information transfer between applications.
- **UDP:** alternative to TCP used for faster, lower bandwidth information transfer. Though it has fewer delays, UDP is less reliable than TCP.
- **Both:** users can use TCP or UDP to access the appliance from this IP address.

NOTE: Be sure to include your own IP address in the white list. If you exclude yourself from the white list and are unable to connect to the appliance, see *Establish Network Settings, page 10*.

3. Click **APPLY** to save your changes, **RESET** to discard your changes, or Delete 🗑 to delete the white list entry.

Set Identification Information

Path: Settings > System > Identification

Storing identification information for the owner of the appliance allows anyone using the appliance to contact that person in case of an emergency. This information is also used by SNMP MIB–2.

Information	Description
Name	Type the name of the appliance owner. (This is called sysName in SNMP MIB–2).
Location	Type the physical location of the appliance. (This is called sysLocation in SNMP MIB–2).
Contact	Enter contact information (for example, an e-mail address) for the appliance owner. (This is called sysContact in SNMP MIB–2.)

Click **APPLY** to save your changes or **RESET** to discard them.

Configure Log Settings

Path: Settings > System > Logging

Firmware v5.1.0 and above

You can configure a remote Syslog server to store log files for events such as rack access events and camera discoveries. (These are separate from the events in the **Logs** Quick Link at the top right of the Web UI.) Once the server is configured, log files are automatically copied to the Syslog server.

Setting	Description
Enable	Enable remote logging.
Server	Enter the host name or IP address of the Syslog server.
Port	Enter the port number used to communicate with your Syslog server.

Firmware v5.0.1

The **Level** drop-down list shows all possible logging event levels in order from highest to lowest urgency. Select the lowest event level to appear in the appliance log. Event levels lower than the selected level will not be recorded. You can view the log by clicking the **Logs** Quick Link at the top right of the Web UI. For more information, see *Quick Links, page 14*.

Configure Network Settings

Path: Settings > System > Network

View and configure network settings.

Setting	Description
Static	Select **Static** to manually configure your Network settings. This setting assigns a static IP address to the appliance.
DHCP	Use a DHCP server to configure network settings automatically. This setting assigns a dynamic IP address to the appliance.
Hostname	The host name of the appliance.
TCP/IP	
IP Address	The IP address of the appliance. Use the format xxx.xxx.xxx.xxx.
Subnet Mask	The subnet mask of the appliance.
Gateway	The IP address of the default gateway.
DNS	
Primary	The IP address of the primary DNS server
Secondary	The IP address of the secondary DNS server
Tertiary	The IP address of the tertiary DNS server

Click **APPLY** to save your changes or **RESET** to discard them.

> **NOTE:** If the network settings are incorrect, you can not reach the appliance through the Web UI. See *Use a Terminal Emulator to Establish Network Settings, page 10* for instructions to change your network settings without access to the Web UI.

Configure a Proxy Server

Path: Settings > System > Proxy Settings

When proxy settings are configured, the appliance uses an HTTP or HTTPS proxy server for all e-mail and HTTP/HTTPS communications, allowing these communications to cross the firewall. When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate. These settings apply only to communications from the appliance.

To enable a proxy server, enter the HTTP or HTTPS Proxy Settings.

Setting	Description
Server	The host name or IP address of the proxy server the appliance uses for e-mail, HTTP Posts, and other outbound communications.
Port	The IP port number to connect to the proxy server.
Username	Enter a user name to allow access through the server.
Password/Confirm Password	Enter a password to allow access through the server.

Click **APPLY** to save your changes, or **RESET** to discard them.

Set Global Auto Lock Timeout

Path: Settings > System > Rack Access

Enter a value in the **Global Door Auto Lock Timeout** field to determine the number of minutes before any unlocked handle re-locks. This only applies to closed handles on closed doors — open handles and open doors will not re-lock, but they will generate alarms when the timer ends.

This setting applies to all doors with Rack Access control. You can also set **Auto Lock Timeouts** for individual doors. See *Schedule Rack Access, page 24* for details.

Configure an SMTP Server

Path: Settings > System > SMTP Server

You must configure an SMTP server before you can configure e-mail notifications.

Setting	Description
SMTP server address	The hostname or IP address of the SMTP server.
Port	The IP port number to connect to the SMTP server (firmware v5.0.1 only).
Use SSL	This optional feature allows you to use Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol to encrypt email notifications. For most port numbers, selecting this option enables STARTTLS. STARTTLS encrypts e-mail content only if your SMTP server supports encryption. In firmware v5.1.0, if you select **Use SSL** and the port number is 465 or 587, SSL/TLS encryption is required. If the SMTP server does not support encryption, the appliance can not connect to the server.
From address	The e-mail address that will appear in the From field for emails generated by the appliance.
Username	User names are optional. If desired, create a user name to allow access through the server.
Password/Confirm Password	Passwords are optional. If desired, create a password to allow access through the server.
Send test email	Select to send an email and confirm the settings are correct.

Click **APPLY** to save your changes, or **RESET** to discard them.

Configure SNMP Settings

Path: Settings > System > SNMP

View or edit the following settings for your SNMP agent or Remote trap receiver. You must configure a Remote trap receiver for the appliance to send out SNMP traps.

Setting	Description	
SNMP agent		
Enable	Select to enable the SNMP agent on your appliance.	
Port	The port number for SNMP communications.	
SNMPv1/ SNMPv3	Select the SNMP version for the agent to use.	
Read-only community name	The read-only community name for SNMP requests. SNMPv1 only.	
Authentication/ Encryption	SNMPv3 only. Select whether to use **No security**, **Authentication only**, or both **Authentication** and **Encryption**.	
Username	Enter the user name to access the SNMP agent.	
Protocol	Authentication protocols: • **SHA1:** Slower, but more secure than MD5 • **MD5:** Faster, but less secure than SHA1	Encryption Protocols: • **AES-128:** More secure than DES. Uses a 128-bit key to encrypt data. • **DES:** Less secure than AES. Uses a 56-bit key.
Password/ Confirm Password	Enter the password to access the SNMP agent.	
Remote trap reciever		
Enable	Select to enable SNMP traps.	
SNMP trap reciever	The IP address or host name of the trap receiver.	
Port	The port number of the remote SNMP trap receiver.	
SNMPv1/ SNMPv3	Specify the trap type by selecting either SNMPv1 or SNMPv3.	
Read-only community	The read-only community name for SNMP trap requests. SNMPv1 only.	
Send test trap	Select to send a test trap to a configured trap recipient.	
Authentication/ Encryption	SNMPv3 only. Select whether to use **No security**, **Authentication only**, or both **Authentication** and **Encryption**.	
Username	Enter the user name to access the remote trap receiver.	
Protocol	Authentication protocols: • **SHA1:** Slower, but more secure than MD5 • **MD5:** Faster, but less secure than SHA1	Encryption Protocols: • **AES-128:** More secure than DES. Uses a 128-bit key to encrypt data. • **DES:** Less secure than AES. Uses a 56-bit key.
Password/ Confirm Password	Enter the password to access the remote trap receiver.	

Click **APPLY** to save your changes, or **RESET** to discard them.

Configure Certificates for Inbound Connections

Path: Settings > System > SSL Certificate

View and install an SSL certificate to support inbound connections. It is not possible to have more than one certificate installed. As soon as you install a new certificate, the existing certificate will be deleted.

You can generate and install a self-signed certificate or install an X.509 certificate:

Self-signed certificates: The NetBotz appliance ships with a RSA 2048 bit selfsigned certificate. If you change the host name of your appliance, the certificate is automatically updated. Self-signed certificates expire after five years. You can regenerate the certificate at any time (see Generate a Self-signed Certificate on this page). The new certificate will expire five years from the date it is generated.

X.509 Certificates: You can replace the self-signed certificate with an X.509 certificate signed by a third party Certificate Authority (CA). The X.509 certificate must match the hostname of your appliance. If your X.509 certificate or key is provided in binary, you must convert it to Privacy Enhanced Mail (PEM) format.

Generate a Self-signed Certificate

Click **GENERATE SELF-SIGNED** and enter the correct information in the following fields:

Field	Description
Common Name (CN)	The hostname for your appliance. This should match the **Hostname** in your network settings (under **Settings > System > Network**). If you change the **Hostname** in your network settings, the certificate will be regenerated automatically. If you change the hostname outside of the appliance's Web UI, a new certificate will be generated with the updated hostname the next time the appliance restarts.
Organization (O)	Your organization.
Organizational Unit (OU)	Your organizational unit.
Locality (L)	The city or town where you, your organizational unit, or the appliance is located.
State or Province (ST)	The state or province where you, your organizational unit, or the appliance is located.
Country (C)	The country where you, your organizational unit, or the appliance is located.
Emai address	Your email address or the email address of the appliance owner.

Click **INSTALL** to generate and install the certificate, or **CANCEL** to exit the **Generate self-signed** window.

Install an X.509 Certificate

Click **INSTALL CERTIFICATE.** Copy and paste your certificate and private key into the appropriate fields. Certificates begin with a header line and end with a footer line. For example:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

The header line, the footer line, and all of the certificate content must be included.

Click **INSTALL** to install the certificate, or **CANCEL** to exit the Install certificate window. After the certificate is installed, the application restarts.

Configure Certificates for Outbound Connections

Path: Settings > System > Trust Store

This page allows you to configure and manage PEM security certificates for outbound connections. You can install any number of certificates in the trust store.

To add a certificate, click **ADD** to open the **Add certificate** window, then copy and paste the certificate into the window. Click **ADD** to save the certificate, or **CANCEL** to discard it.

To view the details for any certificate, click **View**.

To delete a certificate, click Delete 🗑.

Configure LDAP Settings for Rack Access

Path: Settings > System > User Store

NOTE: This feature is available in firmware v5.1.0 and above.

You can use this page to connect to your company's authentication server and verify the existence of specific users.

Select **Enable** to connect to a server, then configure the **Server Settings** and **LDAP Schema**.

Setting	Description
Server Settings	
Hostname	Enter the host name of your company's authentication server.
Port	Enter the IP port number to connect to your company's authentication server.
Use SSL	Select to enable Transport Layer Security. If this setting is enabled and you have a trust store certificate for the LDAP server, the **Hostname** entered on this page is verified against the host name in the trust store certificate. The **Hostname** on this page must match the host name on the certificate
Username	Enter the user name to log into your company's authentication server.
Password	Enter the password to log into your company's authentication server.
Test Server Configuration	Click to test validity of server configuration.
LDAP Schema	
Base DN	Enter the base distinguished name of your company's LDAP directory. You can copy this directly from your LDAP directory. The more specific your filepath is, the shorter the search will be.
Username Attribute	Enter the attribute your company uses to authenticate users. For Active Directory servers, this is typically the Sam account name. For most other LDAP servers, this is the UID (User ID).
Test User Schema	Search for an existing user to ensure your schema is configured properly. Select **Test User Schema**, enter the **Username** and **Password** for an existing user on your company's LDAP server, then click **TEST**.

NOTE: LDAP users can not be created on the appliance. Create users and add user attributes on your company's LDAP server.

Configure Video Capture Settings

Path: Settings > System > Video Capture

You can configure cameras to record video when alarms are generated (see *Configure Alarms, page 30* for details). Use video capture settings to determine how much video is recorded for alarms with Clip Capture enabled.

Setting	Description
Pre-alarm capture time	The total number of seconds prior to an alarm that images are recorded and saved.
Post-alarm capture time	The total number of seconds after an alarm that images are recorded and saved.

Click **APPLY** to save your changes, or **RESET** to discard them.

Set the Web Server Port

Path: Settings > System > Web Server

NOTE: This feature is only available in firmware v5.0.1.

View or change the HTTP or HTTPS port through which the appliance Web server communicates. Enter the port number and click **APPLY** to save your changes, or **RESET** to discard them.

Set Wireless Update Settings

Path: Settings > System > Wireless

Some wireless devices such as the NetBotz USB Coordinator and Router (NBWC100U) have firmware that is updated separately from the NetBotz appliance. Select **Automatic** to update wireless devices automatically when new firmware is installed, or select **Manual** to update wireless devices at your convenience. Click **APPLY** to save your changes, or **RESET** to discard them.

NOTE: You can see the current and target firmware versions for wireless devices in the **Wireless** tab (see *Wireless Tab, page 25*).

View and Edit User Accounts

Path: Settings > Users

Click **ADD** to add a new user, or click Edit ✏ to change an existing user account, then configure the user settings.

Setting	Description
User name	Enter the user name.
Password*	Enter the password for the user to log on to the appliance.
Units	Select **Metric** or **Imperial** units of measurement.
Time format	Select the **12 hour** or **24 hour** time format.

*To change the password for an existing user, the Super User can click **Change password** on the main page.

Click **OK** to save your changes, or **CANCEL** to discard them. The Super User can also click 🗑 Delete to delete a user account.

Update the Appliance Firmware

Path: Settings > Firmware Update

It is recommended that you keep firmware versions current and consistent across your network to allow for implementation of the latest features, performance improvements, and bug fixes. Regular updates also ensure that all units support the same features in the same manner.

Update from Firmware v5.0.1

NOTE: This procedure causes the appliance IP address to be reset. In some cases, you may lose access to the appliance and may need to use a local connection to reset or rediscover the IP address.

1. Download the latest firmware version for free from the APC by Schneider Electric website, *www.apc.com*.
2. Click **Choose File**, navigate to the firmware file on your computer, and select **Open**. Do not close the page while the file is uploading, or the upload will be aborted. (You can work in a different tab or a different browser window.)
3. Click **INSTALL** to install the firmware, or **Start Again** to select a different firmware version. Users can not access the Web UI while the firmware is updating.
4. After updating, the appliance automatically restarts. If the appliance takes longer than six minutes to become available, clear your Web browser cache and refresh the page.
5. Enter `<`*`your appliance's IP address`*`>/rest/settings/appliance/recondition` in the URL address bar.

   Example: `10.218.117.147/rest/settings/appliance/recondition`

   The appliance restarts. The appliance may take about six minutes to restart completely. Until the restart is complete, the Web UI is not available.
6. If needed, use a terminal emulator to view or reset the IP address of the appliance. See *Use a Terminal Emulator to Establish Network Settings, page 10* for instructions.
7. Log on to the appliance using the Super User user name and password (both are **superuser**). You will be required to set the Super User password.

Update from Firmware v5.1.0

1. Download the latest firmware version for free from the APC by Schneider Electric website, *www.apc.com*.
2. Click **Choose File**, navigate to the firmware file on your computer, and select **Open**. Do not close the page while the file is uploading, or the upload will be aborted. (You can work in a different tab or a different browser window.)
3. Click **INSTALL** to install the firmware, or **Start Again** to select a different firmware version. Users can not access the Web UI while the firmware is updating. The appliance restarts when the upload is finished. This process can take about 20 minutes.

Backup and Restore System Settings

Path: Settings > Backup

On this page, you can save the current system settings to a backup file, use a backup file to restore previous system settings, or use a backup file to configure multiple appliances.

When you restore system settings from a backup file, always use a backup file saved from the same firmware version as the current system. If a firmware update is available, restore the system and re-configure the network settings before you update the firmware. Save a backup file immediately after you update the firmware.

> **NOTE:** Backup files do not store network settings and can not be used to configure network settings.

Save a Backup File

The backup file includes all of the configuration settings for your appliance, including user account settings, sensor configurations, and alarm configurations. You can use the backup file to restore this configuration to your appliance at a later date or to configure a new appliance.

To save a backup file,

1. Ensure your system settings are configured as needed.
2. Under **Backup to file**, select ⤓ Download.

> **NOTE:** The file may take several seconds to begin downloading.

A backup file is saved to your computer.

> **NOTE:** The backup file is not encrypted. Save the backup file in a secure location. Consider encrypting the backup file with a tool such as the GNU Privacy Guard (on gnupg.org) and verifying the file before performing a restore.

Restore System Settings

Use a backup file to restore a previous system configuration.

To restore system settings,

1. Select **Restore an existing backup to this device**.
2. Click **Choose File** and navigate to the backup file of your choice.
3. Click **Restore**.

The appliance settings are updated according to the backup file.

Configure New Appliances from a Backup File

Use the settings from one appliance to configure other appliances.

To configure new appliances,

1. Download a backup file from a configured appliance to your computer.
2. On an un-configured appliance, go to the **Settings** tab, select **Backup**, then select **Clone a backup on to new device**.
3. Click **Choose File**, and navigate to the backup file from the configured appliance.
4. Click **CLONE** to configure the appliance, or **CANCEL** to stop the operation.

The appliance settings are updated according to the backup file.

View Appliance Information

Path: Settings > About

On this page, you can view the **Model**, firmware **Version**, **IP Address**, and **Serial Number** of the appliance. Customer support can use this information to help troubleshoot problems with your appliance.

Troubleshooting

Access Issues

Probelm	Solution
Cannot access the appliance through a terminal emulator	• Make sure the serial port is not in use by another application. • Make sure that the terminal settings are configured correctly: 115,200 baud, 8 data bits, no parity, 1 stop bit, and no flow control.
Cannot access the Web UI	• At startup, the Web UI can take about six minutes to become accessible. Wait for six minutes, then try to log in again. • Verify that HTTP or HTTPS access is enabled. Check your browser's proxy settings. • Make sure the URL is consistent with the security system used by the appliance. SSL requires https, not http, at the beginning of the URL. • Verify that you can ping the appliance. • Verify that you are using a supported Web browser. If available, try a different web browser. See *Access the Web User Interface (Web UI), page 11*. • If the appliance has just restarted and SSL security is being set up, the appliance may be generating a server certificate. The appliance may take several minutes to create this certificate, and the SSL server is not available during that time.

APC by Schneider Electric
132 Fairgrounds Rd
02892 West Kingston, RI
USA

www.apc.com

As standards, specifications, and design change from time to time, please ask for confirmation of the information given in this publication.