# NetBotz 4.x

## Security Handbook

**NBRK0450, NBRK0550, NBRK0570, NBWL0355, NBWL0455**

**TME18015**
**October 2022**

www.apc.com

# Legal Information

# Table of Contents

# Introduction

This guide documents security features for the APC™ Rack Monitor 570, 550, 450 and Room Monitor 455 and 355 appliances. It also provides the following:

- information on how the appliances communicate with other systems in order to help users identify possible methods of attack
- recommendations on how to configure and operate the device securely
- decommissioning instructions

For more information on the either appliance, see the *Release Notes*, *Installation and Quick Configuration Manuals*, and *User Guide* on the applicable product pages of www.apc.com. To find a product page, enter the model of your appliance in the search bar, then select the product from the provided list.

# Appliance Information

## Types of User Accounts

Each appliance has two standard types of user accounts:

- Use the **root** account for procedures that require using the Console Port (e.g., using a terminal emulator to specify network settings). Beginning with firmware v4.7.0, you must set the default password the first time you log on. You cannot change the default user name for the root account (**root**). The *root* account is not used for most functions and should be shared with as few people as possible. Ideally, only one person should have access to the *root* account.
- Use the **Administrator** account (**apc**) to log on to the Web UI after initial configuration. You can use Advanced View to create, edit, or delete other Administrator accounts.

Advanced View includes additional user accounts with limited access:

- **Application** user accounts have access to only the Navigation, Sensor Data and selected portions of the Information/Action panes. Application user accounts can view the Cameras, Graphs, Alerts, and About panes. This Privilege Set does not permit access to the Configuration pane or to the Appliance Log, Change Root Password, and Reboot Appliance Tool menu selections.
- **Application (with Alert Update)** accounts have access to only the Navigation, Sensor Data and selected portions of the Information/Action panes. User accounts configured with this privilege set can view the Camera, Graphs, Alerts, and About panes. The user can also resolve alert conditions for thresholds that are configured with the Return-To-Normal Requires User Input setting in their Advanced Settings. This privilege set does not permit access to the Configuration pane.
- **Sensor** accounts have access to only the Navigation, Sensor Data and selected portions of the Information/Action panes. User accounts configured with the Sensor Privilege Set can view the Cameras, Graphs, and About panes. This Privilege Set does not permit access to the Alerts pane, Configuration pane, or to the Appliance Log, Change Root Password, and Reboot Appliance Tool menu selections.
- **Sensor (no camera)** accounts have access to only the Navigation, Sensor Data and selected portions of the Information/Action panes. User accounts configured with the Sensor (No Camera) Privilege Set can view Graphs and About panes. This Privilege Set does not permit access to the Cameras pane, Alerts pane, Configuration pane, or to the Appliance Log, Change Root Password, and Reboot Appliance Tool menu selections.

# Protocol Security

The following sections describe where and how various protocols use encryption to protect your information.

**NOTE:** It is recommended that you use the most secure protocols available whenever possible. HTTPS is more secure than HTTP. SSL/TLS is more secure than STARTTLS. SNMPv3 is more secure than SNMPv1.

## Uses for Protocols with Security Features

| Protocol | Uses |
|---|---|
| Transport Layer Security (TLS) | |
| HTTPS: HyperText Transfer Protocol (HTTP) over TLS | View and manage the appliance through the Web UI client, Advanced View (AV), or Data Center Expert (DCE). HTTPS is enabled by default for the Web UI. However, HTTP is used for camera images and notifications for motion detection when using IP cameras. |
| Simple Mail Transfer Protocol (SMTP) over TLS | Send email to Mail Transfer Agents (MTAs). You can select SSL/TLS with varying levels of verification, or STARTTLS (**Use SSL if available** option) to optionally enable SMTP over TLS. If STARTTLS is selected, but the SMTP server or any intermediate server does not support encryption, the email is not encrypted.<br><br>If SSL/TLS is required, but the SMTP server does not support encryption, the email is not sent. However, if the email passes through multiple servers and only the first one supports encryption, the email is passed along to subsequent servers without encryption regardless of SSL/TLS requirements.<br><br>Never trust sensitive information to an email. |
| SNMPv3* | Monitor downstream devices and allow compatible software to manage the appliance. |
| ZigBee with Schneider Electric master Key and random session key | Facilitate communication between the Coordinator (NBWC100U) and the Wireless Sensor Network. Zigbee is the default communication protocol for wireless sensors. |

*SNMPv1 does not include security features.

# Transport Layer Security (TLS)

Transport Layer Security (TLS) is a protocol that uses certificates and algorithms to encrypt and decrypt information being passed between two parties on the Web. The NetBotz appliance supports TLS 1.1 and TLS 1.2. When the appliance provides options to use **SSL**, **SSL/TLS**, or **STARTTLS** (Use SSL if available), this enables TLS 1.1 and TLS 1.2.

## TLS Cipher Suites

A cipher suite is a set of algorithms used to encrypt information sent between two parties. Before communication starts, a key exchange algorithm is used to share a key. Each party uses the key to encrypt and decrypt shared data using an encryption algorithm. Both the strength of the algorithms and the size of the key contribute to the strength of the cipher suite (larger keys are more secure than smaller keys).

When communicating with another system over TLS, your appliance and the other system negotiate to use the cipher suite which both systems support and which provides the most security.

Your NetBotz appliance supports the following cipher suites, which are ordered from strongest (top) to weakest (bottom).

### TLS 1.2

| Hex code | Cipher Suite Name (OpenSSL) | Key Exchange | Encryption | Key Size (Bits) | Cipher Suite Name in Request for Commants (RFC) articles |
|---|---|---|---|---|---|
| xc014 | ECDHE-RSA-AES256-SHA | ECDH 256 | AES | 256 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA |
| xc013 | ECDHE-RSA-AES128-SHA | ECDH 256 | AES | 128 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA |
| x39 | DHE-RSA-AES256-SHA | DH 2048 | AES | 256 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA |
| x33 | DHE-RSA-AES128-SHA | DH 2048 | AES | 128 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA |
| x35 | AES256-SHA | RSA | AES | 256 | TLS_RSA_WITH_AES_256_CBC_SHA |
| x2f | AES128-SHA | RSA | AES | 128 | TLS_RSA_WITH_AES_128_CBC_SHA |

### TLS 1.1

| Hex code | Cipher Suite Name (OpenSSL) | Key Exchange | Encryption | Key Size (Bits) | Cipher Suite Name in Request for Commants (RFC) articles |
|---|---|---|---|---|---|
| xc014 | ECDHE-RSA-AES256-SHA | ECDH 256 | AES | 256 | TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA |
| xc013 | ECDHE-RSA-AES128-SHA | ECDH 256 | AES | 128 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA |
| x39 | DHE-RSA-AES256-SHA | DH 2048 | AES | 256 | TLS_DHE_RSA_WITH_AES_256_CBC_SHA |
| x33 | DHE-RSA-AES128-SHA | DH 2048 | AES | 128 | TLS_DHE_RSA_WITH_AES_128_CBC_SHA |
| x35 | AES256-SHA | RSA | AES | 256 | TLS_RSA_WITH_AES_256_CBC_SHA |
| x2f | AES128-SHA | RSA | AES | 128 | TLS_RSA_WITH_AES_128_CBC_SHA |

Abbreviations in these tables:

- AES: Advanced Encryption Standard
- DH: Diffie-Hellman algorithm
- ECDH: Elliptic-curve Diffie-Hellman
- SHA: Secure Hash Algorithm
- RSA: Rivest-Shamir-Adleman algorithm

## TLS Authentication for HTTPS

Your appliance is shipped with a self-signed certificate installed. You can replace this certificate with one signed by a Certificate Authority (CA). Each time you access the appliance through a Web browser, the browser checks for the following:

- The appliance's certificate is signed by a recognized Certificate Authority. Web browsers can recognize signatures from commercial Certificate Authorities (CAs) by comparing them to root certificates that are stored on the browser.

  **NOTE:** The Web browser will not initially recognize a self-signed certificate.
- The format of the certificate is correct.
- The certificate is within its designated start date and expiration date.
- The Domain Name specified when a user logs on matches the subject alternative name (SAN) or the common name (CN) if the SAN is not available in the appliance's certificate.

When the appliance's certificate is authenticated, most Web browsers display a small lock icon in the URL address bar. If the certificate is not authenticated, most browsers display a security warning and options to trust the appliance and proceed to the Web UI.

See for instructions to generate and install certificates. You can also instruct your Web browser to permanently accept the appliance's self-signed certificate. See your Web browser documentation for instructions.

**NOTE:** A CA-signed certificate is more secure than a self-signed certificate because it provides authentication in addition to encryption.

## TLS Authentication for SMTP

Your appliance is shipped with several root certificates for major CAs. When the appliance connects to an SMTP server, the server certificate is compared to these root certificates. If the server has a certificate the appliance does not recognize, communication with the server is blocked.

# Configure Certificates for Inbound Connections Using Advanced View

To install an SSL certificate In Advanced View, click **Configuration > SSL > Import Certificate**.

You can generate and install a self-signed certificate or install an X.509, Certificate Authority-signed (CA-signed) certificate. A CA-signed certificate is more secure than a self-signed certificate because it offers authentication.

**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.

**CA-signed 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 or use a wildcard. If your X.509 certificate or key is provided in binary, you must convert it to Privacy Enhanced Mail (PEM) format.

It is not possible to have more than one certificate installed. As soon as you install a new certificate, the existing certificate is deleted. The public key certificate needs to be concatenated with the private key and pasted into the provided window.

## Regenerate a Self-signed Certificate

To regenerate a self-signed certificate,

1. Click **Configuration > Network Interfaces** to open the **Edit Network Interface** dialog.
2. Write down or save the current hostname to a separate file.
3. Enter a new, temporary hostname and click **OK** to apply the change.
4. Reenter the original hostname and click **OK** to apply the change.

   **NOTE:** Changing the hostname will have no effect on a certificate that was installed manually previously using the SSL icon in Advanced View.

## Install an X.509 Certificate

To install an X.509 certificate, click **Configuration > SSL** to open the **SSL Certificate Configuration** dialog. Then copy and paste the certificate and key into the dialog.

The certificate and key must be in PEM format. Certificates begin with a header line and end with a footer line. For example:

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

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

-----END RSA PRIVATE KEY-----
```

The header line, the footer line, and all of the certificate and key content must be included in between the dashed lines.

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

**NOTE:** Once the certificate and key are installed the key will no longer be displayed in the window but it will exist on the system.

# ZigBee for the Wireless Sensor Network

Zigbee is a communication standard for wireless networks. NetBotz appliances use Zigbee to communicate with supported wireless sensors via a wireless coordinator. Communication between each Wireless Sensor and the Coordinator is encrypted using two different keys:

- A Master key programmed into each sensor. This is a Schneider Electric proprietary key, not the Zigbee Alliance's default global trust center link key.
- A Session key negotiated between each sensor and the coordinator. This key is used to encrypt all communication between that sensor and the coordinator.
- Wireless device auto-join is supported but disabled by default. By default, the user must join all wireless devices manually to the appliance through Advanced View.

# Communication Methods

The appliance can communicate with multiple devices and systems. The following tables summarize the different ways the appliance sends and receives information from external devices and systems.

**NOTE:** It is recommended that you use the most secure option available whenever possible. HTTPS is more secure than HTTP. SNMPv3 is more secure than SNMPv1. Encrypted options are always more secure than unencrypted/plain options.

Physical ports provide connections to sensors that form part of the NetBotz system.

### Physical Ports

| Type | Purpose |
|---|---|
| ALink | A-Link sensor input |
| Leak Rope | Leak rope sensor input |
| Door | Door sensor input |
| Handle | Rack handle sensor input |
| Universal sensor | Universal sensors include vibration, temperature, spot leak, dry contact, smoke, and 0–5 V. |
| Beacon | Beacon strobe light |
| Public Ethernet (10/100Network) | 10/100 Megabit (Mb) connection to a customer facing network |
| USB | Used to connect USB devices to the appliance, including a wireless coordinator (NBWC100U). |
| RS485 | ModBus serial interface for Building Management Systems and other ModBus management systems. |
| Voltage output | Provide 12 VDC or 24 VDC (75 mA) to a connected device. |
| Relay output | Used to control external devices. |
| 4–20 mA inputs | Input from custom sensors, including industry standard 4–20 mA sensors. |
| Serial/Console | Local connection to the console. |

Listening ports are non-physical ports on the appliance that wait, or "listen," for specific kinds of incoming information. TCP ports use Transmission Control Protocol, which facilitates more reliable information transfer between applications. UDP ports use User Datagram Protocol, which facilitates faster, lower bandwidth information transfer.

### Listening Ports

| Port | Protocol | Purpose |
|---|---|---|
| TCP 23 | Telnet | Remote command line (disabled by default) |
| TCP 80 | HTTP | WEB interface and Botzspeak (DCE and AV) (disabled by default since 4.7.0) |
| TCP 443 | HTTPS | WEB interface and Botzspeak (DCE and AV) |
| TCP 502 | Modbus | Communications with NetBotz appliance over Modbus-TCP (disabled by default) |
| UDP 161 | SNMPv1 or SNMPv3 | Disabled by default since 4.7.0. The user can enable either protocol if network management is needed. |

External systems can have physical or non-physical connections to the appliance.

### Communication with External Systems

| Device/system | Communication Method | Notes |
|---|---|---|
| Data Center Expert 7 and later | HTTP requests and responses (not encrypted) | Used to read and write configuration information and to retrieve sensor information using Botzspeak (a Schneider Electric proprietary protocol). |
| | HTTPS requests and responses (encrypted) | |
| EcoStruxure IT Gateway | HTTP requests and responses (not encrypted) | Used to read and write configuration information and to retrieve sensor information using Botzspeak (a Schneider Electric proprietary protocol). |
| | HTTPS requests and responses (encrypted) | |
| Camera pod 160 | USB | All communications occur over the hard wired USB connection. |
| Remote camera pods | HTTP requests and responses (not encrypted) | You can choose to use HTTP or HTTPS for the remote camera. |
| | HTTPS requests and responses (encrypted) | |
| Devices (Rack PDU, ATS, and UPS units) | SNMPv1 requests and responses | Retrieve sensor information from the device. |
| | SNMPv3 requests and responses | |
| Serial Console | Terminal input and output | Used to access the console locally. |
| Wireless Coordinator (NBWC100U) | Binary requests and responses | The Wireless Coordinator is plugged directly into the appliance USB port. It communicates with the wireless sensors and then passes all wireless sensor information to the appliance. There is no direct path to the IP connection. |
| Wireless Sensors | ZigBee requests and responses | |
| Web browser | HTTP(S) requests and responses | The Web UI is viewed through your Web browser. |
| Building Management System (BMS) | Modbus TCP | Read/write Modbus registers. This protocol does not include security features. |
| Email server (SMTP server) | Encrypted requests and responses | The SMTP server determines whether or not email messages are encrypted. |
| | SMTP requests and responses | |

# Recommendations for Secure Configuration and Maintenance

The security of your appliance depends on several factors:

- The environment in which the appliance is placed
- The configuration of the appliance
- User behavior

The following recommendations are measures to help you increase the confidentiality of your data and to decrease the likelihood of cyber-attacks or data loss.

## Environment

The appliance's environment consists of the physical setting in which it is placed and the network to which it is connected.

## Physical Security

Attackers with physical access to equipment can access your devices without authorization. To prevent physical attacks, secure the front panel of your device and deploy your devices in a secure location.

Recommendations to secure the front panel: Devices should be locked behind cabinets or protected by physical restraints that prevent unauthorized access or removal from restricted areas. Cabinets should be locked with a suitable key or other physical methods. Access to wires/cabling must also be secure.

Recommendations for secure locations:

- Clearly mark restricted areas for access to authorized personnel only.
- Secure restricted areas with locked doors.
- Only grant access to areas containing covered equipment to personnel who require access based on their job function.
- Ensure facilities containing covered devices give minimum indication of their purpose, with no obvious signs identifying the presence of related functions.
- Test physical access control devices (key card readers, doors and cabinet locks, etc.) prior to use and on a periodic basis (e.g., annually).
- If you are a resource custodian,
  - Produce physical or electronic audit trails to record all personnel's physical access to restricted areas for security incident investigation.
  - Regularly review who has physical access to control devices, and remove any inappropriate access identified during the review.
- If any sensor data is considered critical, use a wired sensor instead of a wireless one. Wired connections are less susceptible to interference than wireless connections.

## Network Configuration

NetBotz appliances are not configured with the security infrastructure to be placed on a public network, or on any network where unauthorized users can access the appliance. It is recommended that you connect your appliance to a Local Area Network (LAN) that meets the following requirements:

- Access to the LAN should be limited to appropriate parties using proper segmentation.
- A firewall should be placed between the LAN and the normal corporate network.

Authorized personnel should use a Virtual Private Network (VPN) to connect to the LAN from an external network.

# Appliance Configuration

## Installation and Password Use

The appliance can be installed by authorized APC employees or by the customer. There are no special installation credentials. The root and WEB accounts are set on first use. See the Installation and Quick Start Manual on www.apc.com for details.

There are no password strength requirements—this helps to avoid conflicts with local password rules. It is recommended that the installer and subsequent users set strong passwords that conform to their company's password standards.

## SNMP

SNMPv3 is more secure than SNMPv1. It is recommended that you use the most secure configuration of SNMPv3 possible for your system. The following SNMPv3 configurations are ordered from most to least secure:

- **AuthPriv:** authentication and encryption (most secure)
- **AuthNoPriv:** authentication but no encryption
- **noAuthNoPriv:** no authentication and no encryption (least secure)

The NetBotz 4.x implementation of SNMPv3 allows the use of the SHA-1 or MD5 protocol for authentication, and the implementation of AES-128 or DES protocols for encryption. It is recommended that you use the more secure protocols: SHA-1 and AES-128.

# User Behavior

## Accessing the Web UI

Web pages that you have recently accessed are saved in the cache of your Web browser and allow you to return to those pages without re-entering your user name and password. Always close your browser session before you leave your computer unattended. Also, log out of the appliance when you are finished using it. Consider setting your computer to run a password protected screen saver after a period of inactivity.

## Backup Files and Change Management

Prior to making any major configuration changes, it is recommended that you create a backup file of your configuration. Backup files may be encrypted by entering a password. It is recommended that you store backup files in a secure place, such as an encrypted computer with password requirements.

It is also recommended that you use good change management practices such as recording the actual changes to your configuration, who made them, and when they were made.

## Software Releases and Patch Management

All software for your appliance is updated with subsequent releases. There are no patch files. This is done purposely to ensure the integrity of the system. Updates are made available on www.apc.com.

## Customer Support Requests

If you choose to pay for support, you may request that a support person make modifications to the appliance configuration. In this case, it is recommended that you create a temporary Admin account and delete the account when it is no longer needed. A support person with an Admin account can make any needed changes. You should remove the account when it is no longer needed.

If you provide a support person with a Root or a normal user's WEB password, it is recommended that you change the password immediately after the support request is fulfilled.

# How to Report a Vulnerability

To report a vulnerability, please direct your submission to Technical Support at apc.com/supportse.com/ww/en/work/support/ and include the following information:

- Product line
- Vulnerable version
- Vulnerability type (CWE ID if available)
- Organization name
- Email
- Phone number
- Country

# How to Decommission the Appliance

1. Disconnect the appliance from the network.
2. Reset the appliance to its default settings. The reset procedure deletes sensor data, resets the database, removes configuration files, and restores the default configuration.
   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 34800 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 correct cable is being used as specified in sub-step **a**.
      - The terminal settings are correct as specified in sub-step **b**.
      - The serial port is not in use by another application.
      - 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 the current root password or alternatively power cycle the unit.
   e. When the system comes up, early on a count down timer will display (Hit any key to stop autoboot). Press a key to interrupt the count down.
   f. At the `NetBotz>` prompt, type `configreset` and press Enter.
   g. Once the `Hit any key to stop autoboot` prompt is displayed again, disconnect power from your appliance.
3. Remove the appliance from all management systems such as Data Center Expert or EcoStruxure IT.

APC
70 Mechanic Street
Foxboro, MA 02035
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.



TME18015