

## NetBotz 5.x

Release Notes for NBRK0750

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

### What's in This Document

Affected Revision Levels .....	1
Supported Browsers and Platforms .....	1
New Features .....	2
Fixed Issues .....	2
Known Issues .....	3
Miscellaneous .....	5
Update the Appliance .....	5
Update the Wireless Sensor Network.....	5
MIB .....	5

## Affected Revision Levels

Component	Version	Details
NetBotz 5.x Application	5.2.2	Firmware for the NetBotz 5.x appliance
Wireless Devices: NBWC100U NBWS100T/H	1.1.1 1.1.2	Firmware for the wireless sensor network

## Supported Browsers and Platforms

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®
- Mozilla® Firefox®
- Microsoft® Internet Explorer® 11.x

## New Features

### NetBotz Application v5.2.2

Added configuration for SNMPv1 Read-write community. This is primarily used for StruxureWare Data Center Expert® integration.

### Wireless Applications (NBWC100U v1.1.1, NBWS100T/H v1.1.2)

None—same as the previous release.

## 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 v5.2.2

- Fixed an error caused when the subnet of the appliance's public network interface overlaps with the subnet of the appliance's private network interface. When undetected, this conflict caused communication issues with the appliance. One side effect was network timeouts caused by unsent response packets. (5745)
 

**NOTE:** Communication issues may still occur if the subnet of a remote network overlaps with the subnet of the appliance's private network. In this case, you can see the FAQ article FA372290 for more detailed information or contact customer support at [www.apc.com](http://www.apc.com) for assistance.
- Simultaneously logging into the Web UIs for two separate appliances no longer causes an error message. (7105)
- Fixed clickjacking security vulnerability. (6121)
- Fixed CSRF token vulnerability. (7175)
- The Motion Masking feature no longer appears for third-party ONVIF cameras, which do not support it. (6257)
- Firmware updates no longer cause the default Common Name (CN) in the self-signed certificate to change to snarc-soca9. The CN automatically matches the appliance host name and cannot be edited. (7112)
- Scheduled tasks are no longer blocked if you move the system time backwards from point A (in the future) to point B (in the present). (7119)
- The Web UI now asks for confirmation to delete a rack access card. (6040)
- Video now appears in Internet Explorer® 11. (1361)
- Alarms for disconnected devices now appear properly. (6880)
- You can now see the motion detection status for a camera in the Overview tab. (6548)
- The proper email notification is now sent when Humidity values return to normal. (6629)
- All Smart UPS sensor readings appear in the correct format. (6961)
- The **Fix Credentials** control can be used to re-establish communication after a downstream device's SNMP configuration has changed. (7136)
- The appliance now supports ID changes on Sensor Pods and Rack Access Pods. (6568)
- Only one alert is generated per disconnected device. (7092)
- Power Factor values for downstream devices are displayed correctly. (7124)
- Battery and RSSI values now appear in StruxureWare Data Center Expert. (7147)

### Wireless Applications (NBWC100U v1.1.1, NBWS100T/H v1.1.2)

None—same as previous release.

# 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 v5.2.2

### New

- In some cases, a Wireless Coordinator (NBWC100U) may not be able to form a network. (When a network is formed, the Coordinator LED flashes green. See the Coordinator *Installation Manual* on [www.apc.com](http://www.apc.com) for more detailed information.) Disconnect and reconnect power to the appliance. This enables the Coordinator to form a network. (5617)
- Downstream device credentials (**Settings > System > Device Credentials**) are not restored during the Backup/Restore process. (7404)
- The appliance memory can be filled if alarms with clip capture are triggered constantly. This can be caused both by alarms that never clear and by alarms that clear and are immediately triggered again. When this happens, you may be unable to log onto the appliance and receive an incorrect password message. Contact customer support at [www.apc.com/support](http://www.apc.com/support) for help with regaining access to the appliance. (7442)
- This appliance may disconnect from StruxureWare Data Center Expert® (DCE) if you set the time forward (**Settings > System > Date and Time**). Restart DCE to reconnect the appliance. (7443)

### 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)
- Some sensors may show a label key instead of the sensor state. For example, the status of a relay input may show **Relay Normal Status - Int Relay NAME: sensor.state.iemRelayNormalStatus.open** instead of **Relay 1: Open**. (7011)
- Deleting a Rack Access Pod 170 causes an error message. To successfully delete the pod, first go to the **Rack Access** tab and delete the associated door configurations. Then go to the **Overview** tab and delete the pod. (7124)
- Universal sensors may show as disconnected after you update the appliance firmware. To correct the sensor status, unplug the sensors, then re-connect them. (7161)
- If you update the appliance firmware while a Sensor Pod 155 (NBPD0155) is connected to the appliance, an extra leak rope sensor may appear. Unplug the Sensor Pod 155. When Sensor Pod 155 shows as disconnected, delete it and any extra or disconnected sensors. Then re-connect the Sensor Pod. (7106)

### Downstream Devices

- If you move a Camera Pod 165 from your company network (a remote connection) to the appliance's private network (a local connection), the camera pod does not appear in the Web UI of the appliance. You can perform a factory reset on the camera pod to fix the connection. See FAQ article FA369386 on [www.apc.com](http://www.apc.com) for details. (6230)
- 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)
- 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)
- Port forwarding does not work when a computer is connected to the appliance's Private LAN. To access the device's Web UI, enter its IP address directly in the URL address bar. To get a list of all downstream devices and their IP addresses, log on to your appliance and enter the following in your URL address bar: `https://appliance_ip_address/rest/discoveries`. (7028)

**(Continued)**

## Miscellaneous

- After updating the appliance firmware, StruxureWare Data Center Expert (DCE) may lose communication with the appliance (in the DCE **Device View**, the **Status** for your appliance will say **Failure**). To establish communication again, go to the appliance Web UI and navigate to **Settings > System > SNMP**.
  1. Under **SNMP Agent**, deselect **Enable**, then click **APPLY**.
  2. Under **SNMP Agent**, select **Enable**, ensure the SNMP settings are correct, then click **APPLY**.(6970)
- **Settings > System > SSL Certificate**: When creating a new self-signed certificate, you can enter a value for the Common Name (**CN**). If the **CN** does not match the appliance host name, a new certificate is generated with a **CN** that does match. The **CN** field will be read-only in a future release. You can change the host name in **Settings > System > Network Settings**. (7121)
- Administrators cannot edit their own profiles. (7126)
- **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.
- **Settings > System > User Store**: After you first configure the **User Store** settings, you can not disable the user store unless you enter values in all available fields. (6232)

**Wireless Applications (NBWC100U v1.1.1, NBWS100T/H v1.1.2)**

None—same as previous version.

# Miscellaneous

## Update the Appliance

1. Download the latest firmware version for free from the applicable product page of [www.apc.com](http://www.apc.com), [se.com](http://se.com), or [sxwhelpcenter.ecostruxureit.com](http://sxwhelpcenter.ecostruxureit.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 30 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](http://www.apc.com).