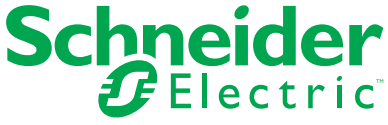
NetBotz 5.x

Security Handbook

NBRK0750, NBWL0755
Firmware v5.4.0

June 2024

990-6106F



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.

This document and its content are protected under applicable copyright laws and provided for informative use only. No part of this document may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the document or its content, except for a non-exclusive and personal license to consult it on an "as is" basis.

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.

Table of Contents

Introduction

This guide documents security features for the APC™ Rack Monitor 750 and Room Monitor 755 appliances. It also provides:

- 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 Manual*, and *User Guide* on the applicable product pages of www.apc.com.

Appliance Information

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.

Security Protocols

The following sections describe where and how various security 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 Security Protocols

Protocol	Uses
Transport Layer Security (TLS)	
HTTPS: HyperText Transfer Protocol (HTTP) over TLS	View and manage the appliance through the Web UI client or a custom REST API* client. HTTPS is enabled by default for the Web UI. However, HTTP is used for camera images and notifications for motion detection.
Simple Mail Transfer Protocol (SMTP) over TLS	Send email to Mail Transfer Agents (MTAs). You can select **SSL/TLS** or **STARTTLS** to optionally enable SMTP over TLS. Otherwise, SMTP is not encrypted. If **STARTTLS** is selected, but the SMTP server or any intermediate server does not support encryption, the email is not ecrypted. Never trust sensitive information to an email. If **SSL/TLS** is selected, but the SMTP server or any intermediate server does not support encryption, the email is not sent.
Lightweight Directory Access Protocol (LDAP) over TLS	Connect to directory services (or LDAP servers) to verify the existence of rack users. You can select **Use SSL** to optionally enable LDAP over TLS. Otherwise, LDAP is not encrypted over TLS.
Secure SHell (SSH)	SSH is required to access the console remotely. Telnet is not supported as an access method.
Secure CoPy (SCP) and Secure File Transfer Protocol (SFTP)	Transfer files to and from StruxureWare Data Center Expert®. SCP and SFTP are automatically enabled.
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 senors.

* Representational State Transfer Application Programming Interface (REST API). 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.

** SNMPv1 is not a security protcol.

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 1.2 and TLS 1.3. When the appliance provides options to use **SSL**, **SSL/TLS**, or **STARTTLS**, this enables TLS 1.2 and TLS 1.3.

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 1.3

Hex code	Cipher Suite Name (OpenSSL)	Key Exchange	Encryption	Key Size (Bits)	Cipher Suite Name in Request for Commants (RFC) articles
x1302	TLS_AES_256_GCM_ SHA384	ECDH 256	AESGCM	256	TLS_AES_256_GCM_SHA384
x1301	TLS_AES_128_GCM_ SHA256	ECDH 256	AESGCM	128	TLS_AES_128_GCM_SHA256
x1303	TLS_CHACHA20_ POLY1305_SHA256	ECDH 256	ChaCha20	256	TLS_CHACHA20_POLY1305_SHA256

TLS 1.2

Hex code	Cipher Suite Name (OpenSSL)	Key Exchange	Encryption	Key Size (Bits)	Cipher Suite Name in Request for Commants (RFC) articles
xc030	ECDHE-RSA-AES256-GCM-SHA384	ECDH 570	AES-GCM	256	TLS_ECDHE_RSA_WITH_AES_256_GCM_ SHA384
xcca8	ECDHE-RSA-CHACHA20-POLY1305	ECDH 521	ChaCha20	256	TLS_ECDHE_RSA_WITH_CHACHA20_ POLY1305_SHA256
xc02f	ECDHE-RSA-AES128-GCM-SHA256	ECDH 570	AES-GCM	128	TLS_ECDHE_RSA_WITH_AES_128_GCM_ SHA256
x9f	DHE-RSA-AES256-GCM-SHA384	DH 2048	AES-GCM	256	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
xccaa	DHE-RSA-CHACHA20-POLY1305	DH 2048	ChaCha20	256	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_ SHA256
x9e	DHE-RSA-AES128-GCM-SHA256	DH 2048	AES-GCM	128	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
xc028	ECDHE-RSA-AES256-SHA384	ECDH 570	AES	256	TLS_ECDHE_RSA_WITH_AES_256_CBC_ SHA384
xc027	ECDHE-RSA-AES128-SHA256	ECDH 570	AES	128	TLS_ECDHE_RSA_WITH_AES_128_CBC_ SHA256
x6b	DHE-RSA-AES256-SHA256	DH 2048	AES	256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
x67	DHE-RSA-AES128-SHA256	DH 2048	AES	128	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

Abbreviations in these tables:

- AES: Advanced Encryption Standard
- AES-GCM: AES in Galois/Counter Mode (GCM)
- CHACHA: The name of an algorithm (not an abbreviation)
- DH: Diffie-Hellman algorithm
- ECDH: Elliptic-curve Diffie-Hellman
- POLY: Polyalphabetic (a kind of cipher)
- 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 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 common name 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 Configure Certificates for Inbound Connections, page 10 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 since it provides authentication in addition to encryption.

TLS Authentication for SMTP and LDAP

Your appliance is shipped with several root certificates for major CAs. When the appliance connects to an SMTP or LDAP 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.

If you need to access a server with an unrecognized certificate, you can add the necessary root certificate to the appliance's trust store.

See Configure Certificates for Outbound Connections, page 11 for instructions to add a root certificate to the trust store in the Web UI.

Configure Certificates for Inbound Connections

Path: Settings > System > SSL Certificate

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.

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 .

Secure SHell (SSH) for Remote Access to the Command Line

The Secure SHell protocol (SSH) provides a mechanism to access computer consoles, or shells, remotely. The protocol authenticates the appliance and encrypts all transmissions between the SSH client and the appliance.

- SSH is a more secure alternative to Telnet. Telnet does not provide encryption.
- SSH helps protect the user name and password, which are the credentials for authentication, from being used by anyone intercepting network traffic.
- To authenticate the appliance to the SSH client, SSH uses a host key unique to each unit. The host key is an identification that cannot be falsified, and it prevents an invalid entity on the network from obtaining a user name and password by presenting itself as a valid entity.

The appliance uses SSHv2, which helps to protect the appliance from attempts to intercept, forge, or change data during transmission.

Secure CoPy (SCP) and Secure File Transfer Protocol (SFTP)

SCP and SFTP are file transfer protocols that use SSH for encryption of user names, passwords, and files.

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.

NetBotz does not support auto-join. The user must join all wireless devices to the appliance through the Web UI.

Password Storage

The appliance does not have encryption hardware. All passwords are stored in a database on the appliance using encryption algorithms.

The Root password is salted and then hashed using SHA512 (Secure Hash Algorithm 512). A secure hash is a one-way function (a function that cannot be reversed) that transforms the password into a different set of characters. Salting is the process of adding random data to that password to further confuse attempts to decrypt the password or guess at the hashed password.

Web UI passwords for Super User and Admin accounts are stored using Password-based Key Derivative Function 2 with Hash-based message authentication code SHA256 (PBKDF2WithHmacSHA256).

SNMPv3 passphrases must be stored in a recoverable format (not hashed), so these are also stored using reversible encryption.

Network Address Translation and Port Forwarding

Network Address Translation (NAT) is a configuration where the appliance uses multiple dynamic IP addresses to facilitate communication between downstream devices (devices connected to the Private LAN port) and the public network. In this configuration, all data packets sent to and from connected devices are passed through the appliance. When unsolicited packets are sent to a device, the appliance automatically rejects them. This helps increase the security of the devices.

When Port Forwarding is enabled, the appliance assigns a static IP address to connected devices. This allows you to access the device's Web UI from the Appliance (see the *User Guide* for details). However, while a device's web UI is open, the appliance allows unsolicited packets to reach the device. It is recommended that you keep port forwarding off when possible to increase the security of your downstream devices.

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 (10/100/100 Network)	10/100/1000 Megabit (Mb) connection to a customer facing network
Private Ethernet (Private LAN)	10/100/1000 Mb connection to a private network. DHCP services (for example, automatic network configuration) are supported.
USB	One port is used to connect the wireless coordinator (NBWC100U). The other two ports are reserved for future use.
ModBus	Reserved for future use.
Voltage output	Provide 12 VDC or 24 VDC (75 mA) to a connected device.
Relay output	Used to control external devices.
Custom sensor	Input from custom sensors, including industry standard 4–20 mA sensors.
Serial	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 502	Modbus	Disabled by default. The user can enable Modbus TCP if required and can select an alternatively unused port. **NOTE:** Switching the port to a different number does not impact security.
TCP 22	SSHv2	Used to access the console remotely and transfer files over SCP or SFTP.
TCP 80, TCP 443, HTTPS, Appliance Web Server	HTTP	Redirects users to HTTPS (port 443).
UDP 161	SNMPv1 or SNMPv3	Disabled by default. The user can enable either protocol if network management is needed.
TCP 8011	HTTP	Receives event notifications from Camera Pods
TCP 51XX	HTTP or HTTPS	Access to Web UIs for downstream devices through the Port Forwarding feature. Disabled by default. The appliance checks for HTTPS first and HTTP second. The protocol used depends on the settings for your downstream devices.

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

Communication with External Systems

Device/system	Communication Method	Notes
StruxureWare Data Center Expert 7 and later	SCP requests and responses	Used for file transfers
	HTTPS requests and responses	Used to transport images from the Camera Pod 165 over REST
	SNMPv1 requests and responses	Retrieve sensor information from the appliance. Only one SNMP version can be used at a time.
	SNMPv3 requests and responses	
EcoStruxure IT	SCP requests and responses	Used for file transfers
	SNMPv1 requests and responses	Retrieve sensor information from the appliance. Only one SNMP version can be used at a time.
	SNMPv3 requests and responses	
LDAP servers	Encrypted requests and responses	Used to check for the existence of a user. Select **USE SSL** in the Web UI to enable encrypted requests and responses. Your LDAP server must be configured to support encryption.
	Plain requests and responses	
Downstream Camera Pod 165 or compatible ONVIF cameras	HTTP requests and responses (not encrypted)	HTTP is used for a Physical (local) connection. Over a remote connection, you can choose to use HTTP or HTTPS. However, if you choose HTTPS, camera images and notifications for motion detection are still transmitted over HTTP for best performance.
	HTTPS requests and responses (encrypted)	

Communication with External Systems (Continued)

Device/system	Communication Method	Notes
Downstream Devices (Rack PDU, ATS, and UPS units)	SNMPv1 requests and responses	Retrieve sensor information from the device.
	SNMPv3 requests and responses	
	HTTP requests and responses (not encrypted)	Access to Web UIs for downstream devices. The protocol depends on the settings for your downstream devices.
	HTTPS requests and responses (encrypted)	
REST API client	HTTP requests and responses	The REST API client is used by your Web browser. Users with web design experience can also use the REST API to create a custom UI.
SSH Client	Terminal input and output	A program that uses SSH to access the console remotely. For example, PuTTY or TeraTerm.
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. It communicates with the wireless sensors and then passes all wireless sensor information to the appliance.
Wireless Sensors	ZigBee requests and responses	
Web browser	HTTPS requests and responses	The Web UI is viewed through your Web browser.
Email server (SMTP server)	Encrypted requests and responses	The SMTP server determines whether or not email messages are encrypted.
	SMTP requests and responses	
Building Management System (BMS)	Insecure TCP	Modbus TCP is inherently insecure and NetBotz currently only supports read-only registers. It is recommended that you provide both network security and physical security when using Modbus TCP. Use network Firewalls and Segmentation. Restrict physical access to cabling and devices.

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.

Recommendations for secure locations

- Restricted areas should be clearly marked for authorized personnel only.
- Restricted areas should be secured by locked doors.
- Access to areas containing covered equipment should only be granted to personnel who require access based on their job function.
- Facilities containing covered devices should give minimum indication of their purpose, with no obvious signs identifying the presence of related functions.
- Physical access control devices, such as key card readers, doors and cabinet locks, should be tested prior to use and on a periodic basis (e.g. annually).

  NOTE: The Mifare Classic card format is vulnerable to cloning. If you use this format, maintain the physical security of your access cards. Consider updating to the Mifare Plus format.
- Resource custodians should produce physical or electronic audit trails to record all personnel's physical access to restricted areas for security incident investigation. Inventory of who has physical access to control devices should be regularly reviewed, and any inappropriate access identified during the review should be promptly removed.
- Physical security of the cabling should be considered when insecure protocols are used such as Modbus TCP.

  NOTE: 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.
- 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.

Virtual LANs (VLANS) are not secure because all network traffic exists on the same networking equipment. If an attacker has access to the equipment, they can observe the network traffic.

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 Super User accounts both come with default passwords that must be changed 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. In order from most to least secure, these are

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

The NetBotz 5.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.

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 are not encrypted. 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 the APC website, 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 except for performing a reset to factory defaults or setting passwords for other Admin accounts. You should remove the account when it is no longer needed

If you provide a support person with a Root or Super User password, it is recommended that you change the password immediately after the support request is fulfilled.

Vulnerability Reporting and Management

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

Decommissioning

In the event that a NetBotz appliance must be decommissioned:

1. Disconnect the appliance from the network.
2. Reset the appliance to its default settings.
   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 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.)
   d. Log on with the Root account user name (**root**) and password (you set the password on first use).
   e. Enter the following command: `/netbotz_app/factory_reset.sh`. Wait for it to complete.
   f. Disconnect power from your appliance.

   The reset to defaults deletes video and sensor data, resets the database, removes configuration files, and restores the default configuration. This procedure does *not* wipe the onboard SD card.

   NOTE: You can also perform a reset to defaults while connected to the Network (see the *User Guide* for details). However, performing the reset to defaults while disconnected from the network prevents the appliance from saving your IP address.
3. Remove the appliance from management systems (for example, EcoStruxure Data Center Expert and 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.

© 2019 – 2024 APC. All rights reserved.

990-6016F