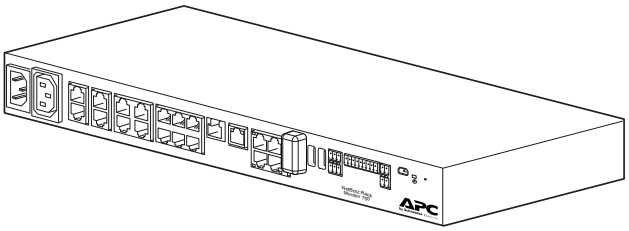
NetBotz 5.x

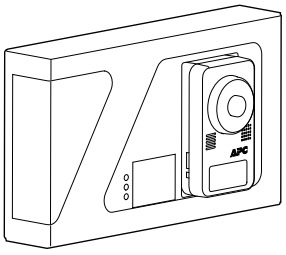
User Guide

NBRK0750
NBWL0755

Release date: 08/2025

990-5934K





www.apc.com

Legal Information

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

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

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

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

APC, the APC logo, NetBotz, EcoStruxure, and Data Center Expert are trademarks owned by Schneider Electric SE. All other brands may be trademarks of their respective owners.

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

NOTICE
The equipment contains, and the software enables, visual 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 insuring 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

NOTE: A REST API client uses RESTful design practices to deliver data between two programs. RESTful practices are designed to take advantage of existing protocols and to be flexible across multiple platforms.

The APC NetBotz™ Rack Monitor 750 (NBRK0750) and Room Monitor 755 (NBWL0755) are central hardware appliances 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) or Representational State Transfer Application Programming Interface (REST API). This manual describes how to use these to configure settings on your appliance, and how to use your appliance to monitor the environment and attached sensors and devices. (See your appliance's *Installation and Quick Configuration Manual* on www.apc.com for information on supported devices.)

Your NetBotz appliance 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.

Updates and Additional Documentation

You can find updates to this document, firmware updates, and these additional documents on the applicable product page of www.apc.com:

- *Installation and Quick Configuration Manual:* Provides instructions to install the appliance and initial setup of TCP/IP
- *Release Notes:* Provides lists of new features, fixed issues, and known issues for the latest firmware version.
- *Security Handbook:* Describes security features and options for the appliance.

To quickly find a product page, enter the part number of your product in the Search field on www.apc.com.

Security Recommendations

NetBotz appliances are not designed 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 help 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., using a terminal emulator to specify network settings. You are required to change the default password the first time you log on. You cannot change the default user name (**root**). The Root account is not used for most functions and should be shared with as few people as possible — ideally, only one person would have access to the Root account.

Password Requirements

Use strong passwords that comply with your company's password requirements.

Starting in NetBotz 5.4.1 and newer:

- Passwords must contain a minimum of 12 characters including:
  - At least 1 uppercase character
  - At least 1 lower case character
  - At least 1 digit
  - At least 1 special character (!@#$%^&+=?)
- When changing the current password, the previous password cannot be reused.

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 (see Establish Network Settings, page 8).
3. Access the Web UI of the appliance (see Access the Web User Interface (Web UI), page 11).

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

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.

You can use a computer to view the DHCP settings or configure the network settings manually. If needed, you can also view or configure network settings with a terminal emulator.

Use Your Computer to Establish Network Settings

1. Use the Public LAN port to connect your appliance to the network.
2. Ensure your computer is set to obtain network settings via DHCP. Connect a network cable from your computer to a Private LAN port on the appliance. Wait about 5 minutes for the computer to establish a working Ethernet connection through the appliance.

   NOTE: Some computers are configured to prevent simultaneous connections to Ethernet and Wi-Fi, so you may need to disable Wi-Fi before connecting to the appliance.
3. For Windows® or Linux® systems, open a command prompt to view the default gateway, then enter the default gateway in your Web browser's URL address bar. The following commands allow you to view the default gateway:

   - Windows: `ipconfig`
   - Linux: `route -n`

   For Macintosh® systems, open the network preferences for your Ethernet connection. Enter the **Router** address in your Web browser's URL address bar. The default gateway or router address takes you to the appliance Web UI.

   NOTE: You may receive a message that the Web page is not secure. This is normal, and you can continue to the Web UI. See Access the Web User Interface (Web UI), page 11 for more information.
4. Use the default user name and password (both are **superuser**) to log on to the appliance, and change the password when prompted. It is recommended that you use a strong password that complies with your company's password requirements.
5. Go to **Settings > System > Network** to view or configure the network settings for your appliance.

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.
6. Test the IP connection of the appliance: Close the Web UI and disconnect your computer from 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.

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. Apply power to your appliance.

   The green Power LED illuminates. The appliance can take up to 2 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.

   NOTE: The Web UI takes about 6 minutes to become available after start up.

   NOTE: You may receive a message that the Web page is not secure. This is normal, and you can continue to the Web UI. See Access the Web User Interface (Web UI), page 11 for more information.

Access the Web User Interface (Web UI)

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 or the latest version of Microsoft Edge®, Google Chrome®, or Mozilla Firefox® 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.

NOTE: The Web UI takes about 6 minutes to become available after start-up.

NOTE: Camera streaming is not supported in IE 11.

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 your computer or a terminal emulator to view your current IP address. Follow steps 1-4 of Use Your Computer to Establish Network Settings, page 9 or 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 a self-signed certificate (the default), and you can continue to the Web UI.

   NOTE: 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 stop the warning message appearing by installing a certificate signed by a Certificate Authority (CA) the Web browser recognizes You can also direct the browser to accept the certificate to stop the warning message appearing.

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**. 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. 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.
2. Disconnect and reconnect power to the appliance. Immediately press any key on your computer. If you do not press a key within 5 seconds of connecting power to the appliance, the appliance will restart normally.
   You will see the following prompt: `SNARC_SOCA9_BESTLA_2G #`.
3. Enter the following commands:

   `setenv resetpwd true`
   `saveenv`
   `printenv resetpwd` (You should receive a `resetpwd=true` response.)
   `boot`

   Wait for the system to restart.
4. Log on as the Root user. When prompted, reset the Root account password. If you are not prompted to reset the password, wait 10 seconds, then press **Enter** to log in again.
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 of connecting power to the appliance, the appliance will restart normally.
6. Enter the following commands:

   `setenv resetpwd`
   `printenv resetpwd` (You should receive a `## Error: "resetpwd" not defined` response.)
   `saveenv`
   `boot`

   Wait for the system to restart. Log on as the Root user.

   NOTE: If you do not complete steps 5 and 6, you will be required to reset the Root password every time you access the console after 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 application 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. 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, then press **Enter**.

   Example: `93.184.216.34/rest/appliance/resetconfig`

   The appliance takes about 6 minutes to restart completely. Until the restart is complete, the Web UI is not available.
3. If needed, see Use Your Computer to Establish Network Settings, page 9 or Use a Terminal Emulator to Establish Network Settings, page 10 for instructions to discover or change the IP address.

The next time you log on to the Web UI, you must reset the Super User password. The next time you log onto the console, you must set the Root account password (see steps 1–5 of Use a Terminal Emulator to Establish Network Settings, page 10). It is recommended that you reset both passwords immediately to increase the security of your system.

Network Management with Other Applications

You can also manage the appliance with the following applications:

- Data Center Expert® (DCE): Provides enterprise-level power management and management of agents, Rack PDUs, and environmental monitors. See Enable DCE Surveillance, page 37 for more information.
- EcoStruxure™ IT: Provides mobile monitoring and smart alarms for Rack PDUs, UPS units, and environmental monitors.

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.
- **Devices:** View detailed information for all downstream devices.
- **Rack Access:** View detailed information for rack access devices and register individual rack access users.
- **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.


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 21 or Configure Alarms, page 34.

Quick Links

Select your user name in the upper right corner to access these quick links:

- **Profile:** View or edit your profile settings.
- **Change Password:** Select this link to change your password.
- **User Guide:** Opens this *User Guide*.

  Resources: Opens a page where you can access helpful documentation including this User Guide, the MIB file, the NetBotz device definition file (DDF), Log files, the Modbus register map, and a table of Supported Devices which includes applicable Vendors, the Family–or category–of a device, the device Type, and the Protocol used to communicate with your NetBotz appliance.

  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.
- **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, or alarm status. See Configure Alarms, page 34 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. • Manually change the state of a state sensor, for example, set an Inactive switched outlet to Active.
Camera details	View a live feed from the camera, or edit camera settings. See Configure the Camera Pod Settings, page 19 for instructions to configure settings.
Outlet-controlled device details	Details windows for outlet-controlled devices show whether the device is **Active** or **Inactive**, and provide an option to change this setting manually.
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 34). If a connected device activates an alarm with this feature enabled, the video recording appears at the bottom of the details window for that device. Video capture is automatically deleted after 96 hours.

Overview Tab

NOTES: Video from Camera Pod 165 units does not appear in Microsoft Internet Explorer®.

You cannot see downstream devices other than cameras on the **Overview** tab. See Devices Tab, page 22 for more information on downstream devices.

You can select the name of any table to view information for that table and edit its title.

The **Overview** tab displays feedback from cameras, sensors, and other devices connected to the appliance. 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. (See Details Windows, page 15 for more information about viewing and editing sensor information.)

There are three default tables for the Rack Monitor 750:

- **Appliance:** This table includes two outputs, one switched outlet, and two current inputs. These correspond to your appliance's relay outputs, voltage output port, and sensor input ports, respectively.
- **Appliance Rack Access:**This empty table can be populated with rack access handles and door sensors on firmware v5.1.0 and higher.

There is one default table for the Room Monitor 755:

- **Appliance:** This table includes one temperature and humidity sensor and two outputs. These correspond to your appliance's internal temperature sensor and relay outputs respectively.

An additional **Rack Access** table appears if you connect a Rack Access Pod to the A-Link port.

IMPORTANT: You must plug an A-Link terminator into the unused A-Link port. See the*Installation Manual* on www.apc.com for more information.

Most devices 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.

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
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. The Super User can also change the states of state sensors manually.

Cascade Sensors and Pods from A-Link Ports

NOTICE

EQUIPMENT DAMAGE RISK

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

Failure to follow these instructions can result in equipment damage.

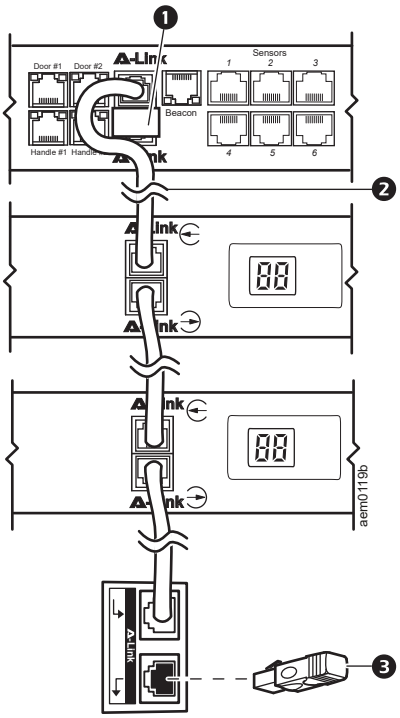
A-Link is an APC proprietary Controller Area Network (CAN) bus. Devices compatible with A-Link are not Ethernet devices and cannot coexist on an Ethernet bus with other networking devices, such as hubs and switches.

Before performing this procedure, follow the installation instructions provided with the devices you plan to cascade.

You can cascade any or all of the following:

A-Link Device	NetBotz Rack Monitor 750 (NBRK0750)	NetBotz Rack Monitor 755 (NBRK0755)
NetBotz Rack Sensor Pod (NBPD0150, NBPD0155)	Up to 4 with no supplemental power Up to 12 with one supplemental power supply (AP9505i) attached for every fourth pod	Up to 2
NetBotz Rack Access Pod (NBPD0171, NBPD0175)	Up to 12 with one supplemental power supply (AP9505i) attached for every fourth pod	1
Temperature/Humidity Sensor with Digital Display (AP9520TH)	Up to 8	Up to 8

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



1. Connect sensors and sensor pods to the in and out ports as shown.
   - The combined length of all A-Link cables (❷) must not exceed 1000 m (3,280 ft).
   - Use CAT-5 (or equivalent) Ethernet patch cables.
2. Plug the second A-Link terminator into the unused A-Link port ❸. (Terminator ❶ is pre-installed. Leave the pre-installed terminator in the appliance unless you want to use the port for a second chain of pods. Be sure to terminate both chains.)
3. Connect supplemental power supplies (AP9505i) to the 24-VDC Inputs on your devices as required.

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

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 34 for instructions.

Configure the Camera Pod Settings

NOTE: If a Camera Pod 165 has previously been connected remotely (or connected to another appliance), reset the camera while it is connected to the appliance. If the camera does not appear after 10 minutes, disconnect the camera, remove it from the Web UI, then re-connect it. 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 lease configuration).

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 mask the entire viewing pane, click **SELECT ALL**. To remove the motion masks, click **CLEAR ALL**. To remove part of a mask, click and drag your mouse while holding the **Alt** key. To undo the last action, click **Undo** .
Motion Detection 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.
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 Connect Downstream Devices, page 23 or Add a Remote Camera, page 24 to connect a Camera Pod 165.

NOTE: See Configure Alarms, page 34 for instructions to configure alarms that are generated by motion-detection settings.

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

NOTES:
When a camera is removed, related alarms and clip-captures from those alarms are deleted.

To add a remote camera, see Add a Remote Camera, page 24

Local cameras which are connected directly to the appliance say **Auto** next to the label. Remote cameras say **Manual** after the label.

To remove a local camera,

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

To remove a remote camera,

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

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.

Select an alarm to view whether the relevant device is connected, graphical information from the time the alarm was activated (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

NOTE: Video for cleared alarms is automatically deleted after 96 hours. If only 2 gigabytes (GB) of storage are left on the appliance, video capture will not be stored until enough video has been deleted to make more space available.

The **Clip Capture** feature records video when an alarm is activated. 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.

Video is recorded for a minimum of 2 seconds before an alarm is activated and 2 seconds after it is activated. To configure the pre-alarm and post-alarm capture times, see Configure Video Capture Settings, page 53.

To configure alarm settings or to enable **Clip Capture**, see Configure Alarms, page 34.

Pagination

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.

Devices Tab

NOTE: Downstream Camera Pod 165 units may be local (connected to a Private LAN port) or remote (connected through your network). See Connect Downstream Devices, page 23 to connect a local camera pod, or Add a Remote Camera, page 24 to connect a remote camera pod.

You can use the **Devices** tab to view downstream devices, which connect to the appliance's private network through the Private LAN ports.

The appliance can support up to ten downstream devices, including up to four cameras. Performance may vary depending on the amount of video recorded or the number of sensors attached to your downstream devices.

Item	Description
+ ADD CAMERA	Select to add a remote camera. See Add a Remote Camera, page 24.
Port Forwarding	Enable or disable Port Forwarding. Port forwarding allows you to open the Web UI of a downstream device by clicking in the details window. HTTP must be enabled on a device to view its Web UI. It is recommended that you keep Port Forwarding disabled when it is not in use.
Name	A user-editable label for the device.
Status	**Initializing:** The appliance is establishing communication with the device. **Connecting:** The appliance is finalizing communication with the device. **Communicating:** The appliance is communicating with the device. **Connection Failed:** Unable to reach the device. Ensure that the device is on and correctly configured. If you have made a remote connection to a Camera, ensure the IP address is correct. Ensure the **Device Credentials*** settings are correct. **Not Authorized:** The login credentials may be incorrect. Select the device, then select **FIX CREDENTIALS** to enter a different user name or password. Ensure the **Device Credentials*** settings are correct. If the device is a Camera Pod 165 that has previously been connected to a different host appliance, the credentials need to be reset. Press the Reset button on the Camera Pod 165 for 20 seconds (the Network LEDs will turn off). Then wait 5–10 minutes for the Camera Pod 165 to restart. *To change the **Device Credentials** settings, see Configure Discovery Settings for Downstream Devices, page 39.
Type	The type of connected device.

You can select a downstream device for additional options:

Option	Description
	Edit the device Name (or Label).
	Delete the disconnected device.
	View detailed information for the device. Video from Camera Pod 165 units does not appear in Microsoft Internet Explorer®.
	Opens the device's Web UI in a separate browser window. Port forwarding must be enabled to use this icon. HTTP must be enabled on a device to view its Web UI. The Web UI for the Camera Pod 165 is only used to update the Camera Pod firmware or change the password remotely. Editing other settings may disrupt normal camera functions.

Connect Downstream Devices

Compatible downstream devices include APC Rack Power Distribution Units (Rack PDUs) with Network Management Cards (NMC), Smart UPS (Uninterruptable Power Supply) units, or NetBotz Camera Pod 165 units. Other ONVIF cameras may work but have not been tested and are not guaranteed to include motion detection features.

To connect downstream devices, go to **Settings > System > Device Credentials**, and configure the following settings to match the settings on your device:

Setting	Description
Camera (ONVIF) **NOTE:** If you have not already set a password on a Camera Pod 165, you do not have to set the ONVIF credentials for that unit. The appliance will assign it a password.	
Username	The user name to access the camera..
Password/Confirm Password	The password to access the camera.
SNMPv1	
Read-only community name	The name used to access the Read-only community.
Read-Write community name	The name used to access the Read-write community.
SNMPv3 (More secure than SNMPv1.)	
Username	The identifier of the user profile.
Authentication/Encryption	Select whether to use **No security**, **Authentication only**, or both **Authentication** and **Encryption**.
Authentication	Verifies that the device communicating through SNMPv3 is the device claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time.
Protocol	**SHA1:** Most secure option. **MD5:** Less secure than SHA1.
Password/ Confirm Password	The password or passphrase used for authentication.
Encryption	Encrypts the data sent over SNMPv3.
Protocol	**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	The password or passphrase used for encryption.

Then connect the devices to your appliance through a Private LAN port. You can connect a network switch or hub to the Private LAN ports to connect up to ten downstream devices, including up to four cameras. Performance may vary depending on the amount of video recorded or the number of sensors attached to your downstream devices.

NOTE: The appliance counts disconnected devices as supported units. Use the icon to remove devices before replacing them with new ones.

If a Camera Pod 165 has previously been connected remotely (or connected to another appliance), reset the camera while it is connected to the appliance. If the camera does not appear after 10 minutes, disconnect the camera, remove it from the Web UI, then re-connect it. 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 lease configuration).

Once your devices are communicating with the appliance, you can change the **Device Credentials** to match a new set of devices without losing the established devices.

Add a Remote Camera

You will need an IP address, username, and password to connect remotely to a camera. Follow the instructions in your camera's documentation to discover its IP address and set a strong password that complies with your company's password requirements.

> **NOTE:** Your appliance automatically assigns a new password to camera pod 165 units with a local connection. If want to change your unit from a local connection to a remote connection, reset to defaults before setting the password. (See Discover Assigned Passwords and Access a Camera Pod Web UI, page 24 to discover the password provided by the appliance before you disconnect the camera.) Alternatively, follow the instructions in your camera documentation to change the password before making a remote connection to the appliance.

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

- **Hostname:** the host name or IP address of the camera
- **Username:** the user name to log on to the camera
- **Password/Confirm Password:** the password to log on to the camera

Update the Firmware or Change the Password on a Local Camera Pod 165

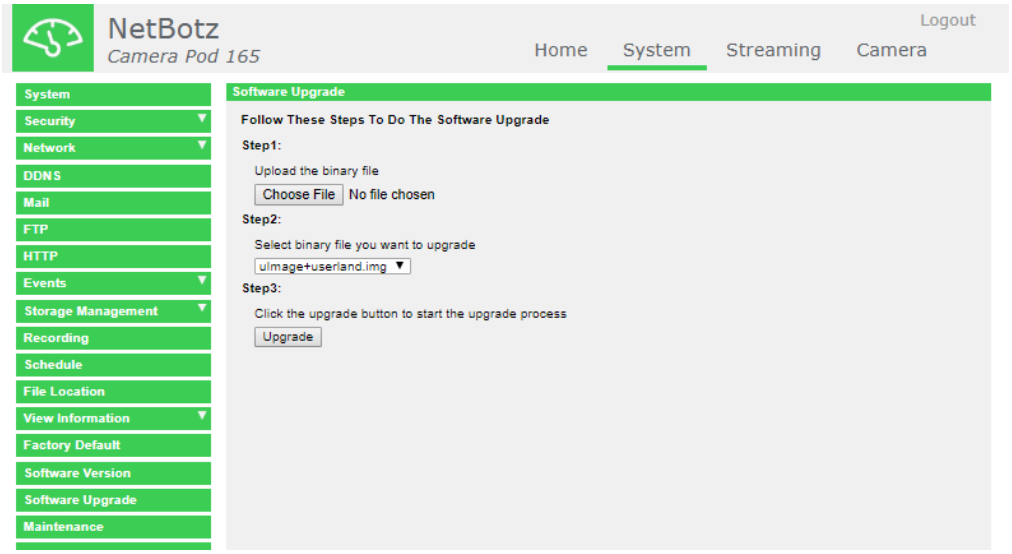
The Camera Pod 165 Web UI is used to update the firmware or change the password on a Camera Pod 165 unit. The appliance automatically assigns passwords to local, unconfigured Camera Pod 165 units (NBPD0165). To access a Camera Pod's Web UI, you must first use the appliance's REST API documentation to discover the assigned password.

Discover Assigned Passwords and Access a Camera Pod Web UI

The appliance automatically assigns passwords to local, unconfigured Camera Pod 165 units (NBPD0165). To discover this password:

1. Log on to the Web UI, then open the REST API documentation by entering `<appliance IP address>/docs/rest` in the URL address bar
2. Go to **assets > GET/assets** to discover the `id` of your camera pod. Enter `camera` in the **types** field, then select **Try it out!** If you have more than one camera, look for the label that matches the camera label in the Web UI. Copy the `id` (for example, `camera-22`).
3. Go to **cameras > GET/cameras/cameraPassword/{id}** to discover the camera password. Paste the `id` in the **id** parameter field, then select **Try it out!** The `property` is the password to access the camera.
4. On the **Devices** tab of the appliance Web UI, enable **Port Forwarding** if needed. Then select the desired Camera Pod and click to open the Camera Pod Web UI.
5. In the **Sign in** dialogue box, enter the default **Username** (**apc**) and the assigned **Password**. Then click **Sign in**.

Update the Camera Pod 165 Firmware



1. Download the latest firmware version from the applicable product page of www.apc.com.
2. Select **System > Software Version** and record the current firmware version.
3. Log into the Camera Pod 165 Web UI then select **System > Software Upgrade**.
4. Under **Step1**, select **Choose File**, then browse to the appropriate firmware file on your computer.
5. Under **Step2**, ensure the drop-down list is set to **uImage+userland.img**.
6. Under **Step3**, click **Upgrade**, then wait for the upgrade to complete. If you lose connection to the Web UI, refresh the page.
7. Select **System > Software Version** to view the current firmware version and verify that the update was successful.

Change a Camera Pod 165 Password

Log on to the camera pod Web UI, then select **System > Security > User**. Enter the new password in the **Admin password** and **Confirm password** fields, then click **Save**.

Rack Access Tab

NOTE: If you plan to use an authentication server to control rack access, configure the server first. (See Configure Rack Access Settings, page 48 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/S, NBPD125)	• H10301 26-bit • H10302 37-bit • H10304 37-bit with facility code • CORP-1000 35-bit
NetBotz 13.56 MHz Handle Kit (NBHN1356/S, NBPD1356)	• MIFARE Classic 4-byte UID • MIFARE Classic 7-byte UID • MIFARE DESFIRE • MIFARE PLUS • iClass

The **Audit** tab 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 or **Download** to download a .csv file of rack access events.

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 **Cards** tab. Under **Actions** for that card, select **Register**.
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 27 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	The **Global Door Auto Lock Timeout** setting applies to all doors and cannot be disabled (see Configure Rack Access Settings, page 48).
Auto Lock Timeout	This value determines the number of seconds before an unlocked handle re-locks, 1 – 86400 seconds (1 second – 24 hours). The default value is 60 seconds (1 minute). **NOTE:** This only applies to closed handles on closed doors — open handles and open doors will not re-lock. Additionally, a door sensor must be installed to communicate the state of the door.

Click **APPLY** to save your changes.

NOTE: More restrictive access is generally more secure.

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 15.)
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 6 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 7 minutes. If the router does not set up communication with your appliance within 7 minutes, it will retry communication setup again in 5 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 31).
	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 31).

The Wireless Sensor Network

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

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

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

Devices on the Wireless Sensor Network

NOTICE
EQUIPMENT DAMAGE RISK Only the devices listed here are compatible with the NetBotz wireless sensor network. Other devices may not function and may damage the appliance or other wireless devices. **Failure to follow these instructions can result in equipment damage.**

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

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

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

Connect the Wireless Sensor Network

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

1. Select the coordinator and routers. If you have a pre-installed USB Coordinator and Router on your appliance, it acts as the coordinator. Note the extended address of the coordinator. If necessary, choose one or more USB Coordinator & Routers to become routers.
2. Choose the locations for the routers and end devices. Do not turn on the routers or end devices at this time.
3. Connect the Coordinator to the designated USB port on the NetBotz appliance.
4. Use an AC-USB adapter to apply power to each router. Routers are not directly connected to the NetBotz appliance.
5. Turn on the end devices after the coordinator and routers. This helps to preserve battery life.
6. Add end devices (wireless sensors) to the wireless sensor network. See Add Sensors to the Wireless Sensor Network, page 30 for instructions.

Add Sensors to the Wireless Sensor Network

Follow the instructions to Connect the Wireless Sensor Network, page 30. Then, in the **Wireless** tab, click **ADD**, and select one of the following options.

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.

NOTE: Wireless devices show as **Disconnected** until they establish communication with the appliance.

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. On the **Wireless** tab, 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.

   NOTE: The **APPLY** button will not activate until every sensor is updated. Allow about 20 minutes per wireless sensor for the update to complete.

NOTE: Wireless updates can be interrupted. If the update does not complete, repeat the update process.

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 Policies

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 Email Server, page 40 for details.) You must configure a remote trap receiver for trap notifications to work. (See Configure SNMP Settings, page 49.)

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 Configurations

NOTE: The options available depend on your appliance and which sensors are connected to it.

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**	Equals	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.
Outlet 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 8 feet per second, generate a warning alarm named “Low.”

You can use the **Alarm Configurations** 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 the Name of an existing alarm configuration to change it, or click**ADD** and select the sensor type to create a new alarm. Then configure the alarm settings.

Setting	Description
General	
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.
Type	Show the sensor type.
Operation	**Equals:** If the device returns a value equal to the **Value** field, the alarm is generated. **Not Equals:** If the device returns a value different from the **Value** field, the alarm is generated. **Less Than:** If the device returns a value less than the **Value** field, the alarm is generated. **Greater Than:** If the device returns a value greater than the **Value** field, the alarm is generated. **Less Thank or Equals:** If the device returns a value less than or equal to the **Value** field, the alarm is generated. **Greater Thank or Equals:** If the device returns a value greater than or 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. **Battery:** Enter a value in Volts (V). **0V-5V:** Enter a value in Volts (V). **4–20mA:** 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.).
Severity	Select the severity of the alarm: **Critical**, **Warning**, or **Informational**. You can also use the severity to configure notification policies.
Hysteresis	Hysteresis reduces chattering from frequently occurring alarms. Enabling hysteresis reduces the number of alarms raised and cleared. Alarms are raised immediately but will take longer to clear. Check the box to **Enable Alarm Hysteresis**,
Sensors	Select any sensors that can cause the alarm to be generated.
Clip Capture	This feature is optional. Select a camera to capture video from before and after the alarm is activated. The captured video will appear in the details window for any device that causes an alarm.
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 times during which the alarm can be generated. The alarm can not be generated during times that are not selected. Select **Use a schedule to control when this configuration is active** for the schedule to take effect.

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:

Enable DCE Surveillance

Path: Settings > System > DCE Surveillance

You can discover NetBotz appliances with Data Center Expert (DCE) and use DCE to monitor sensor readings through the appliance. In DCE v7.7 and later, you can also use the DCE interface to set events that trigger camera recording, record video on demand, and store camera recordings.

The appliance communicates over HTTPS. To establish secure communication with DCE,

1. Save the appliance certificate and DCE certificate to your computer. To obtain a certificate in Google Chrome, enter `https://ip_address` in the URL address bar, where *ip_address* is the IP address of your DCE or appliance Web UI. Click the symbol in far left of the URL address bar (a padlock or warning symbol), then select **Certificate > Details > Copy to File** and follow the prompts to export a Base-64 encoded x.509 certificate to your computer. If this certificate format is not an option, use OpenSSL to convert the downloaded certificate to PEM format.
2. Add the appliance's SSL certificate to DCE. See your DCE documentation for instructions.
3. In the appliance Web UI, go to **Settings > System > DCE Surveillance** and ensure **Verify DCE Certificate in Trust Store** is selected.
4. Add the DCE certificate to your trust store. Open the certificate in a text editor and copy its content. Then go to **Settings > System > Trust Store**. Click **ADD** to open the **Add certificate** window, then paste the certificate in the window. Click **ADD** to save the certificate in your trust store. See Configure Certificates for Outbound Connections, page 52 for more information.
5. Enable SNMP on the appliance (**Settings > System > SNMP**), then use SNMP to discover the appliance in DCE (see your DCE documentation for instructions).
6. In the appliance Web UI (**Settings > System > DCE Surveillance**), the **Data Center Expert URL** list should automatically populate with the DCE server on which your appliance is registered.

For less secure communication, you can choose not to add either certificate. You can still add the DCE URL to the **Data Center Expert URL** list manually: click **+ADD** and paste the DCE URL address into the resulting dialogue box.

> **NOTE: Verify DCE Certificate in Trust Store** checks the DCE certificate registered on the appliance. If you choose not to add the DCE certificate to your appliance, you must deselect **Verify DCE Certificate in Trust Store** .
>
> **NOTE:** If you do not add the appliance's SSL certificate to DCE, you must direct DCE to not verify the SSL certificate in the appliance communication 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.

Configure Discovery Settings for Downstream Devices

Path: Settings > System > Device Credentials

Use the **Device Credentials** page to configure discovery settings for downstream devices. The discovery settings must match the ONVIF, SNMPv1, or SNMPv3 settings on your device, or the device will not be discovered.

Setting	Description
Camera (ONVIF) **NOTE:** If you have not already set a password on a Camera Pod 165, you do not have to set the ONVIF credentials for that unit. The appliance will assign it a password.	
Username	The user name to access the camera..
Password/Confirm Password	The password to access the camera.
SNMPv1	
Read-only community name	The name used to access the Read-only community.
Read-Write community name	The name used to access the Read-write community.
SNMPv3 (More secure than SNMPv1.)	
Username	The identifier of the user profile.
Authentication/ Encryption	Select whether to use **No security**, **Authentication only**, or both **Authentication** and **Encryption**.
Authentication	Verifies that the device communicating through SNMPv3 is the device claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time.
Protocol	**SHA1:** Most secure option. **MD5:** Less secure than SHA1.
Password/ Confirm Password	The password or passphrase used for authentication.
Encryption	Encrypts the data sent over SNMPv3.
Protocol	**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	The password or passphrase used for encryption.

Select **APPLY** to save your changes, or **CANCEL** to discard them.

Configure an Email Server

Path: Settings > System > Email

Configure a service to send notification messages via email when status changes or errors occur. You must configure an SMTP server before you can configure email notifications.

Setting	Description
From email address	The e-mail address that will appear in the From field for emails generated by the appliance.
SMTP server	The hostname or IP address of the SMTP server.
SMTP Port	The IP port number to connect to the SMTP server.
Connection Security	Select a protocol to encrypt email notifications. It is recommended that you use the highest level of security supported by your Mail Transfer Agent (MTA). Use the **Send test email** function to check that email notifications can be sent with your chosen settings. **SSL/TLS:** This is the most secure option. It requires the MTA to encrypt emails through Transport Layer Security (TLS). If the MTA doesn't support encryption, the email is not sent. **STARTTLS:** This option is less secure. If the MTA supports encryption, emails are encrypted through TLS. If the MTA doesn't support encryption, emails are sent without encryption. **None:** This is the least secure option. Email notifications are not encrypted.
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 Log Settings

Path: Settings > System > Logging

You can configure a remote syslog server to store log files for events such as rack access events and camera discoveries. Once the server is configured, log files are automatically copied to the syslog server.

Setting	Description
Level	The 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 are not recorded. This setting also applies to the **Logs** Quick Link at the top right of the web UI.
Enable Remote Logging	Select to enable remote logging.
Server	Enter the host name or IP address of the syslog server.
UDP Port	Enter the UDP port number used to communicate with your syslog server.

Click **APPLY** to save your changes, or **RESET** to discard them. Click **TEST** to verify the connection to the syslog server.

How to Export Configuration Settings

You can use the configuration file (config.ini) of one appliance to configure other appliances. A configuration file can also be useful for backups in case your appliance is lost or damaged. This is the basic procedure to export the configuration file to other appliances. You can also use Data Center Expert to export the configuration settings (see Using Data Center Expert for Mass Configuration, page 44). Before exporting configuration settings, review the Considerations for Using Configuration Files, page 42.

1. Configure the appliance to have the settings you want to export.
2. Retrieve the config.ini file from that appliance. You can do this via SCP (see Use SCP to Retrieve and Upload the Configuration File, page 43) or the Web UI (see Use the Web UI to Export Configuration Settings, page 43).
3. If needed, customize the file (see Customizing the Configuration File, page 43).

   NOTE: Retain the customized file for future use. The appliance deletes the config.ini file after the settings are updated. **The file that you retain is the only record of your comments.**
4. Upload the configuration file to one or more appliances. Each appliance automatically updates its settings. You can upload the file to one appliance at a time via the Web UI (see Use the Web UI to Export Configuration Settings, page 43). You can also upload the config.ini file to one or more appliances over DCE (see your DCE documentation) or SCP (see Use SCP to Retrieve and Upload the Configuration File, page 43).

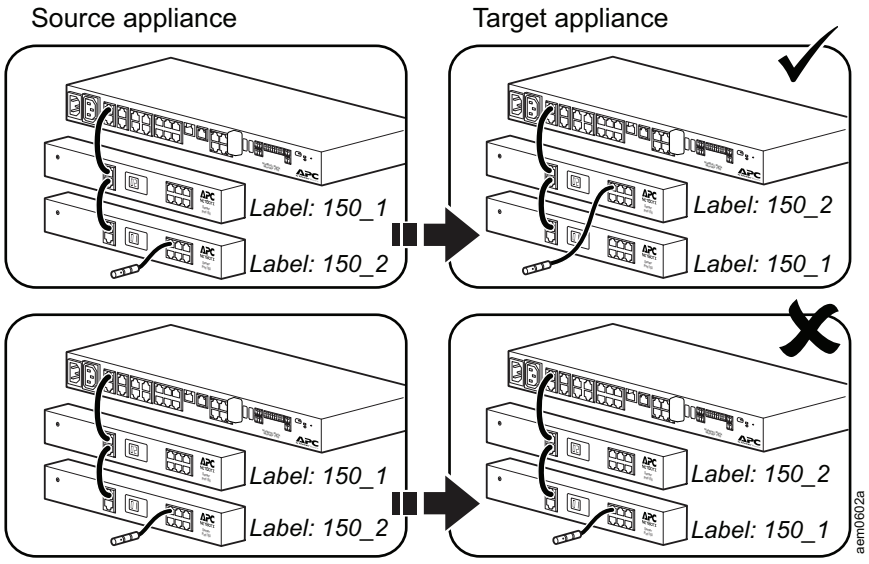
Considerations for Using Configuration Files

Consider the following when using configuration files:

- The firmware on the source appliance and the target appliance must match.
- The following settings are not transferred via configuration files: user passwords and SNMPv3 passwords.
- The devices connected to the source appliance and target appliance must match. Devices that do not match will not be updated. For this reason, it is recommended that you use the same model of source appliance and target appliance (for example, use the config.ini from a Rack Monitor 750 to configure a Rack Monitor 750 and not a Room Monitor 755.)
  - Corresponding devices must be attached to the same ports on each appliance.

    Example: There is a Temperature Sensor (AP9335T) attached to Universal Sensor Port 1 on the source appliance. Another Temperature Sensor (AP9335T) must be attached to Universal Sensor Port 1 on the target appliance.
  - Sensor Pods and Rack Access Pods must have corresponding labels. Pods with corresponding labels must have matching sensors.

    Example: The source appliance has two Sensor Pod 150 (NBPD0150) units cascaded from the A-Link port . The target appliance must have two Sensor Pod 150 units *with the same labels*. The units do not have to be cascaded in the same order, but sensor configurations must match on pods with matching labels.



  - Camera Pod 165 units, Alarm Configurations, and Notification policies must have matching Labels/Names.
- Since alarms are configured for specific sensors, alarm settings configured for nonexistent sensors on the target appliance will not be transferred.
- The IP address and hostname only change if the MAC address is also set in the configuration and it matches that of the target machine.

  NOTE: You can edit labels from the Details Windows, page 15.

Use the Web UI to Export Configuration Settings

Path: Settings > System > Mass Configuration

Click **Download** to download a config.ini configuration file with the current settings of the NetBotz appliance.

Click **Choose File** to upload a configuration file to this appliance, then click **APPLY**.

NOTE: The uploaded configuration file is stored on this page even after the new settings are applied.

Use SCP to Retrieve and Upload the Configuration File

NOTE: The following procedures assume that you are using OpenSSH. Commands may vary for other SSH tools.

To retrieve the file:

1. Configure the appliance with the settings you want to export.
2. Open OpenSSH or a similar tool and use the following command to retrieve the file:

   `scp` *`username@hostname_or_ip_address`*`:config.ini ./config.ini`

   Then enter the correct password.

The following command uploads the config.ini to a single appliance:

`scp C:/`*`local_folder`*`/config.ini` *`username@hostname_or_ip_address`*`:home/root/config.ini`

To upload the file to multiple appliances, you can write a script that incorporates the command for uploading the file to a single appliance.

Customizing the Configuration File

If possible, use the interface of the appliance to configure it with the settings to export. You risk introducing errors when directly editing the config.ini file.

The config.ini file contains the following:

- Section headings and keywords (only those supported for the device from which you retrieve the file): Section headings are category names enclosed in brackets ([ ]). Keywords, under each section heading, are labels describing specific appliance settings. Each keyword is followed by an equals sign and a value (either the default or a configured value).
- The `Override` keyword: With its default value, this keyword prevents the exporting of one or more keywords and their device-specific values, e.g., in the [`NetworkTCP/IP`] section, the default value for `Override` (the MAC address of the appliance) blocks the exporting of values for the `SystemIP`, `SubnetMask`, and `DefaultGateway`.

You can customize the following features and metadata using a text editor:

- Comments: Start each comment line with a pound sign (#).
- Section headings, keywords, and pre-defined values: These are case sensitive.

  “Not configured” indicates a value that is intentionally undefined. It will delete configured values on the target appliance.

Retain the customized configuration file for future use. The file that you retain is the only record of your changes and comments.

Using Data Center Expert for Mass Configuration

Follow the Data Center Expert® (DCE) instructions for Mass Configuration of APC Network Management Card type devices on the EcoStruxure IT Help Center.

Keep the following in mind for the NetBotz Rack Monitor 750 and Room Monitor 755 :

- These are not NMC devices. NetBotz 5.x firmware is separate from APC AOS firmware. FAQs specific to APC AOS firmware and NMC devices do not apply to NetBotz 5.x.
- You will need the NetBotz Scanner DDF version 17 or later and NetBotz firmware v5.3.0 or later to use DCE for mass configuration.
- FTP is not supported.
- If you see “DCE Status Failed: Unable to Connect,” confirm that there is a config. ini file on the NetBotz appliance. You can force one to be created in the appliance Web UI: navigate to **Settings > Mass Configuration** and select **Download**.

Tips for the **Configure Device Settings** dialogue box:

- It is recommended that you configure settings on your NetBotz appliance and not in DCE. Editing settings in DCE risks introducing errors to the configuration settings. Invalid settings are ignored and are not passed on to the target appliance. (See Enumerations, page 45 for more information)
- If you cannot find a setting under the appropriate section, look under **Advanced Settings**.
- If you choose to export one setting on an asset, select all settings for that asset, including the Asset Sensor Type, to ensure the change will be exported.
- If you choose to export “Not Configured” values, this will erase corresponding values configured on the target appliance.
- SNMP settings are only read and used for the enabled SNMP version. Uncheck options for the unused SNMP version.

Enumerations

Enumerations are data points that require specific values to be input. Enumerations with incorrect inputs in DCE will not be configured in the target appliance. The following lists show of acceptable values for each enumeration type.

ApplianceLogLevel • EMERGENCY • ALERT • CRITICAL • ERROR • WARNING • NOTICE • INFORMATION • DEBUG	EmailConnSecurity • NONE • SSL • STARTTLS	MessageFormatOptions • TIME_24_HOUR • TIME_12_HOUR • IMPERIAL_UNITS • METRIC_UNITS • AUTO_SCALE • INCLUDE_UNITS	NotifyType • EMAIL • SNMP_TRAP • HTTP_POST
RackAccessUserType • LOCAL • LDAP	SensorPortType • RACK_HANDLE • RACK_DOOR • UNIVERSAL • BEACON	• RELAY_OUTPUT • SWITCHED_OUTLET • INPUT	• UNKNOWN • INTERNAL • SNMP
SensorType • ACTIVE_POWER • AIRFLOW • AIRFLOW_SPEED • APPARENT_ENERGY • APPARENT_POWER • BATTERY • BEACON • CONTACT • COUNT • CURRENT • CURRENT_INPUT • CURRENT_INPUT_DB • PRESSURE • DEWPOINT • DISTANCE • DOOR • DURATION • ENERGY	• EXTERNAL_RELAY • FLUID_FLOW_HOURS • FLUID_FLOW_MINUTES • FLUID_FLOW_SECONDS • FREQUENCY • OUTPUT_RELAY • DOOR_LOCK • RACK_HANDLE • CARD_READER • LEAK_ROPE • MOTION • NUMERIC • OUTLET • PERCENT • RELATIVE_PERCENT • POWER • POWER_FACTOR • REACTIVE_ENERGY • RELATIVE_HUMIDITY	• REACTIVE_POWER • RPM • RSSI • RUN_HOURS • SMOKE • SPOT_LEAK • STATE • SWITCH • SWITCHED_OUTLET • TEMPERATURE • TEMPERATURE_DELTA • WATER_COLUMN • TIME • VIBRATION • VOLTAGE • MODE • BATTERY_CAPACITY • BREAKER • CPU_TICKS	• CPU_UTILIZATION • CREST_FACTOR • DOOR1_12V • EXT_12V • ROPE_5V • UNI_5V • DOOR2_5V • DOOR1_5V • UNI_24V • EXT_24V • BEACON_24V • ROPE_24V • DEGREE_ANGLE • WATER_CONDUCTIVITY • TRIP_STATUS • INTERNAL_RELAY • LOCK • LINK_STATUS • ***UNKNOWN***
Severity • CRITICAL • INFO • OK • WARNING	SnmpVersion • VERSION1 • VERSION3	SnmpV3Authentication • MD5 • SHA1	SnmpV3Encryption • DES • AES128
SnmpV3SecurityType • NOAUTH_NOPRIV • AUTH_NOPRIV • AUTH_PRIV			

Enable Modbus TCP

Path:Settings > System > Modbus

Enable Modbus TCP to allow a Building Management System to monitor the Rack Monitor 750.

For detailed information on Modbus registers and bit descriptions, see the NetBotz Rack Monitor 750/755 Modbus Register Map available on the APC website.

1. Select **Enable** to allow Modbus TCP as a method of communication with the appliance.
2. Set the **Port** number for the TCP connection, 502 (default, recommended) or 5200-32767.
3. Click **Apply** to save your changes.

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.

Configure Rack Access Settings

Path: Settings > System > Rack Access

Configure Auto Lock Timeout

Under **General**, enter a value in the **Global Door Auto Lock Timeout** field to determine the number of seconds before any unlocked handle re-locks. This only applies to closed handles on closed doors — open handles and open doors will not re-lock. A door switch sensor must be installed to detect whether the door is open or closed.

This setting applies to all doors with Rack Access control. See Schedule Rack Access, page 28 for details.

Configure an Authentication Server

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 (Full DN)	Enter the user name to log into your company's authentication server. Use the full distinguished name—you can copy this directly from your LDAP directory. The more specific your filepath is, the shorter the search will be.
Password	Enter the password to log into your company's authentication server.
Test Connection	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.

Restart the Appliance

Path: Settings > System > Restart Device

Click **RESTART** to restart the appliance.

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	
Device Information: Internet management systems may request the name, system location and contact person for this device to help with identification.		
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.)	
Agent Enable and configure how a SNMP manager (management station) can connect to this SNMP server to perform management operations.		
Enable	Select to enable the SNMP agent on your appliance.	
Port	The port number for SNMP communications.	
SNMPv1		
Read-only community name:	The read-only community name for SNMP requests.	
Read-write community name:	The name used to access the Read-write community.	
SNMPv3 (More secure than SNMPv1.)		
Username	Enter the user name to access the SNMP agent.	
Authentication/ Encryption	SNMPv3 only. Select whether to use **No security**, **Authentication only**, or both **Authentication** and **Encryption**.	
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: View and manage the SNMP trap notifications. The appliance supports up to 10 trap receivers, including any trap receivers automatically generated by Data Center Expert. Visit the **Resources** page to download the NetBotz MIB files.		
ADD	Click to enable and configure where SNMP trap notifications issued by this device are sent to.	
Enable	Select to enable SNMP traps.	
Port	The port number of the remote SNMP trap receiver.	
SNMPv1		
Community name	The community name for SNMP trap requests.	
Send test trap	Select to send a test trap to a configured trap recipient.	
SNMPv3 (More secure than SNMPv1.)		
Username	Enter the user name to access the remote trap receiver.	

Setting	Description	
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

NOTE: You can find more information about certificates, encryption, and authentication in the TLS Authentication for HTTPS and TLS Authentication for SMTP and LDAP sections of the *Security Handbook* on www.apc.com.

You can use this page to 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 Authority-signed (CA-signed) certificate. Both kinds of certificate provide encryption for your information. However, while most Web browsers trust signatures from major Certificate Authorities, they do not trust signatures from self-signed certificates. If your browser generates a warning page at log on, this means it does not recognize the certificate's signature. To stop the warning page from appearing, you can install a certificate with a recognized signature or direct the Web browser to trust the provided signature.

Self-signed certificates: The NetBotz appliance ships with an RSA 2048-bit, self-signed certificate. If you change the host name of your appliance, the certificate is automatically updated. Self-signed certificates expire after 398 days. You can regenerate the certificate at any time (see **Generate a Self-signed Certificate** on this page). The new certificate will expire 398 days 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. 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.
Email 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.

It takes a few minutes to install and activate the new certificate. Refresh the browser and set the new certificate as trusted.

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 Video Capture Settings

Path: Settings > System > Video Capture

NOTE: It may take a few seconds for the camera to stop recording. Total capture time may be longer than the sum of the pre-alarm and post-alarm capture times.

You can configure cameras to record video when alarms are generated (see Configure Alarms, page 34 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 for which images are recorded and saved before an alarm is activated.
Post-alarm capture time	The total number of seconds for which images are recorded and saved after an alarm is activated.

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 29).

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 help to ensure that all units support the same features in the same manner.

Schneider Electric firmware is signed. The hash signature is checked during the firmware update process. If the signature does not match, the firmware is not installed.

DO NOT run the installer if your calculated value does not match the published hash signature. Please contact support to report the issue.

A minimum of NetBotz firmware version 5.3.5 must be installed to update to version 5.5.x. You can update to version 5.5.0 from version 5.3.5 or 5.4.x.

To update the firmware:

1. Download the latest firmware version for free from the APC website, www.apc.com.
2. Under **Settings > Firmware Update**, 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.

How to verify the checksum from Windows PowerShell

1. Download the most current NetBotz 5.x firmware update file to your Windows machine.
2. Open PowerShell. The PowerShell.exe command starts a session in a command window.
3. Navigate to the directory containing the downloaded file.
4. Use the Get-FileHash PowerShell command to calculate the SHA–256 checksum of the file and compare it against the published value in the table.
   - ***Get-FileHash -Path .\ firmware_update_file_name -Algorithm SHA256***

How to verify the checksum from a Linux terminal

1. Download the most current NetBotz 5.x firmware update file to your Linux machine.
2. Open a terminal window.
3. Navigate to the directory containing the downloaded file.
4. Use the ***sha256sum*** terminal command to calculate the SHA256 checksum of the file and compare it against the published value in the table.
   - ***sha256sum firmware_update_file_name***

Firmware Downgrade

You can downgrade from firmware v5.5.0 to v5.4.0. Downgrades from firmware v5.4.0 are not supported.

1. Save a backup file of the current configuration. See Save a Backup File, page 56.
2. Perform the firmware update procedure (Update the Appliance Firmware, page 54) with a previous firmware version.
3. Reset to defaults via the Web UI or the console.

   Web UI:

   a. Log into the Web UI as the Super User.

   b. Open a new browser page, type

      `<your appliance's IP address>/rest/appliance/resetconfig`

      in the URL address bar, then press **Enter**.

      Example: `93.184.216.34/rest/appliance/resetconfig`

      The appliance takes about 6 minutes to restart completely. Until the restart is complete, the Web UI is not available.

   c. If needed, see Use Your Computer to Establish Network Settings, page 9 or Use a Terminal Emulator to Establish Network Settings, page 10 for instructions to discover or change the IP address.

   Console:

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

   b. 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.

   c. 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 correct cable is being used as specified in step a.
      - The terminal settings are correct as specified in step b.
      - The Silicon labs CP210x driver is installed on your computer. You can find the driver on www.silabs.com.

   d. Log on with the Root account user name (**root**) and password (you set the password on first use).

   e. Press **Shift + x** within 5 seconds of logging on. Then enter the following command:

      `/netbotz_app/factory_reset.sh`

   f. Wait about 6 minutes for the appliance to restart.

   g. If necessary, see Use Your Computer to Establish Network Settings, page 9 or Use a Terminal Emulator to Establish Network Settings, page 10.

4. If you have a backup file of the downgraded firmware version, use it to restore the configuration (see Restore System Settings, page 57). You must use a backup file saved from the same firmware version that you downgraded to.

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.

> **NOTE:** This procedure does NOT transfer sensors, sensor pods, camera pods, sensor data, or data logs. This procedure does transfer configurations for notifications and threshold alarms.
>
> Connected sensors, sensor pods, and external devices such as camera pods will be rediscovered after the settings are updated.

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 the Event Log

Path: Settings > Logs

The Event Log lists the most recent events, including the date and time each event occurred, in reverse chronological order. System events are logged for most activities, including abnormal internal system events. You can click **Download Log Files** to download a .csv file of the event log.

Click **Download Troubleshooting Information** to download all the system logs in a zip file, log_export.tar.gz.

REST API

The REST API allows you to interact with the appliance via JSON requests.

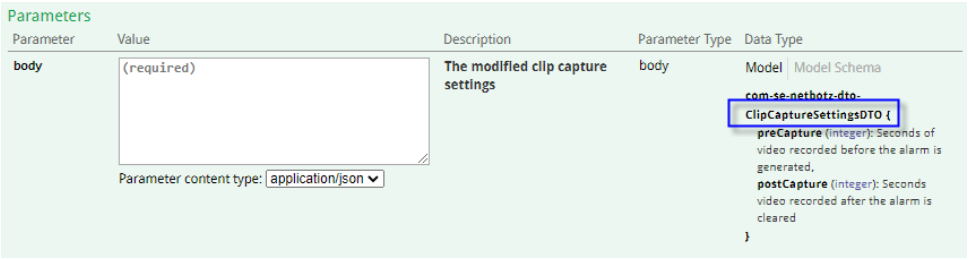
The online REST API documentation provides a list of operations available plus models for requests and responses. It also provides an interactive interface to test operations. Your permissions in the REST API documentation depend on your permissions in the Web UI.

To access the online REST API documentation, log on to the Web UI, then open a new tab and enter *your_appliance_IP_address*/docs/rest in the URL address bar.

To access the REST API, enter *your_appliance_IP_address*/rest.

About Request Body Content

- Include the nbType in every applicable section of a request body. To find the required nbType , go to the REST API documentation for the request body parameter and select **Model**. The nbType is a single string that ends in DTO. For example, the request body for **POST /cameras/clip/settings** requires one nbType: ClipCaptureSettingsDTO.



A properly configured request body would look like this:

```
{
”nbtype”: ClipCaptureSettingsDTO,
”preCapture”: 4,
"postCapture”: 4
}
```

- IDs are automatically generated by the appliance and cannot be changed. When creating a request body, always leave the id blank. Unlike IDs, labels are user-friendly names that you can configure and modify.
- You have the option to leave some request body values unconfigured. To leave an integer value unconfigured, enter 0. To leave a string value unconfigured, enter empty quotes (“ ”) or null (no quotes).
- If a value is not used, ignored, or reserved for future use, enter null (string), 0 (integer), or false (boolean).

About Formatting

- Enter the request body using valid JSON format.
- All values are case sensitive.
- String values (except `null`) must be enclosed in quotation marks. Booleans and integers are not enclosed in quotation marks.
- Use commas to separate inputs for values that accept lists. For example, `asset-1, asset-2, asset-3`.
- Time values (both input and retrieved) are always formatted as milliseconds since the UNIX® epoch (milliseconds since epoch). You can use an online converter such as www.epochconverter.com to check the time values.

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 6 minutes to become accessible. Wait for 6 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
70 Mechanic Street
02035 Foxboro, MA
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.

990-5934K