NetBotz 5.x

Security Handbook

NBRK0750

990-6106A-001
Release date: 10/2019

APC™
by Schneider Electric

Legal Information

Table of Contents

Introduction

This guide documents security features for the APC by Schneider Electric NetBotz® Rack Monitor 750. It also provides:

- information on how the Rack Monitor 750 (the appliance) communicates with other systems in order to help users identify possible methods of attack
- recommendations on how to configure and operate the device securely

For more information on the Rack Monitor 750, see the *Release Notes*, *Installation and Quick Configuration Manual*, and *User Guide* on *www.apc.com.*

Security Protocols

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

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 **Use SSL** to optionally enable SMTP over TLS. Otherwise, SMTP is not encrypted over TLS. If **Use SSL** 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.
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.
SNMP (version 1 or 3)	Establish communication with downstream devices.
ZigBee with APC by 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.

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 uses TLS v1.2. When the appliance provides options to **Use SSL**, this enables 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).

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
xc028	ECDHE-RSA-AES256-SHA384	ECDH 570	AES	256	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
x9f	DHE-RSA-AES256-GCM-SHA384	DH 2048	AES-GCM	256	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
x6b	DHE-RSA-AES256-SHA256	DH 2048	AES	256	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
xc02f	ECDHE-RSA-AES128-GCM-SHA256	ECDH 570	AES-GCM	128	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
xc027	ECDHE-RSA-AES128-SHA256	ECDH 570	AES	128	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
x9e	DHE-RSA-AES128-GCM-SHA256	DH 2048	AES-GCM	128	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
x67	DHE-RSA-AES128-SHA256	DH 2048	AES	128	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

Abbreviations in this table:

- DH: Diffie-Hellman algorithm
- ECDH: Elliptic-curve Diffie-Hellman
- AES: Advanced Encryption Standard
- AES-GCM: AES in Galois/Counter Mode (GCM)
- SHA: Secure Hash 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 that:

- 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 the *User Guide* on *www.apc.com* 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.

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 the *User Guide* on *www.apc.com* for instructions to add a root certificate to the trust store.

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. In NetBotz appliances, communication between each Wireless Sensor and the Coordinator is encrypted using two different keys:

- A Master key programmed into each sensor, and
- A Session key generated for communication between each sensor and the coordinator

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.

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 22	SSHv2	Used to access the console remotely and transfer files over SCP or SFTP.
TCP 80	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)	
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.

Communication with External Systems (Continued)

Device/system	Communication Method	Notes
	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	

Recommendations for Secure Configuration and Maintenance

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.

Installation and Password Use

The appliance can be installed by authorized Schneider Electric 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.

Network Configuration

NetBotz appliances are not configured with the security infrastructure to be placed on the Web or on a public network. 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.

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.

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 by Schneider Electric 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.

APC by Schneider Electric
132 Fairgrounds Rd
02892 West Kingston, RI
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.

990-6016A-001