NetBotz 5.x

Release Notes for NBRK0750, NBWL0755

What's in This Document

Affected Revision Levels

Component	Version	Details
NetBotz 5.x Application	5.3.1	Firmware for NetBotz 5.x appliances
Wireless Devices: NBWC100U NBWS100T/H	 1.1.7 1.1.5	Firmware for the wireless sensor network

APC
70 Mechanic Street
02035 Foxboro, MA
USA

Supported Browsers

The Web UI supports the latest versions of the following Web browsers. Other commonly available browsers and versions may work, but have not been tested.

- Google® Chrome®
- Microsoft® Edge®
- Mozilla® Firefox®
- Microsoft® Internet Explorer® 11.x

New Features

NetBotz Application v5.3.1 You can now add up to 10 SNMP trap receivers.
Wireless Applications (NBWC100U v1.1.7, NBWS100T/H v1.1.5) General improvements for performance and stability.

Fixed Issues

Each issue has a unique tracking number (XXXX) that can be used to identify it in the **Fixed Issues** or **Known Issues** section. Customer Support does not use these tracking numbers.

NetBotz Application v5.3.1

- Upgraded log4j to v2.16.0 to resolve CVE-2021-44228.
- Handles are no longer auto-locked while open (8122).
- Fixed an issue where upgrading from firmware v5.2.1 occasionally caused private-side devices to lose connection with the NetBotz appliance and prevented private-side devices from being discovered (8506).
- Fixed a communication issue with Data Center Expert® (DCE) (8464).
- Fixed an issue that sometimes prevented the user from locking a single door handle from DCE (8323, 8093, 7942).
- Fixed an issue that prevented updates to the wireless firmware (8388).
- Fixed an issue that prevented firmware upgrades from version 5.2.1 (8500).
- Fixed an issue that caused errors after many changes to the system settings (8501).
- Fixed an issue that sometimes caused the temperature/humidity reading to show a value of 0 (8384).

Wireless Applications (NBWC100U v1.1.7, NBWS100T/H v1.1.5)
None.

Known Issues

Each issue has a unique tracking number (XXXX) that can be used to identify it in the **Fixed Issues** or **Known Issues** section. Customer Support does not use these tracking numbers.

NetBotz Application v5.3.1

New

- The IP address of the NetBotz appliance occasionally becomes inaccessible. Reboot the appliance to obtain a new IP address (8434).
- Mass configuration via the Web UI does not work (8448).
- DCE communication is lost after configuring SNMPv3 traps. Re-enter the SNMPv3 agent password to resume communication with DCE (8505).
- Resolved alarms shown in DCE do not always match resolved alarms in the NetBotz appliance (8519).
- The Devices page is sometimes blank. Wait for the page to load, or navigate to a different page and back (8538).
- Changing the SNMP agent version causes the appliance to slow down (8560).
- Spot leak sensors are occasionally disconnected after a reboot. Un-plug and re-plug the sensor to re-establish communication with the appliance (8420).
- DCE trap receivers are not deleted when the appliance is removed from DCE (8429).
- In email notifications for unplugged wireless sensors, the EMS field is blank (8543).
- State values for temperature sensors display incorrectly (8489)
- Network Port Sharing setups for Rack PDUs are not discovered on the NetBotz Rack Monitor 750 (8492).
- Sensors occasionally disconnect and re-connect without user input (8497).
- If the config.ini file is used to change multiple settings on the appliance, the appliance downloads the config.ini file to itself multiple times (8514).
- The Fix Credentials feature does not re-establish communication with discovered devices. You must re-discover devices manually (8536).
- You cannot delete disconnected rack access devices from the Web UI if the devices have previously been configured as part of an alarm control scheme. For example, if a rack access handle is configured to lock in the event of a “smoke detected” alarm, and the handle becomes disconnected, that handle cannot be deleted from the Web UI (8546).
- Rack access cards registered with SSL LDAP users cannot access handles connected to the appliance or to Rack Access Pod 175s. SSL LDAP users can access handles connected to Rack Access Pod 170s (8548).
- Changing the time zone in the NetBotz appliance does not change the time for connected camera pods. You can restart the appliance to force the time zone change in connected camera pods (8553).
- When a forced-entry alarm is cleared, the clear time is not shown in the Web UI (8562).
- Camera pods sometimes begin streaming in night mode (black and white). To return to color streaming, cover the camera lens and light sensor for a few seconds (8568).
- Camera pods occasionally become disconnected and cannot be re-connected (8570).
- After firmware updates, Appliances with DCE connections may show an incorrect DCE trap. (8571).
- Sensor data graphs do not show the date in the x-axis (8427).
- The Wireless page of the Web UI may flicker (8431).
- Some UPS sensor readings are still displayed after the UPS is disconnected (8435).
- The Powernet MIB available for download from the Web UI is an abbreviated version used only by DCE. It will be removed in a future update (8440).
- Details windows for sensor data are not updated dynamically. To see if the sensor reading is changing, close and re-open the details window (8457).

NetBotz Application v5.3.1 (continued)

New (continued)

- **Settings > System > Logging:** The Reset button does not fully discard your changes (8499).
- On the Firmware Upgrade page, the Upload button is not automatically enabled after clicking Start Again. Refresh the page to enable the Upload button (8561).
- “Card reader replugged” email notifications are sent when rack access handles are disconnected. (8650)
- A duplicate default trap may appear after you delete a trap reciever (8569).
- The Rack Monitor 750 sometimes loses communication with internal sensors after a firmware upgrade. Contact customer support at www.apc.com for help resolving this issue (8490).

Sensors and Rack Access Pods

- Manual wireless updates may not complete. If the update does not complete within a few hours, restart the update process (6710).

Downstream Devices

- To discover an rPDU or UPS with SNMPv3, the rPDU/UPS must be using AOS v6.8.2 or later (6948).
- Some label changes in sensors for downstream devices do not update in the appliance Web UI. For example, if you change the name of a Smart UPS Outlet Group, the name is not updated in the appliance Web UI (7002).
- You can enable Port Forwarding to access the Web UI of a downstream device. However, if you disable Port Forwarding while connected to a downstream device’s Web UI, Port Forwarding will not be disabled for the current connection until you close the device’s Web UI. While Port Forwarding is disabled, new connections are not allowed (7026).

Miscellaneous

- **Settings > System > Date and Time:**Users may be automatically logged out after manually changing the system time or moving the time forward (3482).
- **Settings > System > SMTP Server:** The username and passwords do not stay on the page after you click **APPLY**. However, they are saved in the system.
- If the beacon is controlled by multiple sensors, it reacts to every state change in those sensors. Consider the following example: the beacon is set to turn on when either of two output relays are active. If both relays activate, but only one relay de-activates, the beacon turns off (7601).
- Email alerts may show the incorrect sensor label (7710).
- You may receive the following error message when uploading SSL certificates with Elliptical Curve Cryptography: *Command failed, please check the configuration and the certificate and key*. This happens because the appliance only accepts private keys in PKCS8 (PEM) format. Ensure your key is formatted correctly, then try again (7864).
- After updating the firmware, there may be some cases where the Web UI appears empty in Google Chrome®. Press **Ctrl + F5** on Windows®/Linux® systems, or **Cmd + Shift + R** on Macintosh® systems to perform a hard refresh. You only need to do this once.
- When appliance restarts after updating to firmware, the year (under **Date and Time** settings) may be reset. Check the year and correct this setting if needed (8039).
- If you change the appliance Hostname (**Settings > System > Network**), the appliance IP Address may change. This only happens in DHCP mode and depends on the DHCP server configuration (8071).
- You may receive an Incomplete Configuration error message when performing a mass configuration in DCE. This can be caused by different actions:
  - modifying the AssetRack_Name under [RackAccess_1] (8211).
  - modifying an asset name associated with an alarm configuration (8161).

  You can ignore the error message—the settings are still updated.

Wireless Applications (NBWC100U v1.1.7, NBWS100T/H v1.1.5)
None.

Miscellaneous

Update the Appliance Firmware

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.

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.

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.

MIB

You can download the latest version of the MIB from the appropriate product page on www.apc.com.