

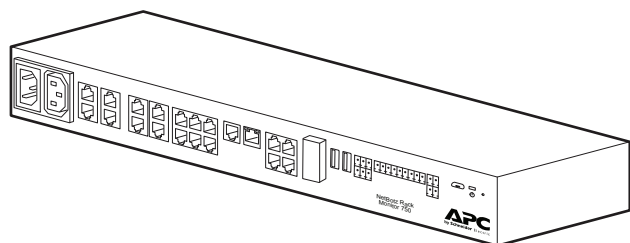
NetBotz 5.x

User Guide

NBRK0750

990-5934C-001

Release date: 08/2019



Legal Information

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this guide are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owners.

This guide and its content are protected under applicable copyright laws and furnished for informational use only. No part of this guide 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 guide or its content, except for a non-exclusive and personal license to consult it on an "as is" basis. Schneider Electric products and equipment should be installed, operated, serviced, and maintained only by qualified personnel.

As standards, specifications, and designs change from time to time, information contained in this guide may be subject to change 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 material or consequences arising out of or resulting from the use of the information contained herein.

APC, the APC logo, NetBotz, and StruxureWare are trademarks owned by Schneider Electric SA. All other trademarks are property of their respective owners.

Table of Contents

Preface.....	7
US Government Restricted Rights	7
Improper Use of Audio/Visual Recording Capabilities	7
Introduction.....	8
Updates and Additional Documentation	8
Security Recommendations	9
Types of User Accounts	9
Physical Description	10
Link (10/100/1000) LED	11
Status LED	11
Getting Started.....	11
Establish Network Settings.....	12
Access the Web User Interface (Web UI).....	14
Reset a Lost Root Account Password	14
Reset a Lost Super User Password.....	15
Reset to Defaults.....	15
Network Management with Other Applications	15
Web UI Features.....	16
Tabs.....	16
Quick Status Icons and the Quick Status Area	16
Quick Links.....	17
Details Windows	17
Overview Tab	18
Customize 4–20 mA Sensors	19
Control Devices by Outlet	19
Configure the Camera Pod Settings.....	19
Remove a Wired Device	20
Remove a Camera	20
Remove a Wireless Sensor.....	20
Alarms Tab.....	21
Clip Capture	21
Pagination	21
Devices Tab.....	22
Connect Downstream Devices	23
Add a Remote Camera	24
Discover an Assigned Camera Password	24
Rack Access Tab	25
Register a Proximity Card	26
Schedule Rack Access	27
Wireless Tab.....	28
The Wireless Sensor Network	29
Devices on the Wireless Sensor Network	29
Connect the Wireless Sensor Network	30

Add Sensors to the Wireless Sensor Network.....	30
Update the Wireless Sensor Network.....	31
Remove a Wireless Sensor.....	31
Settings Tab.....	32
Configure Notification Policies.....	32
Configure Alarms.....	33
Configure System Settings.....	35
Enable DCE Surveillance.....	35
Configure Date and Time Settings.....	36
Configure Discovery Settings for Downstream Devices.....	37
Set Identification Information.....	37
Configure Log Settings.....	38
Configure Network Settings.....	38
Configure a Proxy Server.....	39
Set Global Auto Lock Timeout.....	39
Configure an SMTP Server.....	40
Configure SNMP Settings.....	41
Configure Certificates for Inbound Connections.....	42
Configure Certificates for Outbound Connections.....	43
Configure LDAP Settings for Rack Access.....	43
Configure Video Capture Settings.....	44
Set Wireless Update Settings.....	44
View and Edit User Accounts.....	44
Update the Appliance Firmware.....	45
Backup and Restore System Settings.....	45
Save a Backup File.....	45
Restore System Settings.....	47
Configure New Appliances from a Backup File.....	47
View Appliance Information.....	47
REST API.....	48
Using the API.....	48
Operations.....	49
alarms.....	49
appliance.....	54
assets.....	55
cameras.....	59
configuration.....	63
directory.....	64
discoveries.....	68
firmwareupdate.....	72
logging.....	72
notifications.....	73
ping.....	75
rackaccess.....	76
session.....	80
settings/dceconfig.....	81
settings/dceregistration.....	83

settings/defaultCredentials	84
settings/identification	87
settings/iptables	87
settings/mail	88
settings/network	90
settings/proxy	90
settings/remotelogging	93
settings/snmpagent	94
settings/snmptrap	96
settings/ssl	98
settings/timedate	100
settings /trust-store	102
users	103
wireless	105
Troubleshooting	109
Access Issues	109

Preface

US Government Restricted Rights

Restricted rights legend. Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs (c) (1) and (2) of the Commercial Computer Software- Restricted Rights clause at CFR 52.227-19, as applicable.

Improper Use of Audio/Visual Recording Capabilities

Attention: THE EQUIPMENT CONTAINS, AND THE SOFTWARE ENABLES, AUDIO/VISUAL AND RECORDING CAPABILITIES, THE IMPROPER USE OF WHICH MAY SUBJECT YOU TO CIVIL AND CRIMINAL PENALTIES. APPLICABLE LAWS REGARDING THE USE OF SUCH CAPABILITIES VARY BETWEEN JURISDICTIONS AND MAY REQUIRE AMONG OTHER THINGS EXPRESS WRITTEN CONSENT FROM RECORDED SUBJECTS. YOU ARE SOLELY RESPONSIBLE FOR ENSURING STRICT COMPLIANCE WITH SUCH LAWS AND FOR STRICT ADHERENCE TO ANY/ALL RIGHTS OF PRIVACY AND PERSONALTY. USE OF THIS SOFTWARE FOR ILLEGAL SURVEILLANCE OR MONITORING SHALL BE DEEMED UNAUTHORIZED USE IN VIOLATION OF THE END USER SOFTWARE AGREEMENT AND RESULT IN THE IMMEDIATE TERMINATION OF YOUR LICENSE RIGHTS THEREUNDER.

Introduction

The APC by Schneider Electric NetBotz™ Rack Monitor 750 is a rack-mountable central hardware appliance for an environmental monitoring and control system. Once the system is installed, you can monitor and control your system using the Web User Interface (Web UI) or Representational State Transfer Application Programming Interface (REST API). This manual describes how to use the interfaces of a NetBotz Rack Monitor 750 (NBRK0750) to configure settings on your appliance, and how to use your appliance to monitor the environment and attached sensors and devices. (See the *Installation and Quick Configuration Manual* on www.apc.com for information on supported devices.)

NOTE: 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.

The NetBotz Rack Monitor 750 has these additional features:

- Various levels of access: Super User and Administrator. (These are protected by user name and password requirements.)
- Configurable alarm thresholds that provide network and visual alarms to help avoid and address environmental risks.
- E-mail notifications for system events.
- SNMP traps, Syslog messages, and e-mail notifications based on the severity level of system events.
- Multiple user logon feature which allows up to four users to access the appliance simultaneously.
- Event logging.
- Security protocols for authentication and encryption.

Updates and Additional Documentation

You can find updates to this document, firmware updates, and these additional documents on the applicable product page of www.apc.com:

- *Installation and Quick Configuration Manual*: Provides instructions to install the appliance and initial setup of TCP/IP
- *Release Notes*: Provides lists of new features, fixed issues, and known issues for the latest firmware version.
- *Security Handbook*: Describes security features and options for the appliance.

To quickly find a product page, enter the part number of your product in the Search field on www.apc.com.

Security Recommendations

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 take the following steps to protect your appliance:

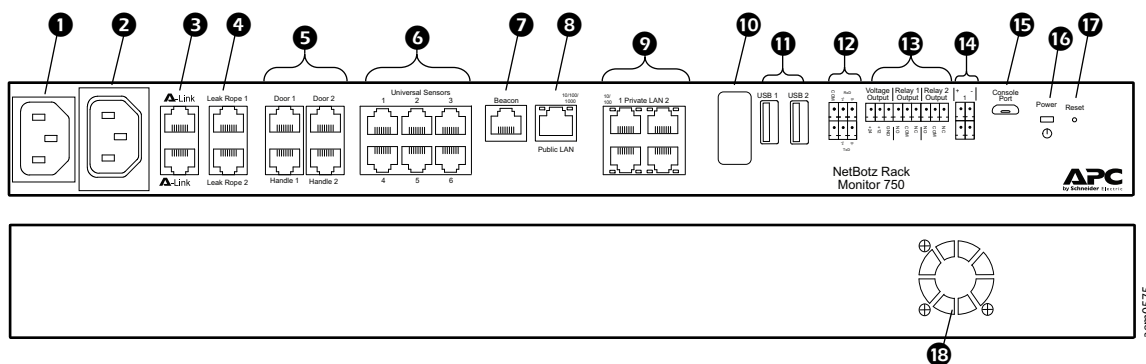
- Connect your appliance to a private network with an appropriate level of access for authorized users.
- Connect your appliance to a subnetwork that is partitioned from your company's corporate network.
- Place a firewall between the appliance's LAN and your company's corporate network.
- Require authorized personnel to use a VPN when connecting to the network the appliance is on.
- Place the appliance in a physical environment where only authorized personnel have access to it.
- If you allow a customer support representative to make changes to your appliance, it is recommended that you create a temporary account for the support representative and remove the account when it is no longer needed.

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., when you use a terminal emulator to specify network settings. You set the default password the first time you log on. You can not change the default user name (**root**).

Physical Description



Item	Description	
1	AC line inlet	Input power connection.
2	Switched Outlet	Provides power to a device at a maximum of 10 A. Activates a connected device when configured events occur. (For example, a fan may be connected to this outlet, and the outlet may be configured to turn on when certain alarms are generated.)
3	A-Link ports	Provide communications and power to connected devices (sensor pods, rack access pods, and temperature/humidity sensors with digital displays) over standard CAT-5 cabling with straight-through wiring. For instructions to cascade devices, see the <i>Installation and Quick Configuration Manual</i> on www.apc.com .
4	Leak Rope port	Used for connecting a NetBotz Leak Rope Sensor (NBES0308).
5	Rack Access Ports*	Ports for the door switch sensors (NBES0302 or NBES0303) and handle sensors (NBHN125 or NBHN1356).
6	Universal Sensor ports	Used to connect APC by Schneider Electric sensors, third-party dry-contact sensors, and standard, third-party 0–5 V sensors. Third-party, dry-contact state sensors require the NetBotz Dry Contact Cable (NBES0304), and third party, 0–5 V sensors require the NetBotz 0–5 V sensor cable (NBES0305).
7	Beacon port	Used for connecting an Alarm Beacon (AP9324).
8	10/100/1000 Network port	Provides a connection to the network. Status and link Light-emitting Diodes (LEDs) indicate network traffic. See <i>Link (10/100/1000) LED</i> , page 11 and <i>Status LED</i> , page 11 for details.
9	Private LAN	Provides a 10/100/1000 connection to a private local area network and 48 VDC to an attached device.
10	Wireless Sensor Coordinator	USB Port with Wireless NetBotz USB Coordinator (NBWC100U) installed. Used with wireless sensors.
11	USB Type A ports	Reserved for future use.
12	Modbus RS485 port	Reserved for future use.
13	Voltage Output	Provides 12 VDC or 24 VDC (75 mA) to one connected device.
	Relay Output ports 1, 2	Used for connecting relay-controlled external devices. Relay Outputs can only be connected to Class 2 circuits.
14	4–20 mA Inputs	Inputs for industry standard 4–20 mA sensors.
15	Console port	Provides a serial connection to the appliance.
16	Power LED	Illuminates when the unit is receiving power.
17	Reset switch	Reboots the appliance.
18	Exhaust fan	Exhausts hot air from the appliance.

*Not supported on firmware version 5.0.1. Update the firmware to access these features. See *Update the Appliance Firmware*, page 45 for instructions to update the firmware.

Link (10/100/1000) LED

The LED on the right of any network port indicates the network status.

Condition	Description
Off	One or more of the following situations exist: <ul style="list-style-type: none"> The appliance is not receiving input power. The cable that connects the appliance to the network is disconnected or not functioning properly. The appliance is turned off or not operating correctly. It may need to be repaired or replaced. Contact Customer Support at www.apc.com/support.
Solid green	The appliance is connected to a network operating at 100 Megabits (Mb) per second or 1000 Mb/1Gigabit (Gb) per second.
Solid orange	The appliance is connected to a network operating at 10 Mb per second.
Flashing green	The appliance is receiving or transmitting data packets at 1 Gb per second.
Flashing orange	The appliance is receiving or transmitting data packets at 10 Mb or 100 Mb per second.

Status LED

The LED on the left side of any network port indicates the status of the appliance.

Condition	Description
Off	One of the following situations exists: <ul style="list-style-type: none"> The appliance is not receiving input power. The appliance is not operating properly. It may need to be repaired or replaced. Contact Customer Support at www.apc.com/support.
Alternately flashing green and amber	The appliance is waiting for a DHCP server to assign a valid IP address.
Solid green	The appliance is on and has a valid IP address.

Getting Started

To start using your NetBotz appliance,

1. Install and apply power to the appliance using the *Installation and Quick Configuration Manual* shipped with your appliance. (You can also find the *Installation and Quick Configuration Manual* on www.apc.com.)
2. Establish network settings.
3. Access the Web UI of the appliance.

Establish Network Settings

You must configure the following TCP/IP settings before the appliance can operate on a network:

- IP address of the appliance
- Subnet mask
- Default gateway
- At least one IP address for a Domain Name System (DNS) server

By default, your appliance uses Dynamic Host Configuration Protocol (DHCP) to configure network settings. When you apply power to the appliance, it automatically attempts to contact a DHCP server. You can use a computer to view or configure network settings. If needed, you can also view or configure network settings with a terminal emulator.

Use Your Computer to Establish Network Settings

NOTE: This procedure is only for Windows operating systems.

1. Ensure your computer is set to obtain network settings via DHCP. Connect a network cable from your computer to one Private LAN ports on the appliance.
2. Use the Public LAN port to connect your appliance to the network.
3. Open a command prompt and enter the following two commands:


```
ipconfig /release
ipconfig /renew
```
4. The command prompt should provide an IP, subnet mask, and default gateway. Open a Web browser and enter the default gateway in the URL address bar.
5. Use the default user name and password (both are **superuser**) to log on to the appliance, and change the password when prompted. It is recommended that you use a strong password that complies with your company's password requirements.
6. Go to **Settings > System > Network** to view or configure the network settings for your appliance.

Setting	Description
Static	Select Static to manually configure your Network settings. This setting assigns a static IP address to the appliance.
DHCP	Use a DHCP server to configure network settings automatically. This setting assigns a dynamic IP address to the appliance.
Hostname	The host name of the appliance.
TCP/IP	
IP Address	The IP address of the appliance. Use the format xxx.xxx.xxx.xxx.
Subnet Mask	The subnet mask of the appliance.
Gateway	The IP address of the default gateway.
DNS	
Primary	The IP address of the primary DNS server
Secondary	The IP address of the secondary DNS server
Tertiary	The IP address of the tertiary DNS server

Use a Terminal Emulator to Establish Network Settings

1. Connect a USB-A to Micro USB-B cable to the Console Port on the NetBotz appliance and a USB port on your computer.
2. Use a PoE-ready ethernet cable to connect the appliance to power.
Plug the power cord provided with your appliance into a wall outlet, and then connect it to the AC line inlet.

The green Power LED illuminates. The appliance can take up to two minutes to initialize, depending on configuration settings.
3. 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.
4. 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.)
5. Log on with the Root account user name (**root**) and password (you set the password on first use).
6. Configure your appliance to use network settings assigned by a DHCP server, or provide an IP address, subnet mask, gateway address, and at least one IP address for a DNS server.
7. Save your configuration settings, and close the terminal emulator.
8. Test the IP connection of the appliance: start your Web browser and type the IP address of the appliance into the URL address bar. Press **Enter**. If the appliance is online and properly configured, the Web UI displays in the browser window.

Access the Web User Interface (Web UI)

After the network settings are configured, you can access the appliance through the Web UI. The Web UI provides a real-time overview of alerts and device details, including sensor readings and images captured by cameras. You can use Microsoft Internet Explorer® (IE) 11 or the latest version of Google Chrome® or Mozilla Firefox® on Windows® 7 and 10 operating systems to access the appliance through its Web UI. Other commonly available browsers and operating systems may work but have not been fully tested.

NOTE: The Web UI takes about six minutes to become available after start-up.

NOTE: Video from Camera Pod 165 units does not appear in IE 11.

1. Enter the host name or IP address of the appliance in the Web browser's URL address bar. (If you used DHCP to automatically obtain the IP address of the appliance, you can use a terminal emulator to view your current IP address. Follow steps 1-4 of *Use Your Computer to Establish Network Settings, page 12* or 1-5 of *Use a Terminal Emulator to Establish Network Settings, page 13*.) You may receive a message that the Web page is not secure. This is normal when using a self-signed certificate (the default), and you can continue to the Web UI.

NOTE: Your appliance comes with a self-signed certificate installed. Browsers generate a security warning because they do not recognize the authority who signed the certificate. You can prevent the warning message by installing a certificate signed by a Certificate Authority (CA) the Web browser recognizes (see *Configure Certificates for Inbound Connections, page 42* for more information). You can also direct the browser to accept the certificate to prevent the warning.

2. Use your user name and case-sensitive password to log on. The default user name and password for the Super User are both **superuser**. The Super User must define the user name and password for Administrators.

Both the Super User and Administrators must change their passwords at first log on. Use strong passwords that comply with your company's password requirements.

Reset a Lost Root Account Password

1. Connect a USB-A to Micro USB-B cable to the Console Port on the NetBotz appliance and a USB port on your computer.
2. Disconnect and reconnect power to the appliance. Immediately press any key on your computer. If you do not press a key within five seconds after you connect power to the appliance, the appliance will restart normally.
3. Enter the following three commands:

```
env set resetpwd true
env save
boot
```

Wait for the system to restart.

4. Log on as the Root user. When prompted, reset the Root account password.
5. Disconnect and reconnect power to the appliance. Immediately press any key on your computer. If you do not press a key within 5 seconds after you connect power to the appliance, the appliance will restart normally.
6. Enter the following three commands:

```
env set resetpwd false
env save
boot
```

Wait for the system to restart.

NOTE: If you do not complete steps 5 and 6, the root password will be reset every time the appliance restarts.

Reset a Lost Super User Password

1. Connect to the appliance with SSH or through the console port on your computer. Log on with the root account user name and password, then press **Shift + x Enter** within 5 seconds of logging on.
2. Navigate to `/netbotz_app` and enter the following command:

```
./restart.sh stop startApp startClubber resetsupwd
```

The appliance restarts.
3. Log on to the appliance as the Super User (both the user name and password are **superuser**).
4. Change the default password.

Reset to Defaults

This procedure reboots the appliance and resets all system settings (including passwords) to factory defaults.

NOTE: This procedure causes the appliance IP address to be reset. In some cases, you may lose access to the appliance and may need to use a local connection to reset or rediscover the IP address.

1. Log into the Web UI as the Super User.
2. Open a new browser page, type `<your appliance's IP address>/rest/appliance/resetconfig` in the URL address bar, the press **Enter**.

Example: `10.218.123.234/rest/appliance/resetconfig`

The appliance takes about six minutes to restart completely. Until the restart is complete, the Web UI is not available.

3. If needed, see *Use Your Computer to Establish Network Settings, page 12* or *Use a Terminal Emulator to Establish Network Settings, page 13* for instructions to discover or change the IP address.

The next time you log on to the appliance, you must reset the Super User password.

Network Management with Other Applications

You can also manage the appliance with the following applications:

- StruxureWare Data Center Expert® (DCE): Provide enterprise-level power management and management of agents, Rack PDUs, and environmental monitors. See *Enable DCE Surveillance, page 35* for more information.

Web UI Features

The following features can be found throughout the Web UI.

Tabs

The following tabs are available:

- **Overview:** The default tab when you log on. View all devices attached to the appliance.
- **Alarms:** View detailed information about alarms. Filter information by alarm and status.
- **Devices:** View detailed information for all downstream devices.
- **Rack Access:** View detailed information for rack access devices and register individual rack access users.
- **Wireless:** View detailed information for all wireless devices, add or remove a wireless sensor, and update the wireless sensor network.
- **Settings:** Configure appliance settings including notifications, alarms, network settings, and user accounts. Update the firmware and create backup files.

Quick Status Icons and the Quick Status Area

Quick status icons indicate the severity of alarms. They appear next to alarms, sensors that generate alarms, and in the Quick Status area.



The Quick Status area (in the upper left of the Web UI) displays the number and severity of active alarms. Click any icon in the Quick Status area to go to the **Alarms** tab.

For more information on alarms, see *Alarms Tab, page 21* or *Configure Alarms, page 33*.





Quick Links

Three links appear in the upper right corner:

- **Help:** opens the *User Guide*.
- **Logs:** Allows you to download information from the appliance log. Customer support can use this information for troubleshooting.
- **Logout:** Select this link to log out of the appliance.

Details Windows

Select any device connected to your appliance to see the details window for that device. Details provided vary by device.

Detail	Description
Label	A customizable name for each device. To change the label for any device, open the details window and click Edit  .
General information	Depending on the device, this may include hardware information (for example, the model or manufacturer of a device), network information (for example, the MAC address or IP address of a wireless sensor), or alarm status. See <i>Configure Alarms</i> , page 33 for instructions to create alarms for individual devices.
Sensor details	For some NetBotz sensors, graphs show up to 96 hours of sensor history. Click any graph to open a graph window, where you can do any of the following: <ul style="list-style-type: none"> • Select Table to view the sensor history as a table. • Click Download  to save a comma separated values (CSV) file of the sensor history to your computer. • Hover over the graph to see sensor measurements from an exact time. <p>State sensors do not show graph information, though you can click the sensor information to view a table or download a CSV file with up to 96 hours of sensor history. This is because state sensors detect a single condition (for example, the presence of smoke) instead of a range of values (for example, the temperature).</p>
Camera details	View a live feed from the camera, or edit camera settings. See <i>Configure the Camera Pod Settings</i> , page 19 for instructions to configure settings.
Outlet-controlled device details	Details windows for outlet-controlled devices show whether the device is Active or Inactive , and provide an option to change this setting manually.
Commissioned/Decommissioned status	Wireless devices only. Commissioned devices are connected to the wireless sensor network and report data to the appliance. Decommissioned devices are not connected to the wireless sensor network and do not report data to the appliance. You must commission a wireless devices for it to report data to the appliance. You must decommission a wireless device before you can remove it. You can change this status by clicking Commission  or Decommission  . See <i>Wireless Tab</i> , page 28 for more information on the wireless sensor network and instructions to add or remove a wireless sensor.
Mode	This setting is exclusive to wireless devices. The Mode indicates what role a wireless device plays on the wireless sensor network. See <i>The Wireless Sensor Network</i> , page 29 for more information.
Zigbee channel	This setting is exclusive to the coordinator for the wireless sensor network. Customer support can use it to help you trouble shoot the wireless sensor network.
Card reader	This setting is exclusive to rack access devices.
Video capture	You can configure alarms so that attached camera pods record video while the alarm is active (see <i>Configure Alarms</i> , page 33). If a connected device triggers an alarm with this feature enabled, the video recording appears at the bottom of the details window for that device. <p>The appliance can store up to 96 hours of video per camera at a resolution of 1920x1080 pixels and a frame rate of 30 frames per second (f/s). Video capture is automatically deleted after 96 hours.</p>

Overview Tab

The **Overview** tab displays feedback from cameras, sensors, and other devices connected to the appliance or the wireless sensor network. You can also use this tab to view detailed sensor information, customize 4–20 mA sensors, control devices by outlet, configure camera settings, and remove any sensor or device from the appliance.

NOTE: Video from Camera Pod 165 units does not appear in Microsoft Internet Explorer®.









NOTE: You cannot see downstream devices other than cameras on the overview tab. See *Devices Tab*, page 22 for more information on downstream devices.

There are three default tables for the Rack Monitor 750:

- **Appliance:** This table includes two outputs, one switched outlet, and two current inputs. These correspond to your appliance's relay outputs, voltage output port, and sensor input ports, respectively.
- **Appliance Rack Access:** This empty table can be populated with rack access handles and door sensors on firmware v5.1.0 and higher.
- **Wireless:** This table automatically includes the wireless coordinator attached to your appliance. If you add more wireless sensors to your wireless sensor network, they will appear here.

Most devices automatically appear in the default tables as you connect them to the appliance. Sensor pods attached to the A-Link ports will appear as separate overview tables with attached and internal sensors listed as table items.

NOTE: You can select the name of any non-wireless table to view information for that table and edit its title.

Information	Description
Alarm status	If there is an active alarm for any device, a quick status icon appears to the left of the device.
Port	<p>A port icon indicates the port the device is connected to. If the port is numbered, the port number is also shown.</p> <ul style="list-style-type: none">  Beacon  4–20 mA input  Switched outlet  Universal, USB, or Voltage output  Rack Access (Available in firmware v5.1.0 or higher)  Leak rope  Wireless
Label	To edit the label for any device, select the device to open its details window, then click Edit  .
Status information	Up to two sets of status information or sensor feedback are shown for each connected device. If a sensor provides more than two kinds of feedback, you can select the sensor to view all feedback in the details window.

Customize 4–20 mA Sensors

Select the sensor, then select **Customize**.

Setting	Description
Sensor type	Determines what units are measured.
Minimum input value	A value in milliamperes (mA) that corresponds to the Minimum mapped value .
Maximum input value	A value in mA that corresponds to the Maximum mapped value .
Minimum mapped value	The minimum value measured by the sensor.
Maximum mapped value	The maximum value measured by the sensor.

NOTE: Wait a few seconds for the sensor to configure itself.

Control Devices by Outlet

Outlet-controlled devices include devices connected to the beacon port, switched outlet, or relay output ports. You can select an outlet-controlled device to view its current status, or manually change the status of the device (from **inactive** to **active** or from **active** to **inactive**).

You can also configure alarms that will change the state of an outlet. See *Configure Alarms*, page 33 for instructions.

Configure the Camera Pod Settings

Select any camera feed to open the details window. Under **Live Feed**, a **Motion** or **No Motion** label tells you whether the camera pod detects motion within your configured parameters. To edit those parameters, select **Settings**, and configure any of the camera pod settings.

Setting	Description
Motion Masking	To detect motion, cameras compare image capture frames for differences in pixels. Configure Motion Masking settings so that the camera only compares pixels in specific parts of the frame. Click and drag your mouse to draw one or more motion masking boxes on the view pane. The camera will not detect motion inside the masking boxes. To remove the motion masks, click CLEAR ALL .
Sensitivity	Specify how much change (in percent of pixels) between image captures is considered movement. Only pixels outside the masking box are measured. Lower values indicate higher sensitivity.
Framerate	Select how many images (or frames) are recorded per second.
Resolution	Select the pixel resolution used for the images captured by the camera.



Click **Apply** to save your changes, or **Reset** to discard them.

NOTE: See *Connect Downstream Devices*, page 23 or *Add a Remote Camera*, page 24 to connect a Camera Pod 165.

NOTE: See *Configure Alarms*, page 33 for instructions to configure alarms that are generated by motion-detection settings.

Remove a Wired Device

NOTE: When a device is removed, history and alarms for that device are deleted.


1. Disconnect the device from your appliance. Wait for the device to show as **Disconnected**  in the Web UI.
2. In the Web UI, select the device. In the details window, click Remove .
3. In the **Confirm** window, click **YES** to remove the device or **NO** to keep the device.

Remove a Camera


NOTE: When a camera is removed, history and alarms for that camera are deleted.

Local cameras (which are connected directly to the appliance) say **Auto** next to the label. Remote cameras (which are connected to the appliance wirelessly) say **Manual** after the label.

To remove a local camera,



1. Disconnect the camera from your appliance. Wait for the camera to show as **Disconnected** in the Web UI.
2. In the Web UI, select the camera. In the details window, click Remove .
3. In the **Confirm** window, click **YES** to remove the camera or **NO** to keep the camera.

To remove a remote camera,

1. Select the camera in the Web UI, then click Remove .
2. In the **Confirm** window, click **YES** to remove the camera or **NO** to keep the camera.

Remove a Wireless Sensor

NOTE: When a sensor is removed, history and alarms for that sensor are deleted.

1. Select the sensor. In the details window, click Decommission , then click **APPLY**.
2. In the **Confirm** window, click **YES**.
3. Select the sensor again, then click Remove .

Alarms Tab

You can use the **Alarms** tab to view all alarms. To view alarms, select parameters that define which alarms you want to view. Each alarm that fits the selected parameters appears with a quick status icon to show the severity of the alarm, a description of what caused the alarm, and the time and date the alarm was activated.

Parameter	Description
Critical	Show critical alarms.
Warning	Show warning alarms.
Informational	Show informational alarms.
All	Show active and resolved alarms.
Active	Show any alarm for which the cause of the alarm still exists.
Resolved	Show any alarm for which the cause of the alarm no longer exists.

NOTE: Resolved alarms are stored for 96 hours. The appliance deletes alarms when the devices that generate the alarms are disconnected or removed from the wireless sensor network.

Select an alarm to view whether the relevant device is connected, graphical information (if applicable), and the time the alarm was resolved (if applicable). If the alarm is resolved, select the date or the quick status icon to view this information.


Clip Capture

The **Clip Capture** feature records video for a set amount of time before an alarm is activated and after it is cleared (video is not stored while the alarm is active). Once an alarm with **Clip Capture** is activated, a camera button appears next to the alarm. You can select the alarm to view the video recording in the details window.

To configure alarm settings or to enable **Clip Capture**, see *Configure Alarms*, page 33. To configure **Clip Capture** settings, see *Configure Video Capture Settings*, page 44.

Pagination

Up to 25 alarms are displayed per page. Click **FIRST**, **PREVIOUS**, **NEXT**, and **LAST** to navigate alarm pages.





The **Alarms** tab is not automatically updated while you view it. Select  **Refresh** to check for new alarms.

Devices Tab

You can use the **Devices** tab to view downstream devices, which connect to the appliance's private network through the Private LAN ports.

Column	Description
Name	A user-editable label for the device.
Status	<p>Initializing: The appliance is establishing communication with the device.</p> <p>Connecting: The appliance is finalizing communication with the device.</p> <p>Communicating: The appliance is communicating with the device.</p> <p>Connection Failed: Unable to reach the device. Ensure that the device is on and correctly configured. If you have made a remote connection to a Camera, ensure the IP address is correct. Ensure the Device Credentials* settings are correct.</p> <p>Not Authorized: The login credentials may be incorrect. Select the device, then select FIX CREDENTIALS to enter a different user name or password. Ensure the Device Credentials* settings are correct.</p> <p><i>*To change the Device Credentials settings, see <i>Configure Discovery Settings for Downstream Devices</i>, page 37.</i></p>
Type	The type of connected device.

You can select a downstream device for additional options:

Option	Description
	Edit the device Name (or Label).
	Delete the device.
	View detailed information for the device. NOTE: Video from Camera Pod 165 units does not appear in Microsoft Internet Explorer®.
	Opens the device's Web UI in a separate browser window. HTTP must be enabled on the device to view the Web UI. NOTE: The Web UI for the Camera Pod 165 is only used to update the Camera Pod firmware or change the password remotely. See FAQ article FA355195 on www.apc.com for instructions to access the Web UI.


Connect Downstream Devices

Compatible downstream devices include APC by Schneider Electric Rack Power Distribution Units (RPDUs) with Network Management Cards (NMC2), Smart UPS (Uninterruptable Power Supply) units, or NetBotz Camera Pod 165 units. Other ONVIF cameras may work but have not been tested.

To connect downstream devices, go to **Settings > System > Device Credentials**, and configure the following settings to match the settings on your device:

Setting	Description
Camera (ONVIF)	
NOTE: If you have not already set a password on a Camera Pod 165, you do not have to set the ONVIF credentials for that unit. The appliance will assign it a password.	
Username	The user name to access the camera..
Password/Confirm Password	The password to access the camera.
SNMPv1	
Read-only community name	The name used to access the Read-only community.
SNMPv3	
Username	The identifier of the user profile.
Authentication/Encryption	Select whether to use No security , Authentication only , or both Authentication and Encryption .
Authentication	Verifies that the device communicating through SNMPv3 is the device claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time.
Protocol	SHA1: Slower, but more secure than MD5 MD5: Faster, but less secure than SHA1
Password/Confirm Password	The password or passphrase used for authentication.
Encryption	Encrypts the data sent over SNMPv3.
Protocol	AES-128: More secure than DES. Uses a 128-bit key to encrypt data. DES: Less secure than AES. Uses a 56-bit key.
Password/Confirm Password	The password or passphrase used for encryption.

Then connect the devices to your appliance through a Private LAN port. You can connect a network switch or hub to the Private LAN ports to connect up to 10 downstream devices. Performance may vary depending on the amount of video recorded or the number of sensors attached to your downstream devices.

NOTE: The appliance counts disconnected devices as supported units. Use the  icon to remove devices before replacing them with new ones.

NOTE: If a Camera Pod 165 has previously been connected remotely, reset the camera after you connect it to the appliance. If you do not reset the camera, it may take hours or days to appear in the Web UI (the time depends on your company's DHCP configuration).

Once your devices are communicating with the appliance, you can change the **Device Credentials** to match a new set of devices without losing the established ones.

Add a Remote Camera

You will need an IP address, username, and password to connect remotely to a camera. Follow the instructions in your camera's documentation to discover its IP address and set a strong password that complies with your company's password requirements.

NOTE: Your appliance automatically assigns a new password to camera pod 165 units with a local connection. If want to change your unit from a local connection to a remote connection, reset to defaults before setting the password. (See *Discover an Assigned Camera Password*, page 24 to discover the password provided by the appliance before you disconnect the camera.) Alternatively, follow the instructions in your camera documentation to change the password before making a remote connection to the appliance.

Click **+ADD CAMERA**, and type the following information into the appropriate fields:

- **Hostname:** the host name or IP address of the camera
- **Username:** the user name to log on to the camera
- **Password/Confirm Password:** the password to log on to the camera

Discover an Assigned Camera Password

The appliance automatically assigns passwords to local, unconfigured Camera Pod 165 units (NPBD0165). To discover this password:


1. Log on to the Web UI, then open the REST API documentation by entering `<appliance IP address>/docs/rest` in the URL address bar
2. Use the **GET/assets** operation to discover the id of your camera pod. Enter `camera` in the **types** field, then select **Try it out!** If you have more than one camera, look for the label that matches the camera label in the Web UI. Copy the `id` value (for example, `camera-22`).
3. Use the **GET/cameras/cameraPassword/{id}** operation to discover the camera password. Paste the `id` in the **id** parameter field, then select **Try it out!** The property value is the password to access the camera.

Rack Access Tab

NOTE: If you plan to use an authentication server to control rack access, configure the server first. (See *Configure LDAP Settings for Rack Access*, page 43 for instructions to configure the authentication server.)

You can use the **Rack Access** tab to register proximity cards and schedule rack access. You can register one card at a time. Your rack access handles determine what kind of cards you can use.

Handle	Supported card types
Rack Access Pod 170 (NBPD0171 or NBPD0172)	<ul style="list-style-type: none"> H10301—Standard 26 bit: An access card with a 26-bit card ID number and a facility code. H10302—37 bit w/o facility code: An access card with a 37-bit card ID number and no facility code. H10304—37 bit w/ facility code: An access card with a 37-bit card ID number and a facility code. Corporate 1000 (CORP-1000) 35-bit: An access card with a 35-bit card ID number and a unique company ID code.. Corporate 1000 (CORP-1000) 48-bit: An access card with a 48-bit card ID number and a unique company ID code.
NetBotz 125 kHz Handle Kit (NBHN0125)	<ul style="list-style-type: none"> H10301 26-bit H10302 37-bit H10304 37-bit with facility code CORP-1000 35-bit
NetBotz 13.56 MHz Handle Kit (NBHN1356)	<ul style="list-style-type: none"> MIFARE Classic 4-byte UID MIFARE Classic 7-byte UID MIFARE DESFIRE MIFARE PLUS iClass

The **Audit** table shows rack access events in the last 96 hours. If there are too many events for one page, you can click **FIRST**, **PREVIOUS**, **NEXT**, or **LAST** to navigate between the pages. The **Audit** table is not automatically updated. Select  **Refresh** to update the **Audit** table.

Register a Proximity Card

Follow this procedure to register a new rack access card, or to re-register a deleted card. Registered cards can be associated with local users or LDAP users.

Local users have information that is stored directly on the appliance.

LDAP users have information stored on your company's LDAP server. When a proximity card is registered, or when a user tries to access a rack, the appliance retrieves and stores user information from your company's LDAP server. This information is used to verify the existence of the user. The appliance uses the stored information if the same user tries to access a rack within the next 10 minutes, or if the LDAP server is unavailable. Otherwise, the appliance retrieves new information every time a user tries to access a rack.

NOTE: If a user is deactivated, they will still be able to access the rack. To remove a user, delete them from the LDAP server.

NOTE: If a user is deleted on the LDAP server and the server becomes unavailable, the user may be able to access the racks using stored information until the server becomes available again.

1. Swipe the proximity card at a rack access handle. The card appears in the **Unregistered Cards** list.
2. If the card user is not stored on your company's authentication server, or if you want to provide the user with permission to access the rack when the LDAP server is unavailable, select **Local User**. If the card user is stored on your company's authentication server, you can select **LDAP**.

Local User: Enter the card owner's name in the **User** field, then click **Register**.

LDAP: Click **SEARCH LDAP**. In the **LDAP Search** window, click **ADD FILTER** and select at least one of the following attributes. Then click **SEARCH**.

Attribute	Description
Common Name	Typically the user's full name (first and last name).
UID	Typically the user's company ID. This is often, but not always, the first letter of the user's first name and the users last name.
Given Name	Typically the user's first name.
Surname	Typically the user's family name.
Sam Account Name	For Microsoft Active Directory® users, this is the name used to log on to Windows™.

You can add more filters to narrow the search, or click delete  to remove a filter.

NOTE: The search will only return results for attributes that have been configured for the user on the company's LDAP server. Users and attributes can not be configured on the NetBotz appliance. New LDAP users and user attributes must be configured through the company's LDAP server.

Select the user. Click **SELECT** to choose that user, then select **REGISTER**.


3. Select at least one door the card user can open from the drop-down list. (If you do not select a door, the card owner can not access the rack.) Click **+ADD** to add the selected door, or **+ADD ALL** to add all available doors.

NOTE: If a door switch sensor is not connected to the appliance, no doors are available to select.

Click **OK** to save your changes or **CANCEL** to discard them.

Schedule Rack Access

NOTE: The proximity card must be registered and assigned to a door before rack access can be scheduled. Complete the procedure to *Register a Proximity Card*, page 26 and click **OK** before you schedule rack access.

Select **Edit**, then click schedule .

Setting	Description
Schedule	By default, the card user is allowed access at all times. Click to disable access during any 15-minute increment. Click again to re-enable access. You can select column headings to disable access during any day of the week, or you can select row headings to disable access during a specific time of the day.
Access	Set Long Access and Auto Lock Timeout for individual doors. The Global Door Auto Lock Timeout setting still applies to all doors and cannot be disabled (see <i>Set Global Auto Lock Timeout</i> , page 39).
Long Access	When enabled, this setting disables Auto Lock Timeout and allows the cardholder unlimited access to the door. When this setting is deselected, Auto Lock Timeout resumes.
Auto Lock Timeout	This value determines the number of seconds before an unlocked handle re-locks. (This only applies to closed handles on closed doors — open handles and open doors will not re-lock). The default value is 10 seconds.

Click **APPLY** to save your changes.

Wireless Tab

You can use the **Wireless** tab to view detailed information about the wireless sensor network, add and remove sensors on the network, and update sensor firmware.

Sensor information		Description
Name		Also called the Label . You can edit this in the details window. (See <i>Details Windows, page 17.</i>)
MAC Address		The MAC address of each wireless device is a unique identifier assigned to the network interfaces for communication. While most networks use traditional 48 bit MAC addresses, the ZigBee technology used in the NetBotz wireless network requires 64 bit addresses. Valid MAC address forms include the following: <ul style="list-style-type: none"> XXXXXXXXXXXXXXXXXX (for example, 282986FFFE123456) XX:XX:XX:XX:XX:XX:XX:XX (for example, 28:29:86:FF:FE:12:34:56) XX-XX-XX-XX-XX-XX-XX-XX (for example, 28-29-86-FF-FE-12-34-56)
Model		The part number for the unit. Because coordinators and routers all have the same part number (NBWC100U), -C is used to set the coordinator apart (NBWC100U-C).
Status		<p>Disconnected: The device is setting up communication with your appliance.</p> <p>For an end device, this process may take up to one hour. If an end device does not set up communication with your appliance within an hour, the end device will wait for six hours before trying to set up communication again. You can restart the end device to force it to retry communication setup immediately.</p> <p>For a router, this process may take up to seven minutes. If the router does not set up communication with your appliance within seven minutes, it will retry communication setup again in five minutes. You can restart the router to force it to retry communication setup immediately.</p> <p>Pending update: New firmware is available.</p> <p>Updating: New firmware is being loaded to the wireless device.</p> <p>Updated: New firmware has been loaded to the wireless device.</p> <p>Error: New firmware could not be loaded to the wireless device.</p> <p>Decommissioned: The sensor is not connected to the wireless sensor network and does not send information to the host appliance.</p> <p>Connected: The sensor is connected to your wireless sensor network and can send information to the host appliance.</p>
Battery		The current battery voltage reading from the wireless device. Firmware updates may not be successful if the battery voltage drops below 2.8 V.
RSSI		Received Signal Strength Indication in decibels (dB).
Versions	Current	The current firmware version used by the wireless device.
	Staging	Firmware that has been loaded to the wireless devices but is not yet active. If the Staging firmware version does not match the Current firmware version, click APPLY . If the Staging firmware version does not match the Target firmware version, update the firmware (see <i>Update the Wireless Sensor Network, page 31</i>).
	Target	The latest wireless firmware available. This is automatically populated when you update the firmware on your appliance. If the Target firmware version does not match the Staging firmware version, update the firmware (see <i>Update the Wireless Sensor Network, page 31</i>).

The Wireless Sensor Network

The wireless sensor network is made of a host appliance, a coordinator, routers, and end devices.

- The **host appliance** (your NetBotz Rack Monitor or Room Monitor) collects data from the wireless sensor network and generates alerts based on sensor readings.
- The **coordinator** is connected directly to the host appliance via USB. It reports data from the sensors on the network and provides available firmware updates to the wireless network. Each wireless sensor network must have only one coordinator, which is connected to a dedicated USB Type A port on the NetBotz appliance.
- **Routers** extend the range of the wireless sensor network. Routers pass information between themselves and the coordinator, and between the coordinator and end devices. Each router is powered by an AC-USB adapter, not directly connected to the host appliance.

Routers are optional. In a data center environment where obstructions are common, routers are recommended if sensors are more than 50 feet from the coordinator.

- **End devices** monitor attached and internal sensors and send data back to the host appliance. End devices are powered by batteries, and are not connected to the host appliance.

Devices on the Wireless Sensor Network

NOTICE

EQUIPMENT DAMAGE RISK

Only the devices listed here are compatible with the NetBotz wireless sensor network. Other devices may not function and may damage the appliance or other wireless devices.

Failure to follow these instructions can result in equipment damage.

Device	Network Role
USB Coordinator & Router (NBWC100U)	Coordinator when connected to the appliance USB port Router when connected wirelessly and powered by an AC-USB adaptor
Wireless Temperature Sensor (NBWS100T)	End device
Wireless Temperature/Humidity Sensor (NBWS100H)	End device

NOTE: Wireless devices have a range of up to 30.5 m (100 ft), line of sight. In a data center environment where obstructions are common, a range of 15 m (50 ft) is typical for any wireless device.

Connect the Wireless Sensor Network

The order in which you configure your wireless sensor network and apply power to your wireless devices is important:

1. Select the coordinator and routers: If a USB Coordinator and Router (NBWC100U) comes pre-installed on your appliance, then the pre-installed USB Coordinator and Router will act as your coordinator. Note the extended address of the coordinator. If necessary, choose one or more USB Coordinator & Routers to become routers.
2. Choose the locations for the routers and end devices. Do not power the routers or end devices at this time.
3. Power the coordinator first: On appliances with a USB Coordinator and Router installed, the coordinator is powered when you power the appliance. Otherwise, connect one USB Coordinator & Router to a USB Type A port on the NetBotz appliance.
4. Use an AC-USB adapter to apply power to each router. Routers are not directly connected to the NetBotz appliance.
5. Apply power to the end devices after the coordinator and the routers are powered. This helps to preserve battery life.
6. Add end devices (wireless sensors) to the wireless sensor network. See *Add Sensors to the Wireless Sensor Network*, page 30 for instructions.

Add Sensors to the Wireless Sensor Network

Follow the instructions to *Connect the Wireless Sensor Network*, page 30. Then, in the **Wireless** tab, click **ADD**, and select one of the following.


Add Detected Sensors

1. Select any automatically detected device, or use the **Search** field to find the MAC address for a specific end device. You can enter a name for any selected sensor in the **Name** field.
2. Click **ADD** to add all selected sensors to the wireless sensor network, or click **CANCEL** to close the window.

Add Sensors Manually

1. Click **Choose File** to navigate to a CSV file saved on your computer, or type the MAC address of the device in the **MAC Address** field. You can enter a name for any selected sensor in the **Name** field. If you do not give the sensor a name, its MAC address is used as the name.

NOTE: The CSV format for each sensor should be *MAC address, optional name*.

2. Select **Add another** to add more than one sensor, or click Remove  to remove a sensor from the list. You can enter the name or MAC address of a specific sensor in the **Search** field to highlight it.
3. Click **ADD** to add all listed sensors to the wireless sensor network, or click **CANCEL** to close the window.



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.

Remove a Wireless Sensor

NOTE: When a sensor is removed, history and alarms for that sensor are deleted.

1. Select the sensor. In the details window, click Decommission , then click **APPLY**.
2. In the **Confirm** window, click **YES**.
3. Select the sensor again, then click Remove .

Settings Tab


You can use the **Settings** tab to view and edit settings for notifications, alarm configurations, system preferences, user accounts, firmware updates, backup processes, and general information about your appliance.

Configure Notification Policies

Path: Settings > Notification

Configure notifications to be sent when alarms are generated. Notifications can be sent via email and Simple Mail Transfer Protocol (SMTP), or via Simple Network Management Protocol (SNMP) traps. You can create new email notification policies or edit existing policies. To configure notifications by SNMP trap, you must edit the **Default Trap Policy**.

NOTE: You must configure an SMTP server for email notifications to work. (See *Configure an SMTP Server, page 40* for details.) You must configure a remote trap receiver for trap notifications to work. (See *Configure SNMP Settings, page 41*.)

Click **ADD** to create a notification policy, or select **Edit**  to change an existing policy. Then configure the notification policy settings.

Setting	Description
Name	This will appear under Name in the Notification page and in the header of a notification email.
Send to email addresses	Enter e-mail addresses for anyone who will receive the notification. To send emails to multiple recipients, separate the email addresses with commas or enter a distribution list.
Notify for severities	Select alarm severities that will cause the notification to be generated.
Units	Select the system used to show measurements in the notification: Metric or Imperial .
Time format	Select the system used to show time in the notification: 12 hour or 24 hour .

Click **OK** to save your policy, or **CANCEL** to discard it.


Configure Alarms

Path: Settings > Alarm Configuration

The appliance comes with default alarms pre-configured for its internal sensors (outlet, switched outlet, and current input). The appliance also creates default alarms when new sensors are connected. For example, if you connect a temperature sensor to the appliance, three **Default Temperature** alarms (**High**, **Low**, and **Too High**) are automatically created for that sensor.

When you connect additional sensors to the appliance, the appliance automatically applies the appropriate default alarms to those sensors. For example, if you connect three more temperature sensors to the appliance, the default temperature alarms are automatically applied to all three sensors. Unless you change these settings, any temperature sensor can set off any temperature alarm.

Sensor type	Name	Operation	Value	Severity	Description
Beacon	Default Beacon	Equals	Active	Informational	If the beacon is activated, generate an informational alarm.
Motion	Default Motion	Equals	Motion Detected	Informational	If motion is detected, generate an informational alarm.
Leak rope	Default Leakrope	Equals	Leak Detected	Informational	If a leak is detected, generate an informational alarm.
Smoke	Default Smoke	Less than	Smoke Detected	Informational	If smoke is detected, generate an informational alarm.
Battery	Default Battery (Too Low)	Less than	2.4 V	Critical	If the battery voltage falls below 2.4 V, generate a critical alarm named "Too Low."
	Default Battery (Low)	Less than	2.65 V	Warning	If the battery voltage falls below 2.65 V, generate a warning alarm named "Low."
Temperature	Default Temperature (Low)	Less than	18°C (64.4°F)	Warning	If the temperature falls below 18°C (64.4°F), generate a warning alarm named "Low."
	Default Temperature (High)	Greater than	27°C (80.6°F)	Warning	If the temperature rises above 27°C (80.6°F), generate a warning alarm named "High."
	Default Temperature (Too high)	Greater than	32°C (89.6°F)	Critical	If the temperature rises above 32°C (89.6°F), generate a warning alarm named "Too High."
Relative Humidity (RH)	Default Humidity (High)	Greater than	80% RH	Warning	If the humidity rises above 80%, generate a warning alarm named "High."
	Default Humidity (Low)	Less than	20% RH	Warning	If the humidity falls below 20%, generate a warning alarm named "Low."
State Door Contact	Default State Default Door Default Contact	Equals	Open	Info	If a State, Door, or Contact sensor is switched to Open , generate an informational alarm.
Vibration	Default Vibration	Equals	Vibration Detected	Info	If vibration is detected, generate an informational alarm.
Spot leak	Default Spot Leak	Equals	Leak Detected	Info	If a leak is detected, generate an informational alarm.
Outlet Relay output Switched Outlet Switch	Default Outlet Default Output Relay Default Switched Outlet Default Switch	Equals	Relay Active	Info	If the status of an Outlet, Relay output, Switched outlet, or Switch is set to Active , generate an informational alarm.
External relay	Default External Relay	Equals	Relay On	Info	If the status of an external relay is set to On , generate an informational alarm.
Airflow	Default Airflow (Low)	Less than	8 ft/sec	Warning	If airflow falls below eight (8) feet per second, generate a warning alarm named "Low."

You can use the **Alarm Configuration** page (under) to edit the default alarms, create new alarms, or delete alarms. If you create new alarms, you must add sensors to the new alarms manually. Select **Edit**  to change an existing alarm configuration, or click **ADD** and select the sensor type to create a new alarm. Then configure the alarm settings.

Setting	Description
Name	The name of the alarm. This appears on the alarm configuration page, the Alarms tab, and the relevant sensor details window when the alarm is generated.
Operation	<p>Greater than: If the device returns a value greater than the Value field, the alarm is generated.</p> <p>Less than: If the device returns a value less than the Value field, the alarm is generated.</p> <p>Equals: If the device returns a value equal to the Value field, the alarm is generated.</p>
Value	<p>The alarm is based on this value. Available values depend on the selected type of device.</p> <p>0V-5V: Enter a value in Volts (V).</p> <p>4mA-20mA: Enter a value in milliamperes (mA).</p> <p>Air Flow: Enter a value in feet per second (ft/sec).</p> <p>Air Flow (speed): Enter a value in feet per minute (ft/min).</p> <p>Beacon: Select Active or Inactive.</p> <p>Humidity: Enter a percent value.</p> <p>Motion: Select No Motion or Motion Detected.</p> <p>Output Relay: Select Active or Inactive.</p> <p>RSSI: Enter a value in decibels (dB).</p> <p>State: Select Open or Closed.</p> <p>Switched Outlet: Select Active or Inactive.</p> <p>Temperature: Enter a value in degrees Fahrenheit or Celsius. The temperature scale is determined in your user settings (see <i>View and Edit User Accounts, page 44</i>).</p>
Severity	<p>Select the severity of the alarm: Critical, Warning, or Informational.</p> <p>You can also use the severity to configure notification policies. See <i>Configure Notification Policies, page 32</i> for more information.</p>
Sensors	Select any sensors that can cause the alarm to be generated.
Clip Capture	This feature is optional. Select a camera to capture video from before and after the alarm is generated. The captured video will appear in the details window for any device that causes an alarm. See <i>Configure Video Capture Settings, page 44</i> to set the duration and resolution of video captures for alarms.
Control	<p>This feature is optional. Determine how other connected devices are affected by the alarm. Under Name, select devices the alarm will control. Under On alarm active and On alarm clear, select what will happen when the alarm activates and is cleared (respectively).</p> <p>For example, if you select Beacon at appliance, the beacon attached to your appliance will be controlled by the alarm. If you select On under On alarm active and select Off under On alarm clear, the beacon turns on when the alarm is generated and turns off when the alarm is cleared.</p>
Schedule	This feature is optional in firmware v5.1.0 and above. Select Schedule , then select times during which the alarm can be generated. The alarm can not be generated during times that are not selected.

Click **OK** to save the alarm configuration, or **CANCEL** to discard it.

To delete an alarm, select  Delete.

Configure System Settings

Use this page to view and set preferences for any of the following:

- **DCE Surveillance**
- **Date and Time**
- **Identification**
- **Logging** (event log)
- **Network**
- **Proxy Settings**
- **Rack Access** (global auto lock timeout)
- **SMTP Server**
- **SNMP**
- **SSL Certificate** (for inbound connections)
- **Trust Store** (certificates for outbound connections)
- **User Store** (LDAP settings for Rack Access)
- **Video Capture**
- **Wireless** (wireless update settings)

Enable DCE Surveillance

Path: Settings > System > DCE Surveillance

You can discover NetBotz appliances with in StruxureWare Data Center Expert (DCE) and use DCE to monitor sensor readings through the appliance. In DCE, v7.7 and later, you can also use the DCE interface to set events that trigger camera recording, record video on demand, and store camera recordings.

The appliance communicates over HTTPS. To establish secure communication with DCE,

1. Save the appliance certificate and DCE certificate to your computer. To obtain a certificate in Google Chrome, enter `https://ip_address` in the URL address bar, where `ip_address` is the IP address of your DCE or appliance Web UI. Click the symbol in far left of the URL address bar (a padlock or warning symbol), then select **Certificate > Details > Copy to File** and follow the prompts to export a Base-64 encoded x.509 certificate to your computer. If this certificate format is not an option, use OpenSSL to convert the downloaded certificate to PEM format.
2. Add the appliance's SSL certificate to DCE. See your DCE documentation for instructions.
3. Add the DCE certificate to your trust store. Open the certificate in a text editor and copy its content. Then go to **Settings > System > Trust Store**. Click **ADD** to open the **Add certificate** window, then paste the certificate in the window. Click **ADD** to save the certificate in your trust store. See *Configure Certificates for Outbound Connections, page 43* for more information.
4. Enable SNMP on the appliance (**Settings > System > SNMP**), then use SNMP to discover the appliance in DCE (see your DCE documentation for instructions).

For less secure communication, you can choose not to add either certificate. If you choose not to add the DCE certificate to your appliance, you must deselect **Verify DCE Certificate in Trust Store** in the DCE Surveillance page. If you do not add the appliance's SSL certificate to DCE, you must direct DCE to not verify the SSL certificate in the appliance communication settings.

Configure Date and Time Settings

Path: Settings > System > Date and Time

NTP: Synchronize the time of the Web UI to the time of the specified Network Time Protocol (NTP) server. The default time is Coordinated Universal Time (UTC).

Setting	Description
Primary Server	Type the hostname or IP address of the NTP server.
Secondary Server	Optional: Type the hostname or IP address of a second NTP server. If the Primary Server fails, the appliance will synchronize with this server.
Tertiary Server	Optional: Type the hostname or IP address of a third NTP server. If the Secondary server fails, the appliance will synchronize with this server.
Timezone	Select your time zone from the drop-down list.

Manual: Configure the date and time yourself. Select the **Date**, **Time**, and your **Timezone** from the drop-down lists.

Click **APPLY** to save your changes or **RESET** to discard your changes.

Configure Discovery Settings for Downstream Devices

Path: Settings > System > Device Credentials

Use the **Device Credentials** page to configure discovery settings for downstream devices. The discovery settings must match the ONVIF, SNMPv1, or SNMPv3 settings on your device, or the device will not be discovered.

Setting	Description
Camera (ONVIF)	
NOTE: If you have not already set a password on a Camera Pod 165, you do not have to set the ONVIF credentials for that unit. The appliance will assign it a password.	
Username	The user name to access the camera..
Password/Confirm Password	The password to access the camera.
SNMPv1	
Read-only community name	The name used to access the Read-only community.
SNMPv3	
Username	The identifier of the user profile.
Authentication/Encryption	Select whether to use No security , Authentication only , or both Authentication and Encryption .
Authentication	Verifies that the device communicating through SNMPv3 is the device claims to be, that the message has not been changed during transmission, and that the message was communicated in a timely manner, indicating that it was not delayed and that it was not copied and sent again later at an inappropriate time.
Protocol	SHA1: Slower, but more secure than MD5 MD5: Faster, but less secure than SHA1
Password/Confirm Password	The password or passphrase used for authentication.
Encryption	Encrypts the data sent over SNMPv3.
Protocol	AES-128: More secure than DES. Uses a 128-bit key to encrypt data. DES: Less secure than AES. Uses a 56-bit key.
Password/Confirm Password	The password or passphrase used for encryption.

Select **APPLY** to save your changes, or **CANCEL** to discard them.

Set Identification Information

Path: Settings > System > Identification

Storing identification information for the owner of the appliance allows anyone using the appliance to contact that person in case of an emergency. This information is also used by SNMP MIB-2.

Information	Description
Name	Type the name of the appliance owner. (This is called sysName in SNMP MIB-2).
Location	Type the physical location of the appliance. (This is called sysLocation in SNMP MIB-2).
Contact	Enter contact information (for example, an e-mail address) for the appliance owner. (This is called sysContact in SNMP MIB-2.)

Click **APPLY** to save your changes or **RESET** to discard them.

Configure Log Settings

Path: Settings > System > Logging

You can configure a remote Syslog server to store log files for events such as rack access events and camera discoveries. Once the server is configured, log files are automatically copied to the Syslog server.

Setting	Description
Level	The drop-down list shows all possible logging event levels in order from highest to lowest urgency. Select the lowest event level to appear in the appliance log. Event levels lower than the selected level are not recorded. This setting also applies to the Logs Quick Link at the top right of the Web UI.
Enable	Enable remote logging.
Server	Enter the host name or IP address of the Syslog server.
UDP Port	Enter the UDP port number used to communicate with your Syslog server.

Configure Network Settings

Path: Settings > System > Network

View and configure network settings.

Setting	Description
Static	Select Static to manually configure your Network settings. This setting assigns a static IP address to the appliance.
DHCP	Use a DHCP server to configure network settings automatically. This setting assigns a dynamic IP address to the appliance.
Hostname	The host name of the appliance.
TCP/IP	
IP Address	The IP address of the appliance. Use the format xxx.xxx.xxx.xxx.
Subnet Mask	The subnet mask of the appliance.
Gateway	The IP address of the default gateway.
DNS	
Primary	The IP address of the primary DNS server
Secondary	The IP address of the secondary DNS server
Tertiary	The IP address of the tertiary DNS server

Click **APPLY** to save your changes or **RESET** to discard them.

NOTE: If the network settings are incorrect, you can not reach the appliance through the Web UI. See *Use a Terminal Emulator to Establish Network Settings*, page 13 for instructions to change your network settings without access to the Web UI.

Configure a Proxy Server

Path: Settings > System > Proxy Settings

When proxy settings are configured, the appliance uses an HTTP or HTTPS proxy server for all e-mail and HTTP/HTTPS communications, allowing these communications to cross the firewall. When HTTPS is enabled, data is encrypted during transmission and authenticated by digital certificate. These settings apply only to communications from the appliance.

To enable a proxy server, enter the HTTP or HTTPS Proxy Settings.

Setting	Description
Server	The host name or IP address of the proxy server the appliance uses for e-mail, HTTP Posts, and other outbound communications.
Port	The IP port number to connect to the proxy server.
Username	Enter a user name to allow access through the server.
Password/Confirm Password	Enter a password to allow access through the server.

Click **APPLY** to save your changes, or **RESET** to discard them.

Set Global Auto Lock Timeout

Path: Settings > System > Rack Access

Enter a value in the **Global Door Auto Lock Timeout** field to determine the number of minutes before any unlocked handle re-locks. This only applies to closed handles on closed doors — open handles and open doors will not re-lock, but they will generate alarms when the timer ends.

This setting applies to all doors with Rack Access control. You can also set **Auto Lock Timeouts** for individual doors. See *Schedule Rack Access*, page 27 for details.

Configure an SMTP Server

Path: Settings > System > SMTP Server

You must configure an SMTP server before you can configure e-mail notifications.

Setting	Description
SMTP server address	The hostname or IP address of the SMTP server.
Port	The IP port number to connect to the SMTP server (firmware v5.0.1 only).
Use SSL	This optional feature allows you to use Secure Sockets Layer (SSL)/Transport Layer Security (TLS) protocol to encrypt email notifications. For most port numbers, selecting this option enables STARTTLS. STARTTLS encrypts e-mail content only if your SMTP server supports encryption. In firmware v5.1.0, if you select Use SSL and the port number is 465 or 587, SSL/TLS encryption is required. If the SMTP server does not support encryption, the appliance can not connect to the server.
From address	The e-mail address that will appear in the From field for emails generated by the appliance.
Username	User names are optional. If desired, create a user name to allow access through the server.
Password/Confirm Password	Passwords are optional. If desired, create a password to allow access through the server.
Send test email	Select to send an email and confirm the settings are correct.

Click **APPLY** to save your changes, or **RESET** to discard them.

Configure SNMP Settings

Path: Settings > System > SNMP

View or edit the following settings for your SNMP agent or Remote trap receiver. You must configure a Remote trap receiver for the appliance to send out SNMP traps.

Setting	Description
SNMP agent	
Enable	Select to enable the SNMP agent on your appliance.
Port	The port number for SNMP communications.
SNMPv1/ SNMPv3	Select the SNMP version for the agent to use.
Read-only community name	The read-only community name for SNMP requests. SNMPv1 only.
Authentication/ Encryption	SNMPv3 only. Select whether to use No security , Authentication only , or both Authentication and Encryption .
Username	Enter the user name to access the SNMP agent.
Protocol	Authentication protocols: <ul style="list-style-type: none"> • SHA1: Slower, but more secure than MD5 • MD5: Faster, but less secure than SHA1 Encryption Protocols: <ul style="list-style-type: none"> • AES-128: More secure than DES. Uses a 128-bit key to encrypt data. • DES: Less secure than AES. Uses a 56-bit key.
Password/ Confirm Password	Enter the password to access the SNMP agent.
Remote trap receiver	
Enable	Select to enable SNMP traps.
SNMP trap receiver	The IP address or host name of the trap receiver.
Port	The port number of the remote SNMP trap receiver.
SNMPv1/ SNMPv3	Specify the trap type by selecting either SNMPv1 or SNMPv3.
Read-only community	The read-only community name for SNMP trap requests. SNMPv1 only.
Send test trap	Select to send a test trap to a configured trap recipient.
Authentication/ Encryption	SNMPv3 only. Select whether to use No security , Authentication only , or both Authentication and Encryption .
Username	Enter the user name to access the remote trap receiver.
Protocol	Authentication protocols: <ul style="list-style-type: none"> • SHA1: Slower, but more secure than MD5 • MD5: Faster, but less secure than SHA1 Encryption Protocols: <ul style="list-style-type: none"> • AES-128: More secure than DES. Uses a 128-bit key to encrypt data. • DES: Less secure than AES. Uses a 56-bit key.
Password/ Confirm Password	Enter the password to access the remote trap receiver.

Click **APPLY** to save your changes, or **RESET** to discard them.

Configure Certificates for Inbound Connections

Path: Settings > System > SSL Certificate

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:

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 five years. You can regenerate the certificate at any time (see Generate a Self-signed Certificate on this page). The new certificate will expire five years 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 (CA). 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.

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 .

Configure LDAP Settings for Rack Access

Path: Settings > System > User Store

NOTE: This feature is available in firmware v5.1.0 and above.

You can use this page to connect to your company's authentication server and verify the existence of specific users.

Select **Enable** to connect to a server, then configure the **Server Settings** and **LDAP Schema**.

Setting	Description
Server Settings	
Hostname	Enter the host name of your company's authentication server.
Port	Enter the IP port number to connect to your company's authentication server.
Use SSL	Select to enable Transport Layer Security. If this setting is enabled and you have a trust store certificate for the LDAP server, the Hostname entered on this page is verified against the host name in the trust store certificate. The Hostname on this page must match the host name on the certificate
Username	Enter the user name to log into your company's authentication server.
Password	Enter the password to log into your company's authentication server.
Test Server Configuration	Click to test validity of server configuration.
LDAP Schema	
Base DN	Enter the base distinguished name of your company's LDAP directory. You can copy this directly from your LDAP directory. The more specific your filepath is, the shorter the search will be.
Username Attribute	Enter the attribute your company uses to authenticate users. For Active Directory servers, this is typically the Sam account name. For most other LDAP servers, this is the UID (User ID).
Test User Schema	Search for an existing user to ensure your schema is configured properly. Select Test User Schema , enter the Username and Password for an existing user on your company's LDAP server, then click TEST .

NOTE: LDAP users can not be created on the appliance. Create users and add user attributes on your company's LDAP server.

Configure Video Capture Settings

Path: Settings > System > Video Capture

You can configure cameras to record video when alarms are generated (see *Configure Alarms*, page 33 for details). Use video capture settings to determine how much video is recorded for alarms with Clip Capture enabled.

Setting	Description
Pre-alarm capture time	The total number of seconds prior to an alarm that images are recorded and saved.
Post-alarm capture time	The total number of seconds after an alarm that images are recorded and saved.

Click **APPLY** to save your changes, or **RESET** to discard them.

Set Wireless Update Settings

Path: Settings > System > Wireless

Some wireless devices such as the NetBotz USB Coordinator and Router (NBWC100U) have firmware that is updated separately from the NetBotz appliance. Select **Automatic** to update wireless devices automatically when new firmware is installed, or select **Manual** to update wireless devices at your convenience. Click **APPLY** to save your changes, or **RESET** to discard them.

NOTE: You can see the current and target firmware versions for wireless devices in the **Wireless** tab (see *Wireless Tab*, page 28).


View and Edit User Accounts

Path: Settings > Users

Click **ADD** to add a new user, or click Edit  to change an existing user account, then configure the user settings.

Setting	Description
User name	Enter the user name.
Password*	Enter the password for the user to log on to the appliance.
Units	Select Metric or Imperial units of measurement.
Time format	Select the 12 hour or 24 hour time format.

*To change the password for an existing user, the Super User can click **Change password** on the main page.

Click **OK** to save your changes, or **CANCEL** to discard them. The Super User can also click  Delete to delete a user account.

Update the Appliance Firmware

Path: Settings > Firmware Update

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 ensure that all units support the same features in the same manner.

To update the firmware,

1. Download the latest firmware version for free from the APC by Schneider Electric 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.

Firmware Downgrade

To downgrade the firmware, perform the firmware update procedure with a previous firmware version, then reset to defaults (see *Reset to Defaults, page 15*) or restore a configuration from the relevant firmware version (see *Restore System Settings, page 47*).

NOTE: You cannot downgrade to firmware version 5.0.1.

Backup and Restore System Settings

Path: Settings > Backup

On this page, you can save the current system settings to a backup file, use a backup file to restore previous system settings, or use a backup file to configure multiple appliances.


When you restore system settings from a backup file, always use a backup file saved from the same firmware version as the current system. If a firmware update is available, restore the system and re-configure the network settings before you update the firmware. Save a backup file immediately after you update the firmware.

NOTE: Backup files do not store network settings and can not be used to configure network settings.

Save a Backup File

The backup file includes all of the configuration settings for your appliance, including user account settings, sensor configurations, and alarm configurations. You can use the backup file to restore this configuration to your appliance at a later date or to configure a new appliance.

To save a backup file,

1. Ensure your system settings are configured as needed.
2. Under **Backup to file**, select  Download.

NOTE: The file may take several seconds to begin downloading.

A backup file is saved to your computer.

NOTE: The backup file is not encrypted. Save the backup file in a secure location. Consider encrypting the backup file with a tool such as the GNU Privacy Guard (on gnupg.org) and verifying the file before performing a restore.

Restore System Settings

Use a backup file to restore a previous system configuration.

To restore system settings,

1. Select **Restore an existing backup to this device**.
2. Click **Choose File** and navigate to the backup file of your choice.
3. Click **Restore**.

The appliance settings are updated according to the backup file.

Configure New Appliances from a Backup File

Use the settings from one appliance to configure other appliances.

To configure new appliances,

1. Download a backup file from a configured appliance to your computer.
2. On an un-configured appliance, go to the **Settings** tab, select **Backup**, then select **Clone a backup on to new device**.
3. Click **Choose File**, and navigate to the backup file from the configured appliance.
4. Click **CLONE** to configure the appliance, or **CANCEL** to stop the operation.

The appliance settings are updated according to the backup file.

View Appliance Information

Path: Settings > About

On this page, you can view the **Model**, firmware **Version**, **IP Address**, and **Serial Number** of the appliance. Customer support can use this information to help troubleshoot problems with your appliance.

REST API

The REST API allows you to interact with the appliance via JSON requests.

This document provides an overview of each operation available and detailed descriptions for request parameters. The online REST API documentation provides models for requests and responses. It also provides an interactive interface to test operations. Your permissions in the REST API documentation depend on your permissions in the Web UI.

To access the online REST API documentation, log on to the Web UI, then open a new tab and enter

```
your_appliance_IP_address/docs/rest
```

in the URL address bar.

To access the REST API, enter *your_appliance_IP_address/rest*.

Using the API

Unless otherwise stated,

- Parameter *s* are case sensitive.
- Time values (both input and retrieved) are always formatted as milliseconds since the UNIX® epoch (milliseconds since epoch).
- Use commas to separate value lists for parameters that accept more than one value. For example, *asset-1, asset-2, asset-3*.
- All operations return a JSON response.

Body parameters contain the request body for the operation. You must enter the entire request body using valid JSON format and include `nbTypes`. In the REST API documentation, you can select the **Model Schema** under **Data Type** to copy the request body into the value field, enter the `nbtypes`, then fill in the request.

The following rules apply to each body request:

- **IDs and labels:** IDs are automatically generated by the appliance and cannot be changed. When filling out the model for a POST command, always leave the `id` blank. Unlike IDs, labels are user-friendly names that you can configure and modify.
- **Quotation marks:** String values (except `null`) must be enclosed in quotation marks. Booleans and integers are not enclosed in quotation marks.
- **Optional values:** You have the option to leave some request body values unconfigured. To leave an integer parameter unconfigured, enter `0`. To leave a string parameter unconfigured, enter empty quotes (`" "`) or `null` (no quotes).
- **Reserved parameters:** If a parameter is not used, ignored, or reserved for future use, enter `null` (string), `0` (integer), or `false` (boolean).

Operations

alarms

GET /alarms

Retrieves a list of alarms based on the specified inputs.

Parameters

Parameter	Description
pageNumber	Zero-based index for the page of alarms requested.
pageSize	The number of alarms in a page.
sort	Comma-separated list or Java Script Object Notation (JSON) array of column names (timestamp or severity) preceded by a plus (+) for ascending or a minus (-) for descending.
severities	Comma-separated or JSON Array of alarm severities to include (OK, INFO, WARNING, or CRITICAL). An asterisk (*) is used to signify all severities. Enter a minus (-) before a severity to exclude it.
timeRange	A date range in milliseconds since the Unix epoch (milliseconds since epoch). Enter as "startTime - endTime". The startTime and endTime can be wildcards (*).
active	A Boolean that specifies whether to include active or inactive alarms in the system. If null or not supplied, both active and inactive alarms are retrieved.
assetIds	Optional. A list of asset IDs to collect alarms from specific assets.

GET /alarms/configurations

Gets a list of all the alarm configurations.

POST /alarms/configurations

Creates a new alarm configuration.

Parameters

Parameter	Description
body	The alarm configuration. See Request body for details.

Request body

nbType	AlarmConfigurationDTO. (Required.)
id	The alarm configuration ID. Automatically generated by the appliance.
label	The label of the alarm configuration. (Required.)
assetIds	Identifiers of assets that can cause the alarm. To create a motion detection alarm, enter the ID of a motion sensor, not a camera.
rule	
nbType	NumericThresholdRuleDTO or StateThresholdRuleDTO. (Required.)
id	The rule ID. Automatically generated by the appliance.
enabled	Defines whether the rule is enabled. (Required.)
label	The label of the rule.
sensorType	The sensor asset type. (Required.)
state	Required for StateThresholdRuleDTO.
operation	EQUALS, GREATER_THAN, or LESS_THAN. Applies to value . (Required for NumericThresholdRuleDTOs.)
value	The alarm threshold. (Required for NumericThresholdRuleDTOs.)
units	The units measured by value . (Required for NumericThresholdRuleDTOs.) METERS_PER_SEC, FEET_PER_SEC, METERS_PER_MIN, FEET_PER_MIN, KVA, VA, KVA_PER_HOUR, VA_PER_HOUR, AMPS, MILLIAMPS, KA, MA, GA, TA, PA, CELSIUS, CENTIMETERS_WATER_COLUMN, INCHES_WATER_COLUMN, FAHRENHEIT, KWH, NUMERIC, HERTZ, KHZ, MHZ, GHZ, THZ, PHZ, PERCENT, RELATIVE_PERCENT, WATTS, KW, MW, GW, TW, PW, PASCAL, HPA, KPA, MPA, GPA, PSI, KVAR, VAR, KVAR_PER_HOUR, VAR_PER_HOUR, STATE, MILLISECONDS, SECONDS, MINUTES, HOURS, DAYS, WEEKS, MONTHS, YEARS, VOLTS, KV, MV, GV, TV, PV, GRAMS, KILOGRAMS, OUNCES, POUNDS, MILLIMETERS, CENTIMETERS, METERS, INCHES, FEET, YARDS, MILES, SQUARE_CENTIMETERS, SQUARE_METERS, SQUARE_INCHES, SQUARE_FEET, BYTES, KB, MB, GB, TB, PB, LITER_PER_SEC, LITER_PER_MIN, LITER_PER_HR, GAL_PER_SEC, GAL_PER_MIN, GAL_PER_HR, RPM, RUN_HOURS, STRING, DB, UNKNOWN
severity	INFO, CRITICAL, or WARNING. (Required.)
cameraIds	Enter the ID of one or more cameras to configure clip capture for the alarm.
controlConfigurations	Configurations for devices that are controlled by the alarm
nbType	ControlConfigurationDTO.
controlSensorId	The ID of the device to control.
onAlarmState	The state the sensor changes to when the alarm is generated.
onClearState	The state the sensor changes to when the alarm is cleared.
scheduled	Determines whether the alarm is on a schedule. Defaults to false. See PUT/alarms/configuration/{id}/schedule to configure a schedule.

NOTE: See *GET /assets*, page 55 for asset IDs and sensor information.

NOTE: Possible states for each sensor type are as follows:

- SMOKE: sensor.state.smoke.smoke-detected, sensor.state.smoke.no-smoke
- BEACON: sensor.state.beacon.active, sensor.state.beacon.inactive
- VIBRATION: sensor.state.vibration.vibration-detected, sensor.state.vibration.no-vibration
- LEAK_ROPE: sensor.state.leakRope.leak, sensor.state.leakRope.no-leak
- SPOT_LEAK: sensor.state.spotLeak.leak, sensor.state.spotLeak.no-leak
- DOOR, RACK_HANDLE, CONTACT: sensor.state.sensor-value-state.open, sensor.state.sensor-value-state.closed
- OUTLET, OUTPUT_RELAY, SWITCHED_OUTLET, SWITCH: sensor.state.internalRelay.active, sensor.state.internalRelay.inactive
- DOOR_LOCK: sensor.state.lock.open, sensor.state.lock.closed
- EXTERNAL_RELAY: sensor.state.externalRelay.on, sensor.state.externalRelay.off
- MOTION: sensor.state.MOTION.motion-detected, sensor.state.MOTION.no-motion
- OUTLET, STATE, SWITCH: not supported

Example

Request

```
{
  "nbType": "AlarmConfigurationDTO",
  "id": null,
  "label": "Low Battery",
  "assetIds": [
    "sensor-61"
  ],
  "rule": {
    "nbType":
      "NumericThresholdRuleDTO",
    "id": null,
    "enabled": true,
    "label": "Default Battery (Too
    Low)",
    "sensorType": "BATTERY",
    "operation": "LESS_THAN",
    "severity": "CRITICAL",
    "value": 2,
    "units": "VOLTS"
  },
  "cameraIds": [],
  "controlConfigurations": [],
  "scheduled": false
}
```

Response

```
{
  "nbType": "AlarmConfigurationDTO",
  "id": "alarm_configuration-80",
  "label": "Low Battery",
  "assetIds": [
    "sensor-61"
  ],
  "rule": {
    "nbType": "NumericThresholdRuleDTO",
    "id": "rule-79",
    "enabled": true,
    "label": "Battery",
    "sensorType": "BATTERY",
    "operation": "LESS_THAN",
    "severity": "CRITICAL",
    "value": 2,
    "units": "VOLTS"
  },
  "cameraIds": [],
  "controlConfigurations": [],
  "scheduled": false
}
```

DELETE /alarms/configurations/{ids}

Deletes one or more alarm configurations by ID.

Parameters

Parameter	Description
ids	A comma-separated string of alarm configuration IDs (for example, alarm_configuration-1, alarm_configuration-2).

GET /alarms/configurations/{id}

Gets an alarm configuration by ID.

Parameters

Parameter	Description
id	The ID of the alarm configuration (for example, alarm_configuration-10).

PUT /alarms/configurations/{id}

Modifies an alarm configuration.

Parameters

Parameter	Description
id	The ID of the alarm configuration (for example, <code>alarm_configuration-10</code>).
body	The modified alarm configuration. See Request body for details.

Request body

nbType	AlarmConfigurationDTO. (Required.)
id	The alarm configuration ID. (Required.)
label	The label of the alarm configuration. (Required.)
assetIds	Identifiers of assets that can cause the alarm. To create a motion detection alarm, enter the ID of a motion sensor, not a camera.
rule	
nbType	NumericThresholdRuleDTO or StateThresholdRuleDTO. (Required.)
id	The rule ID. (Required.)
enabled	Defines whether the rule is enabled. (Required.)
label	The label of the rule.
sensorType	The sensor asset type. (Required.)
state	Required for StateThresholdRuleDTO.
operation	EQUALS, GREATER_THAN, or LESS_THAN. Applies to value . (Required for NumericThresholdRuleDTOs.)
value	The alarm threshold. (Required for NumericThresholdRuleDTOs.)
units	The units measured by value . (Required for NumericThresholdRuleDTOs.) METERS_PER_SEC, FEET_PER_SEC, METERS_PER_MIN, FEET_PER_MIN, KVA, VA, KVA_PER_HOUR, VA_PER_HOUR, AMPS, MILLIAMPS, KA, MA, GA, TA, PA, CELSIUS, CENTIMETERS_WATER_COLUMN, INCHES_WATER_COLUMN, FAHRENHEIT, KWH, NUMERIC, HERTZ, KHZ, MHZ, GHZ, THZ, PHZ, PERCENT, RELATIVE_PERCENT, WATTS, KW, MW, GW, TW, PW, PASCAL, HPA, KPA, MPA, GFA, PSI, KVAR, VAR, KVAR_PER_HOUR, VAR_PER_HOUR, STATE, MILLISECONDS, SECONDS, MINUTES, HOURS, DAYS, WEEKS, MONTHS, YEARS, VOLTS, KV, MV, GV, TV, PV, GRAMS, KILOGRAMS, OUNCES, POUNDS, MILLIMETERS, CENTIMETERS, METERS, INCHES, FEET, YARDS, MILES, SQUARE_CENTIMETERS, SQUARE_METERS, SQUARE_INCHES, SQUARE_FEET, BYTES, KB, MB, GB, TB, PB, LITER_PER_SEC, LITER_PER_MIN, LITER_PER_HR, GAL_PER_SEC, GAL_PER_MIN, GAL_PER_HR, RPM, RUN_HOURS, STRING, DB, UNKNOWN
severity	INFO, CRITICAL, or WARNING. (Required.)
cameraIds	Enter the ID of one or more cameras to configure clip capture for the alarm.
controlConfigurations	Configurations for devices that are controlled by the alarm.
nbType	ControlConfigurationDTO.
controlSensorId	The ID of the device to control.
onAlarmState	The state the sensor changes to when the alarm is generated.
onClearState	The state the sensor changes to when the alarm is cleared.
scheduled	Determines whether the alarm is on a schedule. Defaults to false. See <i>PUT /alarms/configurations/{id}/schedule</i> , page 54 to configure a schedule.

NOTE: See GET/assets for asset IDs and sensor information.

NOTE: Possible states for each sensor type are as follows:

- SMOKE: sensor.state.smoke.smoke-detected, sensor.state.smoke.no-smoke
- BEACON: sensor.state.beacon.active, sensor.state.beacon.inactive
- VIBRATION: sensor.state.vibration.vibration-detected, sensor.state.vibration.no-vibration
- LEAK_ROPE: sensor.state.leakRope.leak, sensor.state.leakRope.no-leak
- SPOT_LEAK: sensor.state.spotLeak.leak, sensor.state.spotLeak.no-leak
- DOOR, RACK_HANDLE, CONTACT: sensor.state.sensor-value-state.open, sensor.state.sensor-value-state.closed
- OUTLET, OUTPUT_RELAY, SWITCHED_OUTLET, SWITCH: sensor.state.internalRelay.active, sensor.state.internalRelay.inactive
- DOOR_LOCK: sensor.state.lock.open, sensor.state.lock.closed
- EXTERNAL_RELAY: sensor.state.externalRelay.on, sensor.state.externalRelay.off
- MOTION: sensor.state.MOTION.motion-detected, sensor.state.MOTION.no-motion
- OUTLET, STATE, SWITCH: not supported

Example request

```
{
  "nbType": "AlarmConfigurationDTO",
  "id": "alarm_configuration-50",
  "label": "Motion door 1",
  "assetIds": [
    "sensor-48"
  ],
  "rule": {
    "nbType": "StateThresholdRuleDTO",
    "id": "rule-49",
    "enabled": true,
    "label": "Motion door 1",
    "sensorType": "MOTION",
    "operation": "EQUALS",
    "severity": "INFO",
    "state": "sensor.state.MOTION.motion-detected",
    "localizedState": "Motion Detected"
  },
  "cameraIds": [
    "camera-44"
  ],
  "controlConfigurations": [
    {
      "controlSensorId": "sensor-22",
      "onAlarmState": "sensor.state.lock.closed",
      "onClearState": "sensor.state.lock.open"
    }
  ],
  "scheduled": true
}
```

GET /alarms/configurations/{id}/schedule

Gets the schedule for an alarm configuration.

If there is no schedule for the alarm configuration, an error is generated. See *POST /alarms/configurations*, page 50 to add a schedule to an alarm.

Alarms are scheduled in 15-minute time slots for each day of the week. Time slots are set using the 24-hour clock (hh_mm). For example, if an alarm is scheduled for the `Monday_13_15` time slot, the alarm can be generated from 1:15 PM to 1:30 PM on Mondays.

Parameters

Parameter	Description
id	The ID of the alarm configuration.

PUT /alarms/configurations/{id}/schedule

Modifies the schedule for an alarm configuration.

You must schedule the alarm before the schedule can be modified. See *PUT /alarms/configurations/{id}*, page 52 or *POST /alarms/configurations*, page 50.

Alarms are scheduled in 15-minute time slots for each day of the week. Time slots are set using the 24-hour clock (hh_mm). For example, if an alarm is scheduled for the `Monday_13_15` time slot, the alarm can be generated from 1:15 PM to 1:30 PM on Mondays.

Parameters

Parameter	Description
id	The ID of the alarm.
body	The modified schedule.

Request body

```
nbType          ScheduledDTO
timeslots       true or false
(day_hh_mm)
```

GET /alarms/counts

Gets the active alarm counts by severity.

GET /alarms/export

Gets a comma-separated list of current alarms to download.

This operation returns a CSV file.

GET /alarms/{id}

Gets an alarm with the alarm ID.

Parameters

Parameter	Description
id	The ID of the alarm to get (for example, <code>alarm-123</code>).

appliance

GET /appliance

Gets the appliance firmware version, product name, serial number, and IP addresses.

GET /appliance/locales

Gets information about the appliance's country and language.

GET /appliance/mode

Gets the appliance mode.

Technical support may use this operation for troubleshooting.

GET /appliance/resetconfig

Resets the appliance to factory defaults as of its last firmware update.

This operation resets *all configurations* and requires a super user session.

assets

GET /assets

Retrieves a list of connected assets.

Assets include both internal and external sensors and devices. Internal assets are located inside their parent assets. For example, motion sensors are internal to Cameras, their parent assets.

The Appliance and its internal sensors (switched outlet, outputs 1 and 2, current inputs 1 and 2, and rack access) are always listed as assets, even when no other devices are connected.

Non-wireless assets are always in END_DEVICE mode.

All parameters except **types** are inactive if null or empty.

Parameters

Parameter	Description
types	Comma-separated list of asset types. Defaults to POD, SENSOR, CAMERA.
podProtocolTypes	Comma-separated list of pod protocol types
sensor-Types	Comma-separated list of sensor types.
sensor-PortTypes	Comma-separated list of sensor port types.
ids	Optional comma-separated list of asset id's.
includeParent	True if parent assets should be included. False for only direct matches
include-Children	True if child assets should be included. False for only direct matches.

GET /assets/attributes

Retrieves a list of asset attributes.

Parameters

Parameter	Description
id	The ID of the asset.

GET /assets/knownSensorTypes

Get a list of sensor types connected to the appliance.

The list of known sensors types includes sensors internal to the appliance.

GET /assets/sensors/controllableTypes

Gets the sensor types for which a you can perform a manual state change.

GET /assets/sensors/custom/availableTypes

Gets a list of sensor types that a custom (4-20 mA) sensor can be mapped to.

GET /assets/sensors/custom/{id}

Gets the configuration for a customizable sensor.

Only customizable sensors have the `sensorMapperConfigID`. You can find this ID under *GET /assets*, page 55.

Parameters

Parameter	Description
id	The ID of the sensor's custom configuration (the <code>sensorMapperConfigID</code>).

PUT /assets/sensors/custom/{id}

Modifies the configuration for a customizable sensor.

You can map a voltage or current input sensor to a customizable sensor type with a different range of measurement. For example, a sensor that measures current input from 4 to 20 mA can be mapped to a sensor that measures airflow from 0 to 40 feet per second.

Parameters

Parameter	Description
id	The ID of the sensor's custom configuration (the <code>sensorMapperConfigID</code>).
body	The modified configuration. See Request body for details.

NOTE: Only customizable sensors have the `sensorMapperConfigID`. You can find this ID under *GET /assets*, page 55.

Request body

<code>nbType</code>	SensorMapperConfigDTO
<code>id</code>	The ID of the sensor's custom configuration (the <code>sensorMapperConfigID</code>)
<code>sensorAssetId</code>	The id of the sensor asset.
<code>sensorTypeInput</code>	The source sensor type: VOLTAGE or CURRENT_INPUT.
<code>sensorTypeMapped</code>	The target sensor type, which the input sensor values are mapped to: AIRFLOW, AIRFLOW_SPEED, CURRENT_INPUT, CURRENT_INPUT_DB, DEWPOINT, RELATIVE_HUMIDITY, TEMPERATURE, or VOLTAGE.
<code>sensorInputMin</code>	A whole number that represents the minimum measurement in milliamperes (mA). This is mapped to the <code>sensorMappedOutputMin</code> . Must be less than the <code>sensorInputMax</code> .
<code>sensorInputMax</code>	A whole number that represents the maximum measurement in mA. This is mapped to the <code>sensorMappedOutputMax</code> . Must be greater than the <code>sensorInputMin</code> .
<code>sensorMappedOutputMin</code>	A number representing the minimum value measured by the sensor. Must be less than <code>sensorMappedOutputMax</code> .
<code>sensorMappedOutputMax</code>	A number representing the maximum value measured by the sensor. Must be greater than <code>sensorMappedOutputMin</code> .
<code>inputMin</code>	4 for current input sensors and 0 for voltage sensors.
<code>inputMax</code>	20 for current input sensors and 5 for voltage sensors.
<code>unitsInput</code>	Corresponds to <code>sensorTypeInput</code>
<code>unitsOutput</code>	Corresponds to the <code>sensorTypeMapped</code> .

NOTE: Possible values for `unitsInput` and `unitsOutput` include the following: METERS_PER_SEC, FEET_PER_SEC, METERS_PER_MIN, FEET_PER_MIN, KVA, VA, KVA_PER_HOUR, VA_PER_HOUR, AMPS, MILLIAMPS, KA, MA, GA, TA, PA, CELSIUS, CENTIMETERS_WATER_COLUMN, INCHES_WATER_COLUMN, FAHRENHEIT, KWH, NUMERIC, HERTZ, KHZ, MHZ, GHZ, THZ, PHZ, PERCENT, RELATIVE_PERCENT, WATTS, KW, MW, GW, TW, PW, PASCAL, HPA, KPA, MPA, GPA, PSI, KVAR, VAR, KVAR_PER_HOUR, VAR_PER_HOUR, STATE, MILLISECONDS, SECONDS, MINUTES, HOURS, DAYS, WEEKS, MONTHS, YEARS, VOLTS, KV, MV, GV, TV, PV, GRAMS, KILOGRAMS, OUNCES, POUNDS, MILLIMETERS, CENTIMETERS, METERS, INCHES, FEET, YARDS, MILES, SQUARE_CENTIMETERS, SQUARE_METERS, SQUARE_INCHES, SQUARE_FEET, BYTES, KB, MB, GB, TB, PB, LITER_PER_SEC, LITER_PER_MIN, LITER_PER_HR, GAL_PER_SEC, GAL_PER_MIN, GAL_PER_HR, RPM, RUN_HOURS, STRING, DB, UNKNOWN

GET /assets/sensors/states

Returns the possible states for specified sensor types, or all sensor types if no argument is given.

State sensor types include BEACON, CONTACT, DOOR, DOOR_LOCK, EXTERNAL_RELAY, LEAK_ROPE, OUTPUT_RELAY, RACK_HANDLE, SMOKE, SPOT_LEAK, SWITCHED_OUTLET, TEMPERATURE, and VIBRATION. (OUTLET, STATE, and SWITCH are not supported.)

Parameters

Parameter	Description
sensor-Types	Comma-separated list of sensor types, or all sensor types if not set.

PUT /assets/sensors/{id}/control

Manually changes the state of a controllable sensor.

Parameters

Parameter	Description
id	The ID of the sensor
action	The state to change to.

NOTE: Possible actions (states) for each controllable sensor type are as follows:

- BEACON: sensor.state.beacon.active, sensor.state.beacon.inactive
- SWITCHED_OUTLET, OUTPUT_RELAY: sensor.state.internalRelay.active, sensor.state.internalRelay.inactive
- DOOR_LOCK: sensor.state.lock.open, sensor.state.lock.closed

OUTLET is not supported

GET /assets/timeseries

Get the time series data for one or more sensor assets.

This operation returns a CSV file. Each item in the series array consists of a timestamp (milliseconds since epoch) and the value (numeric or state).

Parameters

Parameter	Description
id	Comma-separated list of sensor asset IDs to get details on, or all sensors if not set.
interval	The time interval of interest (from oldest to newest).

GET /assets/timeseries-export

Gets the time series data for one or more sensor assets in CSV format.

Parameters

Parameter	Description
ids	The IDs of the sensor assets to get details on.
interval	The time interval of interest (from oldest to newest).

DELETE /assets/{assetIds}

Deletes one or more assets by passing a comma-separated string of asset ID values in the URL.

Parameters

Parameter	Description
assetIds	A comma-separated string of asset IDs.

PUT /assets/{ids}

Modifies an asset label.

Parameters

Parameter	Description
ids	One or more comma-separated asset IDs
label	The label to rename to.

cameras

GET /cameras/cameraPassword/{id}

Get a camera's password by id.

Parameters

Parameter	Description
id	The ID of the camera. For example, camera-12.

GET /cameras/clip

Gets a list of all video clips recorded for a given camera ID.

Video clips are recorded for alarms with the Clip Capture feature enabled.

Parameters

Parameter	Description
cameraId	The ID of the camera. Use <i>GET /assets</i> , page 55 to retrieve a list of camera IDs.

GET /cameras/clip/settings

Gets the clip capture settings.

When clip capture is enabled for an alarm configuration, video is recorded from before and after the alarm based on the video capture setting.

POST /cameras/clip/settings

Configures the clip capture settings.

When clip capture is enabled for an alarm, video is stored from the time before and after the alarm. Clip capture settings determines how much video is stored from before and after the alarm.

Parameters

Parameter	Description
body	The modified clip capture settings. See Request body for details.

Request body

<code>nbType</code>	ClipCaptureSettingsDTO
<code>precapture</code>	Seconds of video recorded before the alarm is generated
<code>postcapture</code>	Seconds video recorded after the alarm is cleared

GET /cameras/clip/{ids}/metadata

Gets the metadata for specified camera clips.

Parameters

Parameter	Description
ids	A comma-separated list of camera clip IDs. Note that these are NOT the camera IDs.

GET /cameras/clip/{id}

Gets a specific camera image.

This operation returns a JPEG file.

Parameters

Parameter	Description
id	The camera clip ID (not the camera ID). For example, <code>camera_clip-42</code> .
index	The frame number (cannot be greater than the number of frames for the video clip).

GET /cameras/clip/{id}/download

Gets a zipped file of all the frames in one video clip.

This operation returns a ZIP file.

Parameters

Parameter	Description
id	The ID of the camera clip to retrieve.

GET /cameras/settings/{id}

Get a camera's settings by ID.

Parameters

Parameter	Description
id	The camera ID.

PUT /cameras/settings/{id}

Modifies a camera's settings.

Parameters

Parameter	Description
id	The Camera ID.
body	The modified settings. See Request body for details.

Request body

nbType	CameraSettingsDTO.
oem	Always true.
motionMask	Motion masking creates areas (or masks) where the camera does not detect motion.
nbType	MotionMaskDTO.
enable	Determines whether motion masking is enabled.
maskAreas	The camera image is divided into masking boxes regardless of resolution (the image is always 40 boxes wide by 30 boxes tall). The boxes are represented by 1s and 0s in rows from top to bottom. 1s represent boxes that can detect motion. 0s represent boxes that are masked and cannot detect motion.
sensitivity	A number (0-100) representing each pixel's sensitivity to motion. Higher numbers indicate higher sensitivity.
percentage	A number representing the minimum change between frames (in percent of pixels) that is considered enough movement to generate motion alarms. Lower numbers indicate higher sensitivity.
interval	The minimum number of seconds before a Motion event can be cleared.
frameRate	
nbType	FrameRateDTO.
rate	The number of frames recorded per second (f/s).
min	The minimum possible frame rate.
max	The maximum possible frame rate.
resolution	The pixel resolution of each camera frame.
availableResolutions	Do not enter a value – retrieves possible resolutions for the camera

GET /cameras/snapshot/{id}

Gets a high-quality image from the live feed.

Parameters

Parameter	Description
id	The camera ID.

DELETE /cameras/streaming/{id}

Stops the specified camera stream.

You must delete the stream ID to close the camera stream.

Parameters

Parameter	Description
id	The camera ID, e.g., camera-1.
streamId	The stream ID (see <i>DELETE /cameras/streaming/{id}</i> , page 62).

GET /cameras/streaming/{id}

Gets an ID to view the camera stream with.

This operation allows you to view the camera feed. The response stream remains open as long as the camera continues to film until you close the connection.

To test this in the online documentation, enter the following in the URL address bar:
https://<appliance_IP_address>/rest/cameras/streaming/<camera_ID>?streamid=<stream_ID>

For example:

<https://10.119.110.120/rest/cameras/streaming/camera-1?stream=1234>

Use *DELETE /cameras/streaming/{id}*, page 62 to cancel the stream before closing the stream. Otherwise, you may get an error response.

NOTE: Internet Explorer does not support this feature.

Parameters

Parameter	Description
id	The camera ID.
streamId	A random number of your choice.
framesPerSecond	The number of frames per second. This can be 1–30.

GET /cameras/thumbnail/{id}

Gets a low-quality image from the live feed.

Parameters

Parameter	Description
id	The camera ID.

configuration

DELETE /configuration

Deletes the backup file stored on the appliance.

GET /configuration/backup

Gets a downloadable backup file for the appliance.

The backup file is not encrypted. Save the backup file in a secure location.

PUT /configuration/clone

Clones the configuration of one appliance to another.

This operation configures appliance and sensor settings using the backup file stored on the appliance (see *PUT /configuration/upload*, page 63). It does not transfer stored sensor data or logs.

PUT /configuration/restore

Restores the appliance to a previous configuration.

This operation restores appliance settings, sensor data, and camera clips using the backup file stored on the appliance (see *PUT /configuration/upload*, page 63). It does not restore logs.

PUT /configuration/upload

Uploads the backup file to the appliance holding area.

You can get a backup file from *GET /configuration/backup*, page 63.

Parameters

Parameter	Description
file	The backup file.

GET /configuration/version

Gets the firmware information of the backup file in the holding area.

This operation only fills in the `applianceVersion` attribute in the response.

directory

GET /directory/search

Gets information for rack access users registered through LDAP.

DELETE /directory/settings

Deletes the LDAP configuration information.

Parameters

Parameter	Description
id	Reserved for future use.

GET /directory/settings

Gets the settings for LDAP authentication.

PUT /directory/settings

Modifies the settings for LDAP authentication.

Parameters

Parameter	Description
body	The modified settings. See Request body for details.

Request body

nbType	IdentityStoreDTO.
name	Reserved for future use.
id	Reserved for future use.
storetype	AD or OpenLDAP. AD = Microsoft Active Directory, OpenLDAP = Open Lightweight Directory Access Protocol other than Microsoft Active Directory.
enabled	Determines whether LDAP is enabled.
host	The host name of the authentication server.
port	The port used to connect to the authentication server.
ssl	Determines whether to connect to the authentication server with SSL/TLS.
securityPrincipal	The user name to log on to the authentication server (the full distinguished name of the LDAP directory).
securityCredential	The password to log on to the authentication server. For security purposes, this appears as an empty string ("").
membershipAttribute	Reserved for future use.
baseContext	The base distinguished name of the LDAP directory.

The following parameters must correspond to settings on your LDAP server. Enter string values in the following format: "parameter": "parameter=value"

For example: "userObjectClass": "userObjectClass=employee",

userObjectClass	Term defined for users on the LDAP server.
userObjectFilter	Select an LDAP objectClass to use as a filter for the Active Directory or LDAP server.
usernameAttribute	These can be mapped to attributes configured on your LDAP server.
groupnameAttribute	
firstnameAttribute	
surnameAttribute	
emailAttribute	
label	Reserved for future use.
customerAttributes	Attributes created by the company.
validateSSL	Reserved for future use.
enableNestedGroup	Always false. This feature is reserved for future use.
pageSize	Reserved for future use.
followReferrals	Reserved for future use.

testLdapUser	
nbType	LdapUserDTO
username	The user's username in the LDAP server. Not used in this operation.
password	The user's password in the LDAP server. Not used in this operation.

POST /directory/settings/test

Test new LDAP settings before modifying the existing ones.

Parameters

Parameter	Description
body	The new LDAP settings. See Request body for details.

Request body

nbType	IdentityStoreDTO.
name	Reserved for future use.
id	Reserved for future use.
storetype	AD or OpenLDAP. AD = Microsoft Active Directory, OpenLDAP = Open Lightweight Directory Access Protocol other than Microsoft Active Directory.
enabled	Determines whether LDAP is enabled.
host	The host name of the authentication server.
port	The port used to connect to the authentication server.
ssl	Determines whether to connect to the authentication server with SSL/TLS.
securityPrincipal	The user name to log on to the authentication server (the full distinguished name of the LDAP directory).
securityCredential	The password to log on to the authentication server. For security purposes, this appears as an empty string ("").
membershipAttribute	Reserved for future use.
baseContext	The base distinguished name of the LDAP directory.

The following parameters must correspond to settings on your LDAP server. Enter string values in the following format: "parameter": "parameter=value"

For example: "userObjectClass": "userObjectClass=employee",

userObjectClass	Term defined for users on the LDAP server.
userObjectFilter	Select an LDAP objectClass to use as a filter for the Active Directory or LDAP server.
usernameAttribute	These can be mapped to attributes configured on your LDAP server.
groupnameAttribute	
firstnameAttribute	
surnameAttribute	
emailAttribute	
label	Reserved for future use.
customerAttributes	Attributes created by the company.
validateSSL	Reserved for future use.
enableNestedGroup	Always false. This feature is reserved for future use.
pageSize	Reserved for future use.
followReferrals	Reserved for future use.

testLdapUser	
nbType	LdapUserDTO
username	The user's username in the LDAP server. Not used in this operation.
password	The user's password in the LDAP server. Not used in this operation.

POST /directory/settings/testUserSchema

Authenticates an existing user to test new LDAP settings before modifying the existing settings.

Parameters

Parameter	Description
body	The modified settings. See Request body for details.

Request body

nbType	IdentityStoreDTO.
name	Reserved for future use.
id	Reserved for future use.
storetype	AD or OpenLDAP. AD = Microsoft Active Directory, OpenLDAP = Open Lightweight Directory Access Protocol other than Microsoft Active Directory.
enabled	Determines whether LDAP is enabled.
host	The host name of the authentication server.
port	The port used to connect to the authentication server.
ssl	Determines whether to connect to the authentication server with SSL/TLS.
securityPrincipal	The user name to log on to the authentication server (the full distinguished name of the LDAP directory).
securityCredential	The password to log on to the authentication server. For security purposes, this appears as an empty string ("").
membershipAttribute	Reserved for future use.
baseContext	The base distinguished name of the LDAP directory.

The following parameters must correspond to settings on your LDAP server. Enter string values in the following format: "parameter": "parameter=value"

For example: "userObjectClass": "userObjectClass=employee",

userObjectClass	Term defined for users on the LDAP server.
userObjectFilter	Select an LDAP objectClass to use as a filter for the Active Directory or LDAP server.
usernameAttribute	These can be mapped to attributes configured on your LDAP server.
groupnameAttribute	
firstnameAttribute	
surnameAttribute	
emailAttribute	
label	Reserved for future use.
customerAttributes	Attributes created by the company.
validateSSL	Reserved for future use.
enableNestedGroup	Always false. This feature is reserved for future use.
pageSize	Reserved for future use.
followReferrals	Reserved for future use.

testLdapUser	
nbType	LdapUserDTO
username	The user's username in the LDAP server.
password	The user's password in the LDAP server.

discoveries

GET /discoveries

Gets all discovered devices.

This is an Alpha feature. Discovered devices are devices on the public network that the appliance has established communication with.

POST /discoveries

Initiates the discovery process for a device on the public network.

This is an Alpha feature.

Parameters

Parameter	Description
body	The discovery configuration. See Request body for details.

Request body

nbType	DiscoveryConfigDTO.
id	The ID of the discovery configuration. Automatically generated by the appliance.
label	A user-friendly name for the discovery configuration.
hostname	DNS host name or IP address of the IP device.
macAddress	Mac address of the downstream device.
autoDiscovered	Always true.
credentials:	
nbType	DiscoveryCredentialsDTO
id	The id of the credential configuration. Not used.
protocol	ONVIF or SNMP. (MODBUS is reserved for future use.)
port	The port to connect to downstream device.
enabled	Determines whether discovery is enabled?
onvifUserName	Required if the protocol is ONVIF.
onvifPassword	Required if the protocol is ONVIF.
snmpCommunityString	The read community name. Required if the protocol is SNMP and the snmpVersion is VERSION1.
snmpWriteCommunityString	The write community name. Required if the protocol is SNMP and the snmpVersion is VERSION1.
snmpVersion	VERSION1 or VERSION3. Required if the protocol is SNMP.
The following are required if the protocol is SNMP and the snmpVersion is VERSION3:	
snmpV3Username	The SNMP user name.
snmpV3Authentication	The authentication protocol. MD5, SHA1, SHA224, SHA256, SHA384, or SHA512
snmpV3AuthPassword	The authentication password.
snmpV3Encryption	The encryption protocol. DES, DES3, AES128, AES192, AES256.
snmpV3EncPassword	The encryption password.
The following are reserved for future use:	
targetDeviceType	
modbusDeviceType	
modbusUsername	
modbusPassword	
modbusSlaveAddress	
ipAddress	The IP address of the downstream device.
communicationState	The internal communication state of the device (communicating, authenticating, etc.). Not used in this operation.
forwardingURI	The link to the admin page of the downstream device. Not used in this operation. Port forwarding must be enabled to get a forwarding URI (see <i>settings/iptables</i> , page 87).

DELETE /discoveries/{ids}

Removes one or more downstream devices by ID.

This is an Alpha feature. This operation also removed IPTable entries.

Parameters

Parameter	Description
id	Comma-separated list of discovery IDs.

GET /discoveries/{ids}

This is an Alpha feature.

Parameters

Parameter	Description
ids	Comma-separated list of discovery IDs.

PUT /discoveries/{id}

Modifies a discovery configuration and re-starts the discovery process for a device on the public network.

This is an Alpha feature.

You can use this feature to update the credentials for a downstream device.

Parameters

Parameter	Description
id	The discovery ID.
body	The modified discovery configuration. See Request body for details.

Request body

nbType	DiscoveryConfigDTO.
id	The ID of the discovery configuration. Automatically generated by the appliance.
label	A user-friendly name for the discovery configuration.
hostname	DNS host name or IP address of the IP device.
macAddress	Mac address of the downstream device.
autoDiscovered	Always true.
credentials:	
nbType	DiscoveryCredentialsDTO
id	The id of the credential configuration. Not used.
protocol	ONVIF or SNMP. (MODBUS is reserved for future use.)
port	The port to connect to downstream device.
enabled	Determines whether discovery is enabled.
onvifUserName	Required if the protocol is ONVIF.
onvifPassword	Required if the protocol is ONVIF.
snmpCommunityString	The read community name. Required if the protocol is SNMP and the snmpVersion is VERSION1.
snmpWriteCommunityString	The write community name. Required if the protocol is SNMP and the snmpVersion is VERSION1.
snmpVersion	VERSION1 or VERSION3. Required if the protocol is SNMP.
The following are required if the protocol is SNMP and the snmpVersion is VERSION3:	
snmpV3Username	The SNMP user name.
snmpV3Authentication	The authentication protocol. MD5, SHA1, SHA224, SHA256, SHA384, or SHA512
snmpV3AuthPassword	The authentication password.
snmpV3Encryption	The encryption protocol. DES, DES3, AES128, AES192, AES256.
snmpV3EncPassword	The encryption password.
The following are reserved for future use:	
targetDeviceType	
modbusDeviceType	
modbusUsername	
modbusPassword	
modbusSlaveAddress	
ipAddress	The IP address of the downstream device.
communicationState	The internal communication state of the device (communicating, authenticating, etc.). Not used in this operation.
forwardingURI	The link to the admin page of the downstream device. Not used in this operation. Port forwarding must be enabled to get a forwarding URI (see <i>settings/iptables</i> , page 87).

firmwareupdate

DELETE /firmwareupdate

Deletes the previously uploaded file.

POST /firmwareupdate

Starts or stops the firmware update process.

Parameters

Parameter	Description
action	INSTALL = Install the firmware version in the holding area. ABORT = Stop the current firmware update.

PUT /firmwareupdate

Uploads a new firmware version to the appliance holding area.

Parameters

Parameter	Description
file	The firmware update file.

GET /firmwareupdate/status

Gets the progress status of the appliance firmware update.

The progressPct value shows what percent of the update process has been completed. Positive numbers indicate progress. Negative values indicate errors.

GET /firmwareupdate/version

Gets the version information of the firmware package in the holding area.

logging

GET /logging/download

Gets the appliance log in a downloadable format.

Parameters

Parameter	Description
format	Specify which file format to use. Defaults to comma-separated values (CSV).

GET /logging/logs

Gets the last *n* log items.

Parameters

Parameter	Description
numEntries	The number of log entries to get.

GET /logging/settings

Gets the logging settings.

POST /logging/settings

Sets the logging settings.

Parameters

Parameter	Description
body	The modified alarm configuration. See Request body for details.

Request body

nbType	ApplianceLogSettingsDTO
id	Automatically generated by the appliance.
level	Events with levels lower than the selected level will not be recorded in the appliance log. From highest to lowest, possible levels include EMERGENCY, ALERT, CRITICAL, ERROR, WARNING, NOTICE, INFORMATION, and DEBUG.

notifications

GET /notifications

Gets a list of all notification policies in the system.

Parameters

Parameter	Description
notifytype	The policy type.

POST /notifications

Creates a notification policy.

You must configure an SMTP server to send email notifications. Currently, you can only create new Email policies.

Parameters

Parameter	Description
body	The settings for the notification policy. See Request body for details.

Request body

<code>nbType</code>	NotificationPolicyDTO
<code>id</code>	The id of the notification policy. Automatically generated by the appliance.
<code>label</code>	The label of the notification policy.
<code>recipients</code>	Required if the notifytype is EMAIL.
<code>nbType</code>	RecipientDTO
<code>id</code>	The ID of the notification recipient. Automatically generated by the appliance.
<code>address</code>	The email address of the recipient.
<code>deviceSpecification</code>	
<code>nbType</code>	DeviceSpecificationDTO
<code>id</code>	The ID of the specification. Automatically generated by the appliance.
<code>deviceTypes</code>	Not used.
<code>severities</code>	The alarm severities that cause the notification to be sent.
<code>notifytype</code>	EMAIL only. HTTP_POST and SNMP_TRAP are reserved for future use.
<code>settings</code>	
<code>nbType</code>	NotificationSettingsDTO
<code>id</code>	The id of the notification configuration. Automatically generated by the appliance.
<code>locale</code>	Always en_US.
<code>imperial</code>	Measurement units (true = imperial, false = metric).
<code>time24</code>	Time format (true = 24-hour, false = 12-hour).
<code>autoScale</code>	When true, autoscale converts detailed sensor measurements to more manageable units. For example, a sensor that measures milliseconds may display measurement in seconds when autoscale is on.

DELETE /notifications/{id}

Deletes one or more notification policies.

Parameters

Parameter	Description
id	A comma-separated list of policy IDs.

GET /notifications/{id}

Gets a notification policy by ID.

Parameters

Parameter	Description
id	The policy ID (for example, <code>notification_policy-102</code>).

PUT /notifications/{id}

Modifies a notification policy.

You can modify existing Email notification policies, or the default trap notification policy.

Parameters

Parameter	Description
id	The ID of the notification policy to be modified.
body	The modified notification policy. See Request body for details.

Request body

nbType	NotificationPolicyDTO
id	The id of the notification policy. Automatically generated by the appliance.
label	The label of the notification policy.
recipients	Required if the notifytype is EMAIL.
nbType	RecipientDTO
id	The ID of the notification recipient. If unconfigured, a new ID is generated.
address	The email address of the recipient.
deviceSpecification	
nbType	DeviceSpecificationDTO
id	The ID of the specification.
deviceTypes	Reserved for future use.
severities	The alarm severities that cause the notification to be sent.
notifytype	EMAIL or SNMP_TRAP. HTTP_POST is reserved for future use.
settings	
nbType	NotificationSettingsDTO
id	The id of the notification configuration. Automatically generated by the appliance.
locale	Always en_US.
imperial	Measurement units (true = imperial, false = metric).
time24	Time format (true = 24-hour, false = 12-hour).
autoScale	When true, autoscale converts detailed sensor measurements to more manageable units. For example, a sensor that measures milliseconds may display measurement in seconds when autoscale is on.

ping

GET /ping

Verifies that the appliance server is still running.

rackaccess

POST /rackaccess/door

Creates a door configuration that can be applied to rack access users.

You can create more than one configuration per door. Existing door configurations are only viewable when associated with a rack access user (see *GET /rackaccess/user*, page 78).

Parameters

Parameter	Description
body	The door configuration. See Request body for details.

Request body

nbType	DoorConfigurationDTO.
id	The ID of the configuration. Automatically generated by the appliance.
autolockSeconds	The number of seconds before an unlocked handle re-locks. A handle only re-locks when both the handle and door are closed.
longAccess	If true, disables the autolockSeconds setting. (The global auto lock setting is still in effect.)
rackDoorId	The ID of the door switch sensor.
rackHandleId cardReaderId doorLockId	The rackHandleId, cardReaderId, and doorLockId are all sensor assets with the same handle (in GET/assets, the handle is represented as a podAsset).

PUT /rackaccess/door

Modifies a door configuration.

You can use GET/rackaccess/user to discover existing door configurations.

Parameters

Parameter	Description
body	The modified door configuration. See Request body for details.

Request body

nbType	DoorConfigurationDTO.
id	The ID of the configuration.
autolockSeconds	The number of seconds before an unlocked handle re-locks. A handle only re-locks when both the handle and door are closed.
longAccess	If true, disables the autolockSeconds setting. (The global auto lock setting is still in effect.)
rackDoorId	The ID of the door switch sensor.
rackHandleId cardReaderId doorLockId	The rackHandleId, cardReaderId, and doorLockId are all sensor assets with the same handle (in GET/assets, the handle is represented as a podAsset).

DELETE /rackaccess/door/{id}

Deletes a door configuration.

You can retrieve door configurations from rack access user profiles.

Parameters

Parameter	Description
id	The ID of the door configuration.

GET /rackaccess/door/{id}/schedule

Gets a user's rack access schedule.

You can retrieve door configuration IDs from rack access user profiles.

Rack access is scheduled in 15-minute intervals for each day of the week. Intervals are configured using the 24-hour format: <hours>_<minutes>.

Parameters

Parameter	Description
id	The ID of the door configuration.

PUT /rackaccess/door/{id}/schedule

Modifies the schedule for a door configuration.

You can retrieve door configuration IDs from rack access user profiles. By default, access is allowed at all times.

Parameters

Parameter	Description
id	The ID of the door configuration.
body	The modified schedule. See Request body for details.

Request body

nbType	ScheduleDTO.
Label	The label for the schedule.
sunday_0_0	Rack access is scheduled in 15-minute intervals for each day of the week. Set an interval to true to allow access during that time, or set the interval to false to deny access during that time. Intervals are configured using the 24-hour format: <hours>_<minutes>.
...	
...	

GET /rackaccess/logs

Gets a list of rack access events.

Parameters

Parameter	Description
pageNumber	The zero-based number for the page requested (0=1, 1=2, etc.).
pageSize	The number of log events in a page.
order	ASC (ascending) or DESC (descending).

GET /rackaccess/logs/export

Gets a downloadable list of all rack access events in CSV format.

GET /rackaccess/settings

Gets the Global Auto Lock Timeout setting.

Auto lock timeout determines when an un-locked handles re-lock. A handle only re-locks when both the handle and door are closed.

The Global Auto Lock Timeout setting applies to all connected handles.

POST /rackaccess/settings

Modifies the Global Auto Lock Timeout setting.

Auto lock timeout determines when an un-locked handles re-lock. A handle only re-locks when both the handle and door are closed

The Global Auto Lock Timeout setting applies to all connected handles.

Parameters

Parameter	Description
body	The new setting to change to.

Request body

<code>nbType</code>	RackAccessSettingsDTO.
<code>autoLockMinutes</code>	Must be 1 or greater.

GET /rackaccess/user

Gets a list of rack access user profiles.

Rack access users are associated with a specific rack access card and do not have access to the Web UI.

Parameters

Parameter	Description
registered	Registration status (true = registered, false = unregistered). If unspecified, retrieves information for all users.

PUT /rackaccess/user

Modifies profile settings for a rack access user.

An unregistered rack access user is created automatically when you swipe a new rack access card.

Parameters

Parameter	Description
body	The modified user profile. See Request body for details.

Request body

nbType	RackAccessUserDTO
id	the rack access user ID (separate from user IDs for the API/Web UI)
label	the rack access user label (or name) - cardNumber: the number of the rack access card can not be altered
rackAccessUserType	LOCAL or LDAP. You must configure an LDAP server (PUT/directory/settings) before an LDAP user can be registered.
registered	Only registered users can access the rack.
doorConfigurations	You can enter only the nbType and ID of an existing configuration or create a new configuration.
nbType	DoorConfigurationDTO
id	The ID of a door configuration for a particular user. For example, door_configuration-75.
autolockSeconds	The number of seconds before an unlocked handle re-locks. A handle only re-locks when both the handle and door are closed.
longAccess	If true, disables autolockSeconds. (The global auto lock setting is still in effect.)
rackDoorId	The ID of the door switch sensor
rackHandleId	The rackHandleId, cardReaderId, and doorLockId are all sensor assets with the same handle (in GET/assets, the handle is represented as a podAsset).
cardReaderId	
doorLockId	
distinguishedName	The full distinguished name (or user name) used to check if the user is still active on the LDAP server. Required if rackAccessUserType is LDAP.

DELETE /rackaccess/door/{id}

Deletes a door configuration.

You can retrieve door configurations from rack access user profiles.

Parameters

Parameter	Description
id	The ID of the door configuration.

GET /rackaccess/user/{id}

Gets the profile for a single rack access user.

Parameters

Parameter	Description
id	The user ID.

session

DELETE /session

Explicitly ends a session by deleting the attributes associated with it.

GET /session

Gets information about the current user and validates that the session is still active.

POST /session

Login using HTTP BASIC authentication.

The login parameters are passed in the HTTP Authorization request header.

settings/dceconfig

GET /settings/dceconfig

Gets the global StruxureWare Data Center Expert (DCE) configuration settings for the appliance.

POST /settings/dceconfig

Creates the initial DCE configuration settings.

This will behave like a PUT if the settings already exist.

Parameters

Parameter	Description
body	The DCE proxy settings.

Request body

nbType	DCEConfigSettingsDTO
dceUrl	Reserved for future use.
UseTrustCertificate	If true (recommended), requires the DCE Certificate to be in the NetBotz Trust store for a successful connection to DCE.
VerifyHostname	If true the certificate's host name must match the DCE's host name. If false, the host name is ignored. Always false for self-signed certificates from DCE.

Example

Request

```
{
  "nbType": "DCEConfigSettingsDTO",
  "dceUrl": null,
  "useTrustStoreCertificate": true,
  "verifyHostname": false
}
```

Response

```
{
  "nbType": "DCEConfigSettingsDTO",
  "dceUrl": null,
  "useTrustStoreCertificate": true,
  "verifyHostname": false
}
```

PUT /settings/dceconfig

Modifies the DCE configuration settings.

Parameters

Parameter	Description
body	The modified DCE proxy settings.

Request body

<code>nbType</code>	DCEConfigSettingsDTO
<code>dceUrl</code>	Reserved for future use.
<code>UseTrustCertificate</code>	If true (recommended), requires the DCE Certificate to be in the NetBotz Trust store for a successful connection to DCE.
<code>VerifyHostname</code>	If true the certificate's host name must match the DCE's host name. If false, the host name is ignored. Always false for self-signed certificates from DCE.

Example

Request

```
{
  "nbType": "DCEConfigSettingsDTO",
  "dceUrl": null,
  "useTrustStoreCertificate": true,
  "verifyHostname": false
}
```

Response

```
{
  "nbType": "DCEConfigSettingsDTO",
  "dceUrl": null,
  "useTrustStoreCertificate": true,
  "verifyHostname": false
}
```

settings/dceregistration

DELETE /settings/dceRegistration

Deletes an existing DCE registration

If the registration does not exist, the request will return success.

Parameters

Parameter	Description
body	The DCE registration to be deleted.

GET /settings/dceRegistration

Gets a list of all registered DCE accounts that this appliance sends alert images to.

POST /settings/dceRegistration

Creates a new DCE registration.

If the registration is a duplicate, it will not be added, but the request will return success.

Parameters

Parameter	Description
body	A JSON representation of the DCE registration. The registration is a URL used to communicate with the DCE server.

Request body

nbType	DceRegistrationSettingsNodeDTO
id	Automatically generated by the appliance.

settings/defaultCredentials

GET /settings/defaultCredentials

Returns the default credentials for downstream devices.

If the default credentials do not match the credentials required by a downstream device, the appliance will not be able to communicate with it. (However, the device can still be discovered).

Parameters

Parameter	Description
body	The configured credentials. See Request body for details.

Request body

nbType	DefaultCredentialsSettingsDTO
DefaultCredentialsSnmpV1SettingsDTO	
nbType	DefaultCredentialsSnmpV1SettingsDTO.
readOnlyCommunityName	The read only community name.
writeCommunityName	The write community name.
DefaultCredentialsSnmpV3-SettingsDTO	
nbType	DefaultCredentialsSnmpV3SettingsDTO.
userName	The SNMPv3 user name.
securityType	NOAUTH_NOPRIV = no authentication or encryption. Authentication and encryption protocols/passwords are not required. AUTH_NOPRIV = authentication but no encryption. Protocols/passwords are required for authentication, but not for encryption. AUTH_PRIV = authentication and encryption. All protocols and passwords required.
authenticationProtocol	MD5, SHA1, SHA224, SHA256, SHA384, or SHA512.
authenticationPassword	The authentication password for SNMPv3.
encryptionProtocol	DES, DES3, AES128, AES192, or AES256.
encryptionPassword	The encryption password for SNMPv3
DefaultCredentialsOnvif-SettingsDTO	
nbType	DefaultCredentialsOnvifSettingsDTO.
userName	The Onvif user name.
password	The Onvif password.
algorithm	Reserved for future use.

POST /settings/defaultCredentials

Sets default credentials for the discovery of downstream devices.

If the default credentials do not match the credentials required by a downstream device, the appliance will not be able to communicate with it. (However, the device can still be discovered).

Parameters

Parameter	Description
body	The configured credentials. See Request body for details.

Request body

nbType	DefaultCredentialsSettingsDTO
DefaultCredentialsSnmpV1SettingsDTO	
nbType	DefaultCredentialsSnmpV1SettingsDTO.
readOnlyCommunityName	The read only community name.
writeCommunityName	The write community name.
DefaultCredentialsSnmpV3SettingsDTO	
nbType	DefaultCredentialsSnmpV3SettingsDTO.
userName	The SNMPv3 user name.
securityType	NOAUTH_NOPRIV = no authentication or encryption. Authentication and encryption protocols/passwords are not required. AUTH_NOPRIV = authentication but no encryption. Protocols/passwords are required for authentication, but not for encryption. AUTH_PRIV = authentication and encryption. All protocols and passwords required.
authenticationProtocol	MD5, SHA1, SHA224, SHA256, SHA384, or SHA512.
authenticationPassword	The authentication password for SNMPv3.
encryptionProtocol	DES, DES3, AES128, AES192, or AES256.
encryptionPassword	The encryption password for SNMPv3
DefaultCredentialsOnvifSettingsDTO	
nbType	DefaultCredentialsOnvifSettingsDTO.
userName	The Onvif user name.
password	The Onvif password.
algorithm	Reserved for future use.

PUT /settings/defaultCredentials

Modifies the default credentials for downstream devices.

Parameters

Parameter	Description
body	The modified credentials. See Request body for details.

Request body

nbType	DefaultCredentialsSettingsDTO
DefaultCredentialsSnmpV1SettingsDTO	
nbType	DefaultCredentialsSnmpV1SettingsDTO.
readOnlyCommunityName	The read only community name.
writeCommunityName	The write community name.
DefaultCredentialsSnmpV3SettingsDTO	
nbType	DefaultCredentialsSnmpV3SettingsDTO.
userName	The SNMPv3 user name.
securityType	NOAUTH_NOPRIV = no authentication or encryption. Authentication and encryption protocols/passwords are not required. AUTH_NOPRIV = authentication but no encryption. Protocols/passwords are required for authentication, but not for encryption. AUTH_PRIV = authentication and encryption. All protocols and passwords required.
authenticationProtocol	MD5, SHA1, SHA224, SHA256, SHA384, or SHA512.
authenticationPassword	The authentication password for SNMPv3.
encryptionProtocol	DES, DES3, AES128, AES192, or AES256.
encryptionPassword	The encryption password for SNMPv3
DefaultCredentialsOnvifSettingsDTO	
nbType	DefaultCredentialsOnvifSettingsDTO.
userName	The Onvif user name.
password	The Onvif password.
algorithm	Reserved for future use.

settings/identification

GET /settings/identification

Retrieves the system identification information used for SNMP MIB-2.

PUT /settings/identification

Modifies the system identification information used for SNMP MIB-2.

Enter the name and contact information for the appliance owner, and the location of the appliance.

Parameters

Parameter	Description
body	The modified identification information. See Request body for details.

Request body

nbType	IdentificationSettingsDTO.
name	The name of the appliance owner.
location	The location of the appliance.
contact	The contact information (for example, an Email address) of the appliance owner.

settings/iptables

GET /settings/iptables

Determines whether port forwarding is enabled.

You can get a link to the device's management UI (see *GET /discoveries*, page 68) if port forwarding is enabled.

POST /settings/iptables

Initially enables or disables port forwarding.

This will behave like a PUT if the settings already exist.

Parameters

Parameters	Description
body	The modified credentials. See Request body for details.

Request body

nbType	IPTablesSettingsDTO
portForwardingEnabled	You can get a link to the device's management UI (see <i>GET /discoveries</i> , page 68) if port forwarding is enabled.

PUT /settings/iptables

Enables or disables port forwarding after the initial configuration has been set.

Parameters

Parameters	Description
body	The modified credentials. See Request body for details.

Request body

<code>nbType</code>	IPTablesSettingsDTO
<code>portForwardingEnabled</code>	You can get a link to the device's management UI (see <i>GET /discoveries</i> , page 68) if port forwarding is enabled.

settings/mail

GET /settings/mail

Gets the SMTP mail settings.

The `smtpPassword` is not returned for security reasons.

The `passwordFlag` field indicates whether a password has been set for the SMTP user.

PUT /settings/mail

Configures the SMTP email settings.

Parameters

Parameters	Description
body	The settings to apply. See Request body for details.

Request body

<code>nbType</code>	MailSettingsDTO.
<code>smtpServer</code>	The hostname or IP address of the SMTP server
<code>smtpUser</code>	A user name to allow access through the SMTP server
<code>smtpPassword</code>	A password to allow access through the SMTP server. Changing the <code>smtpPassword</code> to any non-empty value will save that password in the system properties. However, the response for this field will always be <code>null</code> for security reasons.
<code>smtpPort</code>	The IP port number to connect to the SMTP server
<code>from</code>	The email address that will appear in the From field
<code>sslEnabled</code>	Determines whether SSL/TLS is used to encrypt notifications.
<code>passwordFlag</code>	Indicates the intent to remove the password. The <code>passwordFlag</code> will only remove the saved password if there is no <code>smtpPassword</code> value in the request. Otherwise, the specified <code>smtpPassword</code> will be set as the new password. The meaning of the password flag for this operation is different than it is for the GET operation.

POST /settings/mail/test

Sends an email to test the SMTP settings.

If the test is successful, you will receive an Email in the specified account.

Parameters

Parameters	Description
to	Comma-separated list of email addresses.
subject	Email subject line
message	Email body
body	The email settings to test. If these are not specified, the current settings are used. See Request body for details.

Request body

<code>nbType</code>	MailSettingsDTO.
<code>smtpServer</code>	The hostname or IP address of the SMTP server
<code>smtpUser</code>	A user name to allow access through the SMTP server
<code>smtpPassword</code>	A password to allow access through the SMTP server. Changing the <code>smtpPassword</code> to any non-empty value will save that password in the system properties. However, the response for this field will always be <code>null</code> for security reasons.
<code>smtpPort</code>	The IP port number to connect to the SMTP server
<code>from</code>	The email address that will appear in the From field
<code>sslEnabled</code>	Determines whether SSL/TLS is used to encrypt notifications.
<code>passwordFlag</code>	Indicates the intent to remove the password. The <code>passwordFlag</code> will only remove the saved password if there is no <code>smtpPassword</code> value in the request. Otherwise, the specified <code>smtpPassword</code> will be set as the new password. The meaning of the password flag for this operation is different than it is for the GET operation.

settings/network

GET /settings/network/wan

Returns the current network settings.

PUT /settings/network/wan

Modifies the network settings for the appliance.

Parameters

Parameters	Description
body	The modified network settings. See Request body for details.

Request body

nbType	NetworkSettingsDTO
deviceName	This value is ignored.
dhcp	Determines whether a DHCP server automatically assigns the appliance a dynamic IP address. If using DHCP, set the other network settings to null.
ipAddress	The IP address of the appliance
macAddress	This value is ignored.
gateway	The default gateway of the appliance
subnetMask	The subnet mask of the appliance
hostname	The host name of the appliance
dns1	The IP address of the primary DNS server
dns2	The IP address of the secondary DNS server
dns3	The IP address of the tertiary DNS server

settings/proxy

DELETE /settings/proxy

Deletes all the proxy settings, essentially returning the proxy settings to factory defaults.

GET /settings/proxy

Gets the proxy settings for the appliance.

POST /settings/proxy

Creates the initial proxy settings.

This will behave like a PUT if the settings already exist.

Parameters

Parameters	Description
body	The proxy settings. See Request body for details.

Request body

nbType	ProxySettingsDTO
httpServer	The address or DNS name of the proxy http server (optional if https server is being set).
httpPort	The port the proxy http server is using (optional).
httpsServer	The address or DNS name of the proxy https server (optional if https server is being set).
httpsPort	The port the proxy https server is using (optional). - httpUsername: The name of the account for the proxy http server (optional).
httpPassword	The password of the account for the proxy http server (optional).
httpsUsername	The name of the account for the proxy https server (optional).
httpsPassword	The password of the account for the proxy https server (optional).

Example

Request

```
{
  "nbType": "ProxySettingsDTO",
  "proxyType": "PROXY_SETTINGS",
  "httpServer": "10.9.4.173",
  "httpsServer": "10.9.4.174",
  "httpPort": "980",
  "httpsPort": "9443",
  "httpUsername": "netbotz",
  "httpPassword": "password",
  "httpsUsername": "netbotzsec",
  "httpsPassword": "passwordsecure"
}
```

Response

```
{
  "nbType": "ProxySettingsDTO",
  "id": "proxy_settings-1",
  "label": null,
  "status": null,
  "type": "PROXY_SETTINGS",
  "httpServer": "10.9.4.173",
  "httpsServer": "10.9.4.174",
  "httpPort": 980,
  "httpsPort": 9443,
  "httpUsername": "netbotz",
  "httpPassword": "password",
  "httpsUsername": "netbotzsec",
  "httpsPassword": "passwordsecure"
}
```

PUT /settings/proxy

Modifies the proxy settings.

Parameters

Parameters	Description
body	The modified proxy settings. See Request body for details.

Request body

nbType	ProxySettingsDTO
httpServer	The address or DNS name of the proxy http server (optional if https server is being set).
httpPort	The port the proxy http server is using (optional).
httpsServer	The address or DNS name of the proxy https server (optional if https server is being set).
httpsPort	The port the proxy https server is using (optional). - httpUsername: The name of the account for the proxy http server (optional).
httpPassword	The password of the account for the proxy http server (optional).
httpsUsername	The name of the account for the proxy https server (optional).
httpsPassword	The password of the account for the proxy https server (optional).

Example

Request

```
{
  "nbType": "ProxySettingsDTO",
  "proxyType": "PROXY_SETTINGS",
  "httpServer": "10.9.4.173",
  "httpsServer": "10.9.4.174",
  "httpPort": "980",
  "httpsPort": "9443",
  "httpUsername": "netbotz",
  "httpPassword": "password",
  "httpsUsername": "netbotzsec",
  "httpsPassword": "passwordsecure"
}
```

Response

```
{
  "nbType": "ProxySettingsDTO",
  "id": "proxy_settings-1",
  "label": null,
  "status": null,
  "type": "PROXY_SETTINGS",
  "httpServer": "10.9.4.173",
  "httpsServer": "10.9.4.174",
  "httpPort": 980,
  "httpsPort": 9443,
  "httpUsername": "netbotz",
  "httpPassword": "password",
  "httpsUsername": "netbotzsec",
  "httpsPassword": "passwordsecure"
}
```

GET /settings/proxy/test

Tests the proxy settings by sending a request to a URL.

Parameters

Parameters	Description
Method	The request method e.g., GET or POST.
url	URL to send the request to. For example, https://www.schneider-electric.com .

settings/remotelogging

DELETE /settings/remotelogging

Deletes all the remote logging settings, essentially returning the logging settings to factory defaults.

GET /settings/remotelogging

Gets the remote logging settings for the appliance.

POST /settings/remotelogging

Creates the initial remote logging settings.

This will behave like a PUT if the settings already exist.

Parameters

Parameters	Description
body	The remote logging settings. See Request body for details.

Request body

nbType	RemoteLoggingSettingsDTO.
server	The address or host name of the remote log server
port	If not set, defaults to 514 or the last set value.
enabled	Determines whether remote logging is enabled.

Example

Request

```
{
  "nbType":
  "RemoteLoggingSettingsDTO",
  "server": "10.169.104.98",
  "port": 514,
  "enabled": false
}
```

Response

```
{
  "nbType": "RemoteLoggingSettingsDTO",
  "server": "10.169.104.98",
  "port": 514,
  "enabled": false
}
```

PUT /settings/remotelogging

Modifies the remote logging settings.

Parameters

Parameters	Description
body	The remote logging settings. See Request body for details.

Request body

nbType	RemoteLoggingSettingsDTO.
server	The address or host name of the remote log server
port	If not set, defaults to 514 or the last set value.
enabled	Determines whether remote logging is enabled.

Example

Request

```
{
  "nbType": "RemoteLoggingSettingsDTO",
  "enabled": "true",
  "port": "514",
  "server": "10.169.104.98"
}
```

settings/snmpagent

GET /settings/snmpagent

Retrieves the current SNMP agent configuration.

PUT /settings/snmpagent

Modifies the SNMP agent configuration.

Parameters

Parameter	Description
body	The modified SNMP agent configuration. See Request body for details.

Request body

nbType	SnmAgentSettingsDTO
enabled	Determines whether the SNMP agent on your appliance is enabled.
port	The port number for SNMP communications. Ports other than 161 are not currently supported.
version	The SNMP version (VERSION1 or VERSION3).
Settings	
nbType	SnmV1SettingsDTO or SnmpV3SettingsDTO. This must match the version.
readonlyCommunityName	Required for SNMPv1.

The following are required for SNMPv3

userName	The SNMPv3 user name.
securityType	NOAUTH_NOPRIV = no authentication or encryption. Authentication and encryption protocols/passwords are not required. AUTH_NOPRIV = authentication but no encryption. Protocols/passwords are required for authentication, but not for encryption. AUTH_PRIV = authentication and encryption. All protocols and passwords required.
authenticationProtocol	MD5, SHA1, SHA224, SHA256, SHA384, or SHA512.
authenticationPassword	The authentication password for SNMPv3.
encryptionProtocol	DES, DES3, AES128, AES192, or AES256.
encryptionPassword	The encryption password for SNMPv3.

settings/snmptrap

GET /settings/snmptrap

Retrieves the current SNMP trap configuration.

PUT /settings/snmptrap

Configures SNMP trap settings.

Parameters

Parameter	Description
body	The SNMP trap settings. See Request body for details.

Request body

nbType	SnmTrapSettingsDTO.
id	The ID of the SNMP trap configuration.
enabled	Determines whether SNMP traps are enabled.
port	The port for the trap receiver.
version	The SNMP version (VERSION1 or VERSION3).
Settings	
nbType	SnmV1SettingsDTO or SmnP3SettingsDTO. This must match the version.
readonlyCommunityName	Required for SNMPv1.
The following are required for SNMPv3	
userName	The SNMPv3 user name.
securityType	NOAUTH_NOPRIV = no authentication or encryption. Authentication and encryption protocols/passwords are not required. AUTH_NOPRIV = authentication but no encryption. Protocols/passwords are required for authentication, but not for encryption. AUTH_PRIV = authentication and encryption. All protocols and passwords required.
authenticationProtocol	MD5, SHA1, SHA224, SHA256, SHA384, or SHA512.
authenticationPassword	The authentication password for SNMPv3.
encryptionProtocol	DES, DES3, AES128, AES192, or AES256.
encryptionPassword	The encryption password for SNMPv3.
trapIPv4	The IPv4 address of the trap receiver.

POST /settings/snmptrap/test

Sends an SNMP trap message to test SNMP trap settings.

Parameters

Parameter	Description
body	The SNMP trap settings to test. See Request body for details.

Request body

nbType	SnmTrapSettingsDTO.
id	The ID of the SNMP trap configuration.
enabled	Determines whether SNMP traps are enabled.
port	The port for the trap receiver.
version	The SNMP version (VERSION1 or VERSION3).
Settings	
nbType	SnmV1SettingsDTO or SmnPv3SettingsDTO. This must match the version.
readonlyCommunityName	Required for SNMPv1.

The following are required for SNMPv3

userName	The SNMPv3 user name.
securityType	NOAUTH_NOPRIV = no authentication or encryption. Authentication and encryption protocols/passwords are not required. AUTH_NOPRIV = authentication but no encryption. Protocols/passwords are required for authentication, but not for encryption. AUTH_PRIV = authentication and encryption. All protocols and passwords required.
authenticationProtocol	MD5, SHA1, SHA224, SHA256, SHA384, or SHA512.
authenticationPassword	The authentication password for SNMPv3.
encryptionProtocol	DES, DES3, AES128, AES192, or AES256.
encryptionPassword	The encryption password for SNMPv3.
trapIPv4	The IPv4 address of the trap receiver.

settings/ssl

GET /settings/ssl

Gets the current SSL/TLS certificate information.

POST /settings/ssl/ca

Installs a CA-signed certificate.

This will replace the current self-signed or CA-signed certificate.

Parameters

Parameters	Description
body	The configuration for the CA-signed certificate being installed. See Request body for details.

Request body

nbtpe SSLCertPEMsDTO
publickey Enter the public key in PEM format.
privatekey Enter the private key in PEM format.

NOTE:

- The two supplied PEM values are used to generate the certificate. This certificate is used for inbound connections, while trust store certificates are used for outbound connections.
- Certificate private and public keys begin with a header line and end with a footer line.

For example:

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

The header line, the footer line, and the entire certificate content must be included.

POST /settings/ssl/ss

Creates and installs a self-signed certificate.

This will replace the current self-signed or CA-signed certificate. Self-signed certificates expire after five years and must be re-generated.

Parameters

Parameters	Description
body	The information used to create the certificate. See Request body for details.

Request body

nbType	SSLCertSubjectDTO.
id	The ID of the certificate. Automatically generated by the appliance.
commonName	The hostname for your appliance. This should match the Hostname in your network settings.
organizationalUnits	Reserved for future use.
organizational unit	Your organizational unit.
organization	Your organization.
locality	The city or town where you, your organizational unit, or your appliance is located.
stateOrProvinceName	The state or province where you, your organizational unit, or your appliance is located.
countryName	The country where you, your organizational unit, or your appliance is located.
email	Your email address or the email address of the appliance owner.

settings/timedate

GET /settings/timedate

Returns the current time and date settings for the appliance.

POST /settings/timedate

Sets the time and date settings for the appliance.

Parameters

Parameters	Description
body	The time and date settings. See Request body for details.

Request body

<code>nbType</code>	TimeDateConfigSettingsDTO.
<code>zonedDateTime</code>	Reserved for future use.
<code>currentDateTime</code>	Reserved for future use.
<code>mode</code>	MANUAL or NTP. MANUAL = the time and date are determined by your entry for <code>zonedTimeString</code> . NTP = the time and date are determined by the NTP server.
<code>ntpServerPrimary</code>	IP address or host name of the primary NTP server. Required if <code>mode = NTP</code> .
<code>ntpServerSecondary</code>	IP address or host name of the secondary NTP server (optional).
<code>ntpServerTertiary</code>	IP address or host name of the tertiary NTP server (optional).
<code>timezone</code>	See <code>GET/settings/timedate/available-timezones</code> for a list of available values.
<code>zonedDateTimeString</code>	The current date and time in the form of YYYY-MM-DD HH:MM, e.g., 2017-12-02 07:53. Time is in 24-hour format.
<code>serverTimezoneOffsetMilli</code>	

Example

Request

```
{
  "nbType" :
  "TimeDateConfigSettingsDTO",
  "zonedDateTime" : null,
  "currentDateTime" : 1512415028904,
  "mode" : "NTP",
  "ntpServerPrimary" : "0.north-america.pool.ntp.org",
  "ntpServerSecondary" : "",
  "ntpServerTertiary" : "",
  "timezone" : "America/Los_Angeles",
  "availableTimezones" : null,
  "zonedDateTimeString" : "2017-12-4 11:17:08",
  "serverTimezoneOffsetMilli": 0
}
```

Response

```
{
  "nbType" : "TimeDateConfigSettingsDTO",
  "zonedDateTime" : null,
  "currentDateTime" : 1512415028904,
  "mode" : "NTP",
  "ntpServerPrimary" : "0.north-america.pool.ntp.org",
  "ntpServerSecondary" : "",
  "ntpServerTertiary" : "",
  "timezone" : "America/Los_Angeles",
  "availableTimezones" : null,
  "zonedDateTimeString" : "2017-12-4 11:17:08",
  "serverTimezoneOffsetMilli": 0
}
```

PUT /settings/timedate

Modifies the time and date settings

Parameters

Parameters	Description
body	The modified time and date settings. See Request body for details.

Request body

nbType	TimeDateConfigSettingsDTO.
zonedDateTime	Reserved for future use.
currentDateTime	Reserved for future use.
mode	MANUAL or NTP. MANUAL = the time and date are determined by your entry for zonedTimeString. NTP = the time and date are determined by the NTP server.
ntpServerPrimary	IP address or host name of the primary NTP server. Required if mode = NTP.
ntpServerSecondary	IP address or host name of the secondary NTP server (optional).
ntpServerTertiary	IP address or host name of the tertiary NTP server (optional).
timezone	See GET/settings/timedate/available-timezones for a list of available values.
zonedTimeString	The current date and time in the form of YYYY-MM-DD HH:MM. For example, 2017-12-02 07:53. Time is in 24-hour format.
serverTimezoneOffsetMilli	

Example

Request

```
{
  "nbType" :
  "TimeDateConfigSettingsDTO",
  "zonedDateTime" : null,

  "currentDateTime" : 1512415028904,
  "mode" : "NTP",

  "ntpServerPrimary" : "0.north-
america.pool.ntp.org",
  "ntpServerSecondary" : "",
  "ntpServerTertiary" : "",
  "timezone" : "America/Los_Angeles",
  "availableTimezones" : null,

  "zonedTimeString" : "2017-12-4
11:17:08",
  "serverTimezoneOffsetMilli" : 0
}
```

Response

```
{
  "nbType" : "TimeDateConfigSettingsDTO",
  "zonedDateTime" : null,
  "currentDateTime" : 1512415028904,
  "mode" : "NTP",
  "ntpServerPrimary" : "0.north-america.
pool.ntp.org",
  "ntpServerSecondary" : "",
  "ntpServerTertiary" : "",
  "timezone" : "America/Los_Angeles",
  "availableTimezones" : null,
  "zonedTimeString" : "2017-12-4
11:17:08",
  "serverTimezoneOffsetMilli" : 0
}
```

GET /settings/timedate/available-timezones

Returns a list of time zones supported by the NetBotz appliance.

GET /settings/timedate/info

Returns the current time and date information for the appliance.

POST /settings/timedate/synchronize

Sets the current time zone.

Parameters

Parameters	Description
body	The time zone setting. See Request body for details.

Request body

nbType	TimeDateSyncRequestDTO
timezone	See <i>GET /settings/timedate/available-timezones</i> , page 101 for a list of available timezones.

Example

Request	Response
<pre>{ "nbType": "TimeDateSyncRequestDTO", "timezone": "America/New_York" }</pre>	<pre>{ "nbType": "TimeDateSyncResponseDTO", "currentDateTime": 1556131745022, "zonedDateTime": 1556131745000, "zonedDateTimeString": "2019-04-24 14:49:05" }</pre>

settings /trust-store

GET /settings/trust-store

Gets information for all trust store certificates.

The alias can be used to delete the certificate.

POST /settings/trust-store

Adds a PEM-formatted root or intermediate certificate to the trust store.

Trust store certificates are used primarily for outbound connections (to SMTP servers, LDAP servers, some Proxy servers, etc.). The appliance generates a unique alias for each certificate when it is installed.

Parameters

Parameters	Description
body	A root or intermediate certificate in PEM format. See Request body for details.

Request body

nbType	StringDTO.
id	The ID of the certificate. Automatically generated by the appliance.
property	A root or intermediate certificate in PEM format.

DELETE /settings/trust-store/{alias}

Deletes the certificate based on its alias.

Parameters

Parameters	Description
alias	the certificate alias.

users

GET /users

Retrieves a list of all user accounts.

Parameters

Parameters	Description
deviceUserOnly	Always false. Reserved for future use.

POST /users

Creates a new user account.

Parameters

Parameter	Description
body	The user account settings. See Request body for details.

Request body

nbType	UserDTO
username	The user's name.
password	The password to log on to the appliance.
isAdmin	Enter true if the user is granted administrative privileges.
isSuperUser	Not used for this operation.
settings	
nbType	UserSettingsDTO
id	The ID of the settings. Automatically generated by the appliance.
locale	Always en_US.
imperial	Measurement units (true = imperial, false = metric).
time24	Time format (true = 24-hour, false = 12-hour).
autoScale	When true, autoscale converts detailed sensor measurements to more manageable units. For example, a sensor that measures milliseconds may display measurement in seconds when autoscale is on.

DELETE /users/{id}

Deletes an account.

Parameters

Parameter	Description
id	The ID of the account to be deleted.

GET /users/{id}

Retrieves a user account .

Parameters

Parameter	Description
id	The user account ID.

PUT /users/{id}

Modifies an existing user account.

Parameters

Parameter	Description
id	The user ID of the account to be modified.
body	The modified account settings. See Request body for details.

Request body

nbType	UserDTO
username	The user's name.
password	The password to log on to the appliance. Ignored for this operation.
isAdmin	Enter true if the user is granted administrative privileges.
isSuperUser	Enter true if the user is the superuser.
settings	
nbType	UserSettingsDTO
id	The ID of the settings. Automatically generated by the appliance.
locale	Always en_US.
imperial	Measurement units (true = imperial, false = metric).
time24	Time format (true = 24-hour, false = 12-hour).
autoScale	When true, autoscale converts detailed sensor measurements to more manageable units. For example, a sensor that measures milliseconds may display measurement in seconds when autoscale is on.

PUT /users/{id}/password

Modifies an existing user account's password.

Only a super user or the user identified by the account have access to this operation.

Parameters

Parameter	Description
id	The user ID of the account to be modified.
body	The requested password changes. See Request body for details.

Request body

nbType	PasswordChangesDTO.
oldPassword	The current password for the account. Not required if the Super User changes an Admin's password.
newPassword	The password to change to.

wireless

GET /wireless/details

Retrieves detailed information for each of the wireless devices.

This includes the firmware type; the runtime (current), SPI (staging), and target firmware versions; and the progress percentage of any in-progress firmware updates.

GET /wireless/details/{id}

Retrieves detailed information for a wireless device.

Parameters

Parameter	Description
id	The ID of the pod asset for the wireless device.

GET /wireless/firmware/file/versions

Retrieves the target firmware version for each of the wireless devices.

The target firmware version is the latest wireless firmware available. The firmware files are downloaded when the appliance is updated (see *firmwareupdate*, page 72).

PUT /wireless/firmware/update

Manually starts or stops a wireless firmware update.

Before updating the wireless firmware, you must update the appliance firmware (see *firmwareupdate*, page 72).

Parameters

Parameter	Description
stage	Wireless update stages.

NOTE: Use the parameters to invoke each wireless update stage in order.

1. UPDATE: Validates the wireless firmware files already deposited on the system by the appliance's firmware update process. This is required before any other stage may be invoked.
2. TRANSFER: Transfers the firmware files to the devices in the wireless network. After this stage, the new firmware is shown as both the target version and the SPI version.
3. APPLY: Commands each wireless node to switch from its current runtime firmware to the downloaded SPI version. Each device must restart to install the SPI version. Once this command has been issued, it cannot be aborted. Restarting the network may take 15 minutes or more.

Select CANCEL to terminate the UPDATE or TRANSFER operations. The APPLY operation cannot be terminated.

GET /wireless/knownDevices

Lists wireless devices discovered by the appliance.

Devices are represented by their extended MAC address (16 hexadecimal digits, for example, 28298600000081FB6).

Parameters

Parameter	Description
Status	AVAILABLE: Get devices that are available on the network. JOINED: Get devices that are managed by the appliance. ALL: Get both AVAILABLE and JOINED devices.

POST /wireless/nodes

Adds new wireless devices to the commission list and re-forms the network.

Parameters

Parameter	Description
body	The wireless devices to add. See Request body for details.

Request body

nbType	WirelessNodeConfigsDTO.
items	
nbType	WirelessNodeConfigDTO.
macAddress	You can find the MAC address on the back of the sensor. The MAC address must be in Zigbee Extended Address form: 16 hexadecimal digits that can optionally include a hyphen (-) or colon (:) every two digits. <ul style="list-style-type: none"> • 2829860000081FB6 • 28:29:86:00:00:08:1F:B6 • 28-29-86-00-00-08-1F-B6
name	A user-friendly name for the sensor.

NOTE: All values in the request body are required.

DELETE /wireless/nodes/{macAddress}

Removes a wireless device from the commission list and re-forms the network.

This operation decommissions wireless devices. It does not remove them from the system.

Parameters

Parameter	Description
macAddress	The MAC address of the device to delete. The MAC address must be in Zigbee Extended Address form: 16 hexadecimal digits that can optionally include a hyphen (-) or colon (:) every two digits. <ul style="list-style-type: none"> • 2829860000081FB6 • 28:29:86:00:00:08:1F:B6 • 28-29-86-00-00-08-1F-B6

GET /wireless/settings

Gets the wireless firmware update type.

AUTOMATIC = Wireless firmware is updated when the appliance firmware is updated.

MANUAL = You update the wireless firmware at your convenience.

POST /wireless/settings

Sets the wireless update type.

Parameters

Parameter	Description
body	The wireless update setting (AUTOMATIC or MANUAL). See Request body for details.

Request body

nbType	WirelessSettingsDTO.
updateType	AUTOMATIC = Wireless firmware is updated when the appliance firmware is updated. MANUAL = You update the wireless firmware at your convenience.

GET /wireless/status

Retrieves the current status of the wireless sub-system, including whether updates are available.

Troubleshooting

Access Issues

Problem	Solution
Cannot access the appliance through a terminal emulator	<ul style="list-style-type: none"> • Make sure the serial port is not in use by another application. • Make sure that the terminal settings are configured correctly: 115,200 baud, 8 data bits, no parity, 1 stop bit, and no flow control.
Cannot access the Web UI	<ul style="list-style-type: none"> • At startup, the Web UI can take about six minutes to become accessible. Wait for six minutes, then try to log in again. • Verify that HTTP or HTTPS access is enabled. Check your browser's proxy settings. • Make sure the URL is consistent with the security system used by the appliance. SSL requires https, not http, at the beginning of the URL. • Verify that you can ping the appliance. • Verify that you are using a supported Web browser. If available, try a different web browser. See <i>Access the Web User Interface (Web UI)</i>, page 14. • If the appliance has just restarted and SSL security is being set up, the appliance may be generating a server certificate. The appliance may take several minutes to create this certificate, and the SSL server is not available during that time.

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.

© 2018 – 2019 APC by Schneider Electric. All rights reserved.

990-5934C-001