NetBotz 5.x

Release Notes for NBRK0750, NBWL0755

What's in This Document

Affected Revision Levels

Component	Version	Details
NetBotz 5.x Application	5.5.0	Firmware for NetBotz 5.x appliances A minimum of NetBotz firmware version 5.3.5 must be installed to update to version 5.5.x.
Wireless Devices: NBWC100U NBWS100T/H	 1.2.0 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®

New Features

NetBotz Application v5.5.0

- Logging improvements
  - Download all the system logs for troubleshooting in one click to a compressed zip file (log_export.tar.gz) in Settings > Logs.
  - Test the connection to the syslog server in Settings > System > Logging.
  - Syslog messages are now sent for system log in/log out and user credential changes.
- Alarm improvements
  - Configure hysteresis to reduce chattering from frequently occurring alarms in Settings > Alarm Configurations.
- General improvements for performance and stability

Wireless Applications (NBWC100U v1.2.0 NBWS100T/H v1.1.5)

None

Fixed Issues

NetBotz Application v5.5.0 • Cameras can now be discovered using HTTPS. • The beacon state changes as expected when the alarm threshold is manually changed.
Wireless Applications (NBWC100U v1.2.0 NBWS100T/H v1.1.5) None

Security updates

This release includes various component updates to improve overall security.

Known Issues

NetBotz Application v5.5.0

New

- After upgrading to v5.5.0, Remote Logging is enabled with the Server value 514. This is an invalid value and does not impact the operation of the system. To disable remote logging, go to Settings > System > Logging, uncheck the Enable Remote Logging box, and click Apply.

Sensors and Rack Access Pods

- When rack access handle or door sensors are unplugged, both the unplugged and replugged email alerts are sent.
- Disconnected/Reconnected alarms occasionally occur for Appliance Rack Access when no Rack Access Pods or Handles are connected to the appliance.
- Rack Access Pods, Handles, and Door Sensors cannot be deleted if they are part of an alarm control configuration.
- 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.
- 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.
- You can only lock or unlock one Rack Access Handle at a time from Data Center Expert (DCE).
- “Card reader replugged” email notifications are sent when rack access handles are disconnected.
- Consecutive duplicate data points are not displayed in the graphs for state and numeric sensors.

  See FAQ000255915
- Details windows for sensor data are not updated dynamically. To see if the sensor reading is changing, close and re-open the details window.
- Some UPS sensor readings are still displayed after the UPS is disconnected.
- Sensor data graphs do not show the date in the x-axis.
- Sensors occasionally disconnect and reconnect without user input.
- In email notifications for unplugged wireless sensors, the EMS field is blank.
- State values for temperature sensors display incorrectly.
- Spot leak sensors are occasionally disconnected after a reboot. Unplug and re-plug the sensor to re-establish communication with the appliance.
- Manual wireless updates may not complete. If the update does not complete within a few hours, restart the update process.

NetBotz Application v5.5.0 (continued)

Downstream Devices

- Camera settings are not applied as expected when you select the camera from the Devices option and launch its UI. Access the camera's UI from a new browser window. With port forwarding enabled, add 5100 to the URL, for example, https://cameraIPaddress:5100.

  See FAQ000232700
- UPS and Rack PDU units connected to the Private LAN port are not discovered automatically. You can still discover them manually by selecting **+ADD** from the **Devices** tab.
- The alarm count in the Quick Status Area does not always match the number of active alarms in the Alarms tab.
- When you change a camera label, associated camera rules are not automatically updated to match the new label. Mass-configuration will not succeed until you update the labels manually and export a new config.ini file with the updated rules.
- **Settings > System > Date and Time > NTP:** If you click refresh , the **APPLY** button is deactivated, preventing you from saving changes to the NTP settings.
- 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.
- Camera pods occasionally become disconnected and cannot be re-connected.
- Camera clips associated with active alarms may be deleted when the alarms are 96 hours old.
- 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.
- Network Port Sharing setups for Rack PDUs are not discovered on the NetBotz Rack Monitor 750.
- The Devices page is sometimes blank. Wait for the page to load, or navigate to a different page and back.
- To discover a Rack PDU or UPS with SNMPv3, the Rack PDU/UPS must be using AOS v6.8.2 or later.
- 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.
- 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.
- 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.

Data Center Expert (DCE)

- DCE trap receivers are not deleted when the appliance is removed from DCE.
- Resolved alarms shown in DCE do not always match resolved alarms in the NetBotz appliance.
- After firmware updates, Appliances with DCE connections may show an incorrect DCE trap.
- 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].
  - Modifying an asset name associated with an alarm configuration.

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

Miscellaneous

- A duplicate default trap may appear after you delete a trap receiver.
- **Settings > System > Logging:** The Reset button does not fully discard your changes.
- On the Firmware Upgrade page, the Upload button is not automatically enabled after clicking Start Again. Refresh the page to enable the Upload button.
- The Wireless page of the Web UI may flicker.
- When a forced-entry alarm is cleared, the clear time is not shown in the Web UI.

- 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.
- The Fix Credentials feature does not re-establish communication with discovered devices. You must re-discover devices manually.
- Changing the SNMP agent version causes the appliance to slow down.
- Mass configuration via the web UI may fail if the system is busy. No error is displayed. A subsequent attempt succeeds as expected.
- The IP address of the NetBotz appliance occasionally becomes inaccessible. Reboot the appliance to obtain a new IP address.
- **Settings > System > Date and Time:**Users may be automatically logged out after manually changing the system time or moving the time forward.
- **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.
- Email alerts may show the incorrect sensor label.
- 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.
- 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 the appliance restarts after updating the firmware, the year (under **Date and Time** settings) may be reset. Check the year and correct this setting if needed.
- 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.

Wireless Applications (NBWC100U v1.2.0 NBWS100T/H v1.1.5)

None

Miscellaneous

Firmware Download

You can download firmware version 5.5.0 from https://download.ecostruxureit.com/netbotz/5.5.0.187/NBRK0750_Build_5.5.0.187.sedp.

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.

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***

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, or from the Resources quick link in the appliance Web UI.