InfraStruXure™ Central

Version 4.1

User’s Reference

Preface

Copyright

Trademarks

Federal Communications Commission (FCC) Declaration of Conformity Statement

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

U.S. 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/Video 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 INSURING 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.

Availability of Open Source Technologies

This product includes technologies that are governed by the GNU Public License. The GPL source code contained in our products is available for free download from:

http://support.netbotz.com/gpl

Contents

Mass Configuration: Device Settings...................... 159

Introduction

InfraStruXure Central works with your APC NetBotz devices, APC devices, and other 3rd-party manufacturer devices to provide a comprehensive monitoring solution for your IT environment and equipment. With InfraStruXure Central, you can instantly view environment readings and a camera image from any site on your network where an APC NetBotz device has been deployed. If environment readings for a site go outside of thresholds you have set, the icon label for that site turns red in the InfraStruXure Central Map view. A Table view presents users with a table that shows all current sensor data for APC NetBotz devices in a selected group, allowing users to see at a glance where there is an alert condition. Historical alarm data is quickly accessible by appliance and date.

InfraStruXure Central works with logical, dynamically updated groups of devices that you set up. Your IT group saves time by executing configuration and threshold operations against an entire group at once. You have powerful analytical capabilities at your disposal with the Graph/Report view, where you can generate graphs or reports to display sensor data for one or more appliances over a specified date/time range. Data can be exported for use in other applications. The administrator of InfraStruXure Central can choose precisely what capabilities to grant to each user and which groups or appliances they can access.

In addition to enhancing your monitoring and management capabilities, InfraStruXure Central improves network availability through a fully distributed architecture combined with remote and local storage. All of your environmental monitoring and management data can be stored on up 5 remote data repositories, greatly enhancing the volume of data that you can access and complementing your organization's standardized back-up and recovery procedures. Likewise, Surveillance video clips are stored on the appliances that generate them until they are needed, enabling you to centrally manage your Surveillance data while also saving bandwidth and preserving processing power.

InfraStruXure Central features extensive administrator customizability. View data operational logs, set preferences for device discovery, data collection, network functionality, and security. Create user-specific accounts that limit access to sensitive data and powerful configuration tasks. User Accounts enable you to allow employees or clients access to InfraStruXure Central data without giving them the “keys to the kingdom.” Create user accounts that limit access to InfraStruXure Central functionality and features to those that are appropriate for a given user. Specify read or write access to specific InfraStruXure Central tasks, and limit user access to specific device groups.

Managing Additional Devices

By default, your InfraStruXure Central device comes pre-licensed to manage up to 25 network-attached supported devices. If you need to manage more than 25 devices (up to a maximum of 1025 unique devices) you will need to purchase a Device Pack license key upgrade for use on your InfraStruXure Central server. This license key upgrade will enable you to manage additional devices. Simply contact APC Corp. or the vendor from whom you purchased your InfraStruXure Central server, purchase a Device Pack license key, and install the license key using the License Keys task. For more information, see “License Keys” on page 89.

Upgrading InfraStruXure Central

InfraStruXure Central can be upgraded with additional functionality with InfraStruXure Central upgrade packs such as Surveillance View. Upgrades are available for purchase from APC Corp. or from an APC Authorized Reseller. For more information about Surveillance View, see “Surveillance View” on page 267.

About the Installer CD

You can use the *InfraStruXure Central Installer* CD to install the following applications on any supported system:

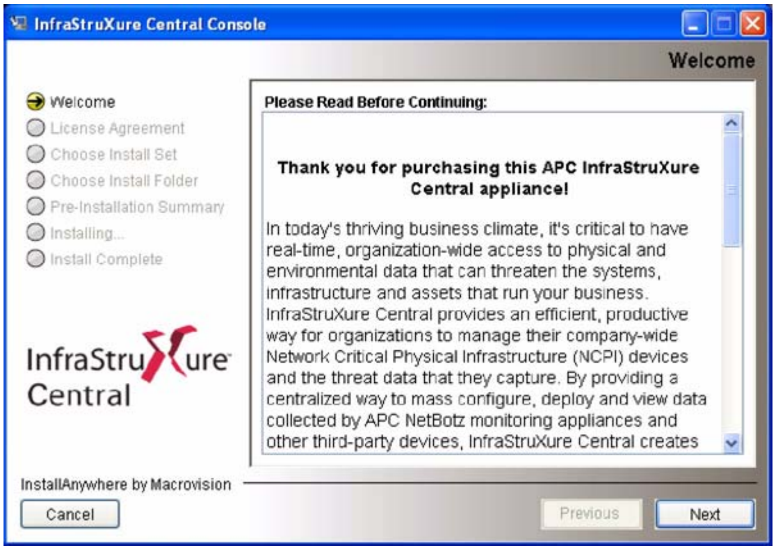
- InfraStruXure Central Console: A Java-based user interface designed to work with the InfraStruXure Central server. The InfraStruXure Central console simplifies monitoring and managing your NetBotz devices, APC devices, and other 3rd party devices.
- Serial Configuration Utility: A Java-based application that you can use to configure the network settings on your InfraStruXure Central server or any other NetBotz device.
- Java Runtime Environment (JRE)

By default, the *InfraStruXure Central Installer* will copy the InfraStruXure Central documentation to your system. You can also access these PDF files from the DOCS subdirectory of the CD.

Installing on a Windows System

To install the applications and the JRE on a supported Windows system

1. Place the *InfraStruXure Central Installer* CD-ROM in the CD-ROM drive of the system that you will use to configure and manage your server. The InfraStruXure Central Installer will start automatically. If you have disabled Autostart on your system, click Start > Run, type *x*:\install.exe in the Open field (where *x* is the drive letter assigned to your CD-ROM drive) and then click OK.
2. The Welcome screen appears. Read the window contents and then click Next to continue.



Please Read Before Continuing:

Thank you for purchasing this APC InfraStruXure Central appliance!

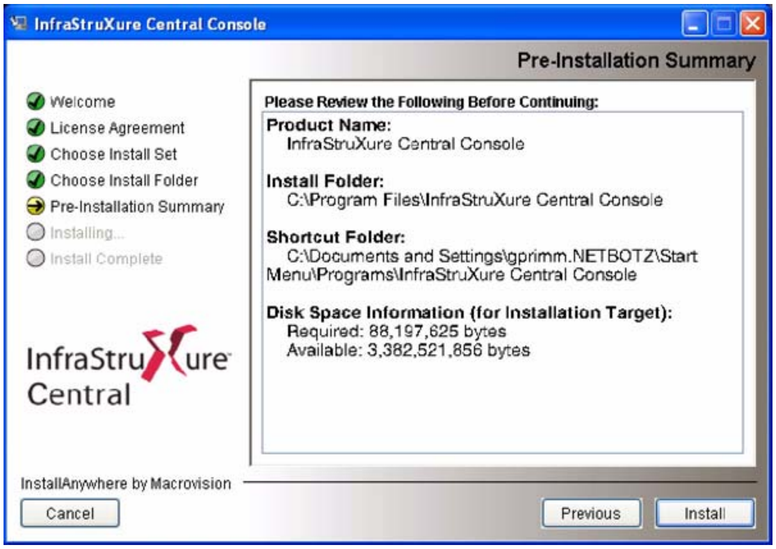
In today's thriving business climate, it's critical to have real-time, organization-wide access to physical and environmental data that can threaten the systems, infrastructure and assets that run your business. InfraStruXure Central provides an efficient, productive way for organizations to manage their company-wide Network Critical Physical Infrastructure (NCPI) devices and the threat data that they capture. By providing a centralized way to mass configure, deploy and view data collected by APC NetBotz monitoring appliances and other third-party devices, InfraStruXure Central creates

3. The License Agreement window appears. Read the window contents, click I Accept the terms of the License Agreement to agree to the terms and conditions of the license agreement and then click Next. If you do not agree to the terms and conditions of the license agreement, click Cancel to close the installation program.
4. The Choose Install Set window appears. You can choose to install the **Typical** product features,

Minimal product features, or **Custom** product features.

- If you choose **Typical** the Serial Configuration Utility, product documentation, and InfraStruXure Central Console application will be installed on your system.
- If you choose **Minimal** only the Serial Configuration Utility and the InfraStruXure Central Console application will be installed on your system.
- If you choose **Custom** you can select which components you want installed on your system.

5. The Pre-Installation Summary window appears and displays information about the installation options you have chosen. Click Install to continue.



Please Review the Following Before Continuing:

Product Name:
InfraStruXure Central Console

Install Folder:
C:\Program Files\InfraStruXure Central Console

Shortcut Folder:
C:\Documents and Settings\gprimm.NETBOTZ\Start Menu\Programs\InfraStruXure Central Console

Disk Space Information (for Installation Target):
Required: 88,197,625 bytes
Available: 3,382,521,856 bytes

6. The Install Complete window appears. Click Done to finish your installation and close the InfraStruXure Central Installer.

Installing on a Linux System

To install the applications and the JRE on a supported Linux system:

1. Place the *InfraStruXure Central Installer* CD-ROM in the CD-ROM drive of the system that you will use to configure and manage your server. Be sure to mount the drive if necessary.
2. Run install.bin from the Linux subdirectory on the CD. For example, if you mounted the CD-ROM drive as /mnt/cdrom, execute the following command:

   ```
   sh /mnt/cdrom/linux/install.bin
   ```

3. The InfraStruXure Central Installer starts and the Welcome screen appears. Read the window contents and then click Next to continue.
4. The License Agreement window appears. Read the window contents, click I Accept the terms of the License Agreement to agree to the terms and conditions of the license agreement and then click Next. If you do not agree to the terms and conditions of the license agreement, click Exit to close the installation program.
5. The Choose Install Set window appears. You can choose to install the **Typical** product features,

Minimal product features, or **Custom** product features.

- If you choose **Typical** the Serial Configuration Utility, product documentation, and InfraStruXure Central Console application will be installed on your system.
- If you choose **Minimal** only the Serial Configuration Utility and the InfraStruXure Central Console application will be installed on your system.
- If you choose **Custom** you can select which components you want installed on your system.

6. The Pre-Installation Summary window appears and displays information about the installation options you have chosen. Click Install to continue.
7. The Install Complete window appears. Click Done to finish your installation and close the InfraStruXure Central Installer.

Installation and Configuration

Installing your InfraStruXure Central Server

The InfraStruXure Central server is designed to be installed in a server rack or cabinet. Rack mounting configurations differ depending on rack or cabinet design and manufacturer. Please refer to your rack or cabinet documentation for detailed instructions on how to mount equipment in your rack or cabinet.

Note

To configure the IP settings on your InfraStruXure Central server you will need to connect a Windows 2000, NT 4.0, or XP system to the server using the included null modem cable. Before installing be sure to consider the following issues:

- Depending on your rack or cabinet design and location, it may be difficult to access the serial port on the back of the InfraStruXure Central server after you install it in your rack.
- If the cabinet or rack is in a difficult-to-access location, it may be difficult to get the required Windows system close enough to the rack- or cabinet-mounted server to easily connect the two systems with the included null modem cable.

If you believe you may encounter either of these scenarios, we suggest that you configure the IP settings on the server first, and then install it in your rack or cabinet.

After you have installed the server in your rack or cabinet, be sure to connect the server to your 10 Mbit, 100 Mbit, or 1000 Mbit Ethernet network and to connect the power cable to a properly grounded power outlet or power distribution unit.

Configuring Your InfraStruXure Central Server

Before installing your InfraStruXure Central server, you must configure your device's network settings. You can use the Serial Configuration Utility to specify network settings (including IP address, gateway address, subnet mask, and hostname) to be used by the device.

Using the Serial Configuration Utility

You can use the Serial Configuration Utility to assign your server network settings.

To configure your server using the Serial Configuration Utility:

1. Click Start > Programs > InfraStruXure Central Console > Serial Configuration Utility to start the Serial Configuration Utility. If the Serial Configuration Utility has not yet been installed on your system, see "About the Installer CD" on page 13 for instructions on how to do so.
2. Connect one end of the null modem cable to a serial connector on your system and the other end of the cable to the serial port on the InfraStruXure Central server.
3. Plug the InfraStruXure Central server power supply into a wall outlet, and then connect it to the power cord connection. When the server is finished starting up click Next to continue.
4. The Serial Configuration Utility automatically scans your systems COM ports to determine if a device is connected to the system. If a device is discovered the utility will note the presence of the server in the Device column of the window. Select the radio button that corresponds to the

server you wish to configure and then click Next to continue configuring your server.

Note

If the COM port associated with the port to which your serial cable is connected is currently in use by another application, the message beside the COM port in the Owner column will indicate that the port is not currently available. To correct this, close the application that is using the COM port and then click Scan Serial Ports.

1. The Root Password window appears. Type in the Password field the administrator account password for this server (by default this password is set to “apc.”) and then click OK.
2. The utility scans the server and displays the network settings (IP Address, Netmask, and Gateway) that are currently stored on the server. The network settings are divided into Ethernet Card Settings and DNS Settings.
3. Specify the Ethernet Card settings. Provide an IP address, subnet mask, and gateway address for the server.
4. Specify the DNS Settings. Provide the desired domain and DNS server information.
5. Click Next to save your configuration settings. When the save process is complete you can click Finish to close the Serial Configuration Utility.

To test the InfraStruXure Central server IP connection, start your web browser and type the IP address that was assigned to the server into the address field. Then, press Enter. If the InfraStruXure Central server is online and properly configured the InfraStruXure Central welcome page will be displayed in the browser window.

Install Your InfraStruXure Central Server

The InfraStruXure Central server is designed to be installed in a server rack or cabinet. Use the following safety guidelines to help ensure your own personal safety and to help protect your system and working environment from potential damage. For complete safety information, see the Product Information Guide.

SAFETY: Rack Mounting of Systems

Observe the following precautions for rack stability and safety.

- Systems are considered to be components in a rack. Thus, “component” refers to any system as well as to various peripherals or supporting hardware.

Caution

Installing systems in a rack without the front and side stabilizers installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizers before installing components in the rack.
After installing system/components in a rack, never pull more than one component out of the rack on its slide assemblies at one time. The weight of more than one extended component could cause the rack to tip over and injure someone.

Note

Your system is safety-certified as a free-standing unit and as a component for use in a rack cabinet using the customer rack kit. The installation of your system and rack kit in any other rack cabinet has not been approved by any safety agencies. It is your responsibility to ensure that the final combination of system and rack complies with all applicable safety standards and local electric code requirements. The manufacturer disclaims all liability and warranties in connection with such combinations.

- System rack kits are intended to be installed in a rack by trained service technicians. If you install the kit in any other rack, be sure that the rack meets the specifications.

⚠ Caution

Do not move racks by yourself. Due to the height and weight of the rack, a minimum of two people should accomplish this task.

- Before working on the rack, make sure that the stabilizers are secured to the rack, extended to the floor, and that the full weight of the rack rests on the floor. Install front and side stabilizers on a single rack or front stabilizers for joined multiple racks before working on the rack.
- Always load the rack from the bottom up, and load the heaviest item in the rack first.
- Make sure that the rack is level and stable before extending a component from the rack.
- Use caution when pressing the component rail release latches and sliding a component into or out of a rack; the slide rails can pinch your fingers.
- After a component is inserted into the rack, carefully extend the rail into a locking position, and then slide the component into the rack.
- Do not overload the AC supply branch circuit that provides power to the rack. The total rack load should not exceed 80 percent of the branch circuit rating.
- Ensure that proper airflow is provided to components in the rack.
- Do not step on or stand on any component when servicing other components in a rack.

Installation Instructions

This installation guide provides instructions for trained service technicians installing one or more systems in a rack cabinet. The RapidRails™ rack kit can be installed without tools in manufacturer’s rack cabinets that have square holes. One rack kit is required for each system installed in the rack. VersaRails™ rack kits, which are designed for use with rack cabinets that have round holes, are available for purchase separately.

Before attempting this installation, you should read through this entire procedure carefully.

⚠ Caution

Do not install rack kit components designed for another system. Use only the rack kit for your system. Using the rack kit for another system may result in damage to the system and personal injury to yourself and to others.

Before You Begin

Before you begin installing your system in the rack, carefully read the safety instructions found at the beginning of this guide, as well as the safety instructions found in your system’s Product Information Guide for additional information.

Observe the following safety precautions when installing your system in the rack.

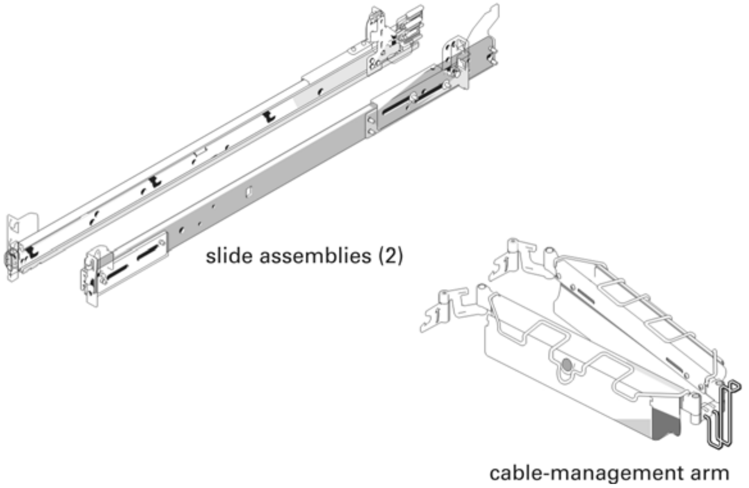
Caution

- When installing multiple systems in a rack, complete all of the procedures for the current system before attempting to install the next system.
- Rack cabinets can be extremely heavy and move easily on the casters. The cabinet has no brakes. Use extreme caution while moving the rack cabinet. Retract the leveling feet when relocating the rack cabinet. Avoid long or steep inclines or ramps where loss of cabinet control may occur. Extend the leveling feet for support and to prevent the cabinet from rolling.
- You must strictly follow the procedures in this document to protect yourself as well as others who may be involved. Your system may be very large and heavy, and proper preparation and planning are important to prevent injury to yourself and to others. This becomes increasingly important when systems are installed high up in the rack.
- Installing systems in a rack without the front and side stabilizer feet installed could cause the rack to tip over, potentially resulting in bodily injury under certain circumstances. Therefore, always install the stabilizer feet before installing components in the rack. The stabilizer feet help prevent the rack from tipping over when a system or other component is pulled out of the rack with the slide assemblies fully extended. Refer to the documentation provided with the rack cabinet for instructions on installing and anchoring the stabilizer feet.
- After installing systems in a rack, never pull more than one system out of the rack on its slide assemblies at one time. The weight of more than one extended system could cause the rack to tip over and cause injury.

RapidRails Rack Kit Contents

The RapidRails rack kit includes the following items (see Figure 1-1):

- One pair of RapidRails slide assemblies
- One cable-management arm
- Tie-wraps (not shown)



Installation Tasks

Installing a rack kit involves performing the following tasks in their numbered order:

1. Removing the rack doors
2. Select an installation location within the rack
3. Installing the RapidRails slide assemblies in the rack
4. Installing the system in the rack
5. Installing the cable-management arm
6. Routing cables
7. Replacing the rack doors

Removing the Rack Doors

See the procedures for removing doors in the documentation provided with your rack cabinet.

Caution

- Because of the size and weight of the rack cabinet doors, never attempt to remove or install them by yourself.
- Store the two doors where they will not injure someone if the doors accidently fall over.

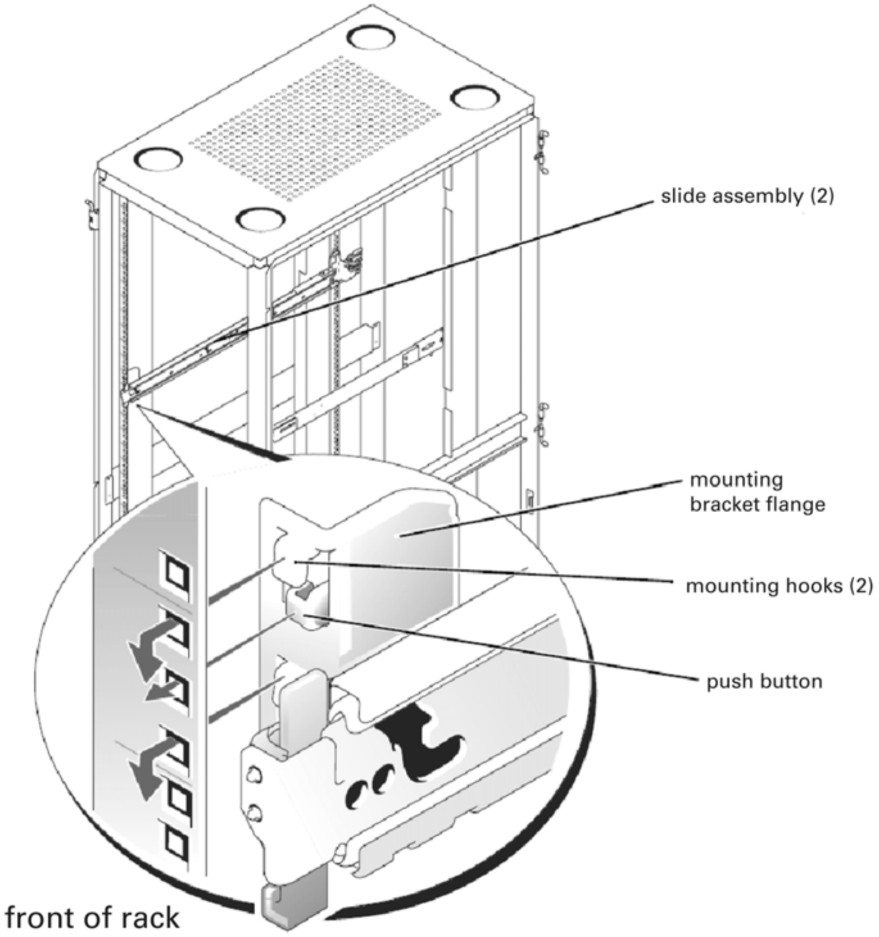
Selecting a Location within the Rack

You must allow 1 U (44 mm, 1.75 inches) of vertical space for each InfraStruXure Central Standard Edition system or 2 U (88 mm, or 3.5 inches) of vertical space for each InfraStruXure Central Enterprise Edition system you install in the rack. Rack cabinets that meet EIA-310 standards have an alternating pattern of three holes per rack unit with center-to-center hole spacing (beginning at the top hole of a 1-U space) of 15.9 mm, 15.9 mm, and 12.7 mm (0.625 inch, 0.625 inch, and 0.5 inch) for the front and back vertical rails (see Figure 1-3). Rack cabinets may have round or square holes. The RapidRails™ rack kit can be installed without tools in manufacturer’s rack cabinets that have square holes. VersaRails™ rack kits, which are designed for use with rack cabinets that have round holes, are available for purchase separately.

Installing the RapidRails Slide Assemblies

1. At the front of the rack cabinet, position one of the RapidRails slide assemblies so that its mounting-bracket flange fits between the marks or tape you placed on the rack (see below). The top mounting hook on the slide assembly’s front mounting bracket flange should enter the top hole between the marks you made on the vertical rails.
2. Push the slide assembly forward until the top mounting hook enters the top square hole that you placed a mark just above on the vertical rail, and then push down on the mounting-bracket flange until the mounting hooks seat in the square holes and the push button pops out and clicks (see

below).



3. At the back of the cabinet, pull back on the mounting-bracket flange until the top mounting hook is in the top square hole, and then push down on the flange until the mounting hooks seat in the square holes and the push button pops out and clicks.
4. Repeat steps 1 through 3 for the slide assembly on the other side of the rack.

Note

Ensure that the slide assemblies are mounted at the same position on the vertical rails on each side of the rack.

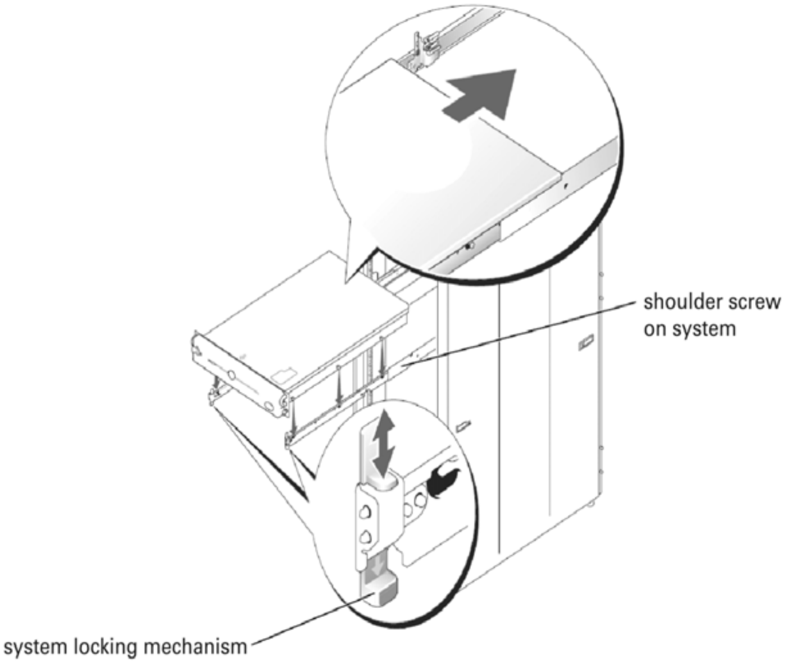
Installing the System in the Rack

Caution

- If you are installing more than one system, install the first system in the lowest available position in the rack.
- Never pull more than one component out of the rack at a time.
- Because of the size and weight of the system, never attempt to install the system in the slide assemblies by yourself.

1. Pull the two slide assemblies out of the rack until they lock in the fully extended position. Lift the

system into position in front of the extended slides (see below).



2. Place one hand on the front-bottom of the system and the other hand on the back-bottom of the system.
3. Tilt the back of the system down while aligning the back shoulder screws on the sides of the system with the back slots on the slide assemblies.
4. Engage the back shoulder screws into their slots.
5. Lower the front of the system and engage the front and middle shoulder screws in their slots (the middle slot is just behind the yellow system release latch).

   When all shoulder screws are properly seated, the system locking mechanism at the front of each slide assembly clicks and locks the system into the slide assembly.
6. Press up on the slide release latch at the side of each slide to slide the system completely into the rack.
7. Push in and turn the captive thumbscrews on each side of the front chassis panel to secure the system to the rack.

Note

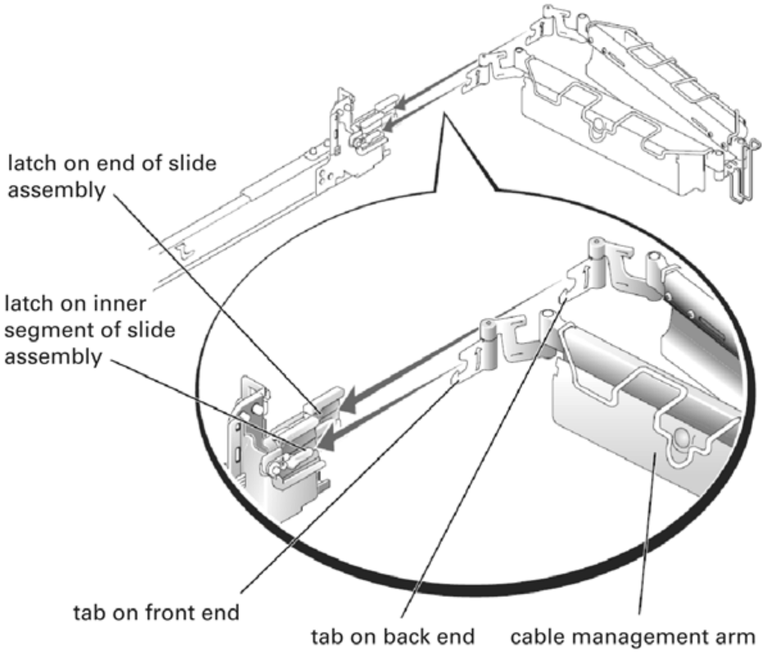
To remove the system from the slide assemblies, press down on the thumbpads of the system locking mechanism, and then pull the system forward.

Installing the Cable-Management Arm

Note The cable-management arm can only be installed on the right side of the rack cabinet (as viewed from the back).

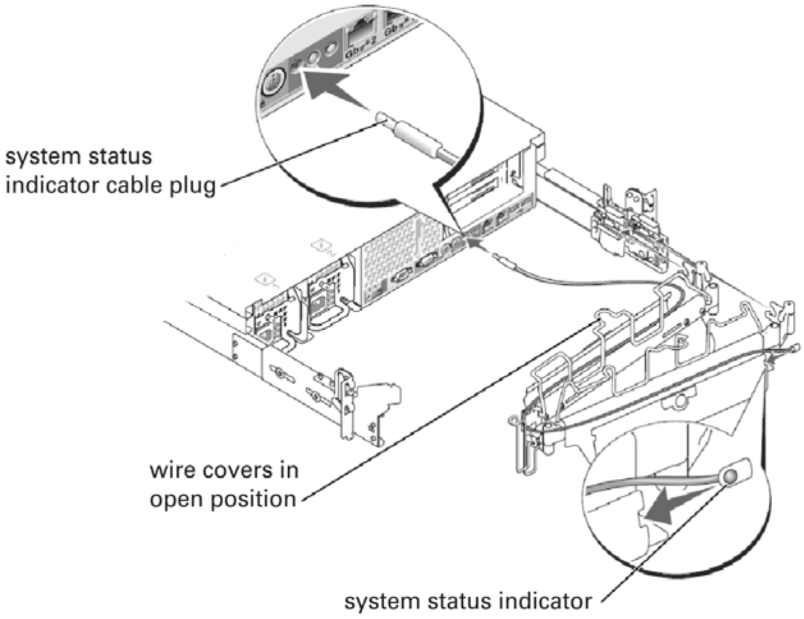
To install the cable-management arm on the system, perform the following steps:

1. Facing the back of the rack cabinet, locate the latch on the end of the slide assembly.
2. Push the tab on the back end of the cable-management arm into the latch on the end of the slide assembly (see below). The latch clicks when locked.
3. Push the tab on the front end of the cable-management arm into a mating latch on the inner segment of the slide assembly (see below). The latch clicks when locked.


latch on end of slide assembly
latch on inner segment of slide assembly
tab on front end
tab on back end
cable management arm

4. If applicable, install the system status indicator cable plug into its connector (see Figure 1-9).
5. Open the wire covers on the cable-management arm by lifting the center of the wire over the top of the embossed round button on the front of the forward part of the arm and lifting the wire over the top of a similar round button on the back part of the arm. The wire cover swings open to enable cables to be routed within the arm.
6. Route the system status indicator end of the cable through the cable-management arm, and install

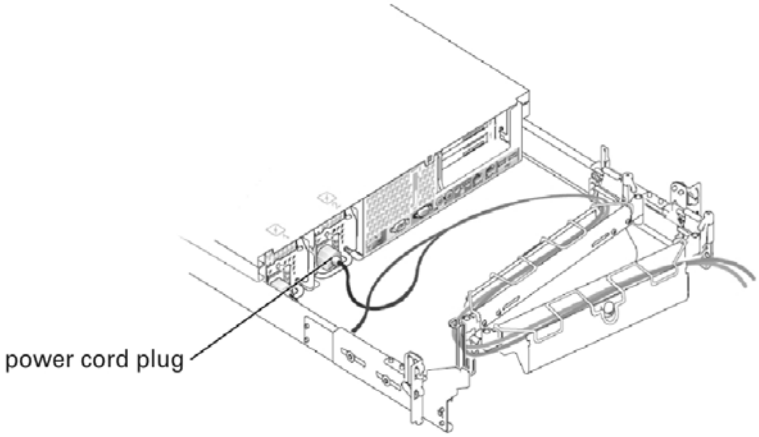
the indicator in its slot at the back end of the cable-management arm (see below).


system status indicator cable plug
wire covers in open position
system status indicator

7. Connect the power cords to their receptacles on the back panel (see below).

Note

Use the strain-relief loops (if available) on the back of the power supplies to provide strain relief for the power cables.



Caution

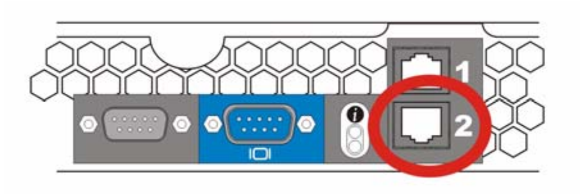
Allow some slack in each cable as you route them around hinges in the cable-management arm.

8. Attach the I/O and network cable connectors to their respective connectors on the system back

panel.

Caution

If you will ne enabling the internal DHCP LAN functionality on your InfraStruXure Central, the private LAN connection **must** be connected to LAN Port 2. Once this feature is enabled, ensure that LAN Port 2 is NOT connected to a public LAN. Enabling this functionality on an InfraStruXure Central with LAN Port 2 connected to a public LAN will result in serious network connectivity issues. For more information on the internal DHCP LAN functionality, see “Server Settings” on page 93.



9. Route the power and I/O cables through the cable-management arm, using four loosely secured tie-wraps (two in the middle and one on each end of the cable-management arm).

   – Do not fully tighten the tie-wraps at this time.

   – Allow some cable slack in the cable-management arm to prevent damage to the cables.

10. Secure the cables to the cable-management arm:

    a. After connecting the cables to the system, unscrew the thumbscrews that secure the front of the system to the front vertical rail.

    b. Slide the system forward to the fully extended position.

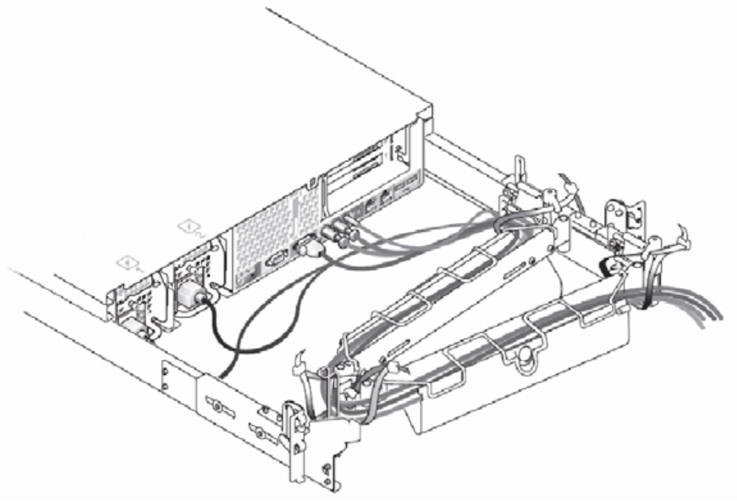
    c. Route the cables along the cable-management arm, make any adjustments needed to the cable slack at the hinge positions, secure the cables to the cable-management arm with the tie-wraps, and close the wire covers over the cable-management arm.

Note

As you pull the system out to its furthest extension, the slide assemblies will lock in the extended position. To push the system back into the rack, press the slide release latch on the side of the slide, and then slide the system completely into the rack.

11. Slide the system in and out of the rack to verify that the cables are routed correctly and do not bind,

stretch, or pinch with the movement of the cable-management arm.



12. Tighten the tie-wraps just enough to ensure that the cable slack is neither too tight to cause excessive pinching nor too loose, yet keep the cables from slipping as the system is moved in and out of the rack.

Replacing the Rack Doors

Refer to the procedures for replacing doors in the documentation provided with your rack.

Caution

Because of the size and weight of the rack cabinet doors, never attempt to remove or install them by yourself.

This completes the rack installation of your system in a four-post rack cabinet.

Getting Started

This Getting Started section is designed to help you become familiar with the InfraStruXure Central interface, and to guide you through the basic configuration and functionality of the InfraStruXure Central console. The procedures described in this section will enable you to configure InfraStruXure Central so that you can automatically discover, monitor, and manage physical infrastructure devices on your network.

These procedures are also available in an online tutorial which starts automatically the first time you start the InfraStruXure Central interface. The tutorial will automatically start each time you start the InfraStruXure Central console until you un-check the **Show this at next startup** check box. If you have dismissed the tutorial and need to view the tutorial again, just right-click on the InfraStruXure Central interface and select **Show Tutorial**.

In addition to this Getting Started procedure and online tutorial, InfraStruXure Central features extensive task-specific online help. Just click the **Help** button on any Configuration or Administration window or right-click on the InfraStruXure Central interface and select **Show Help** to view detailed information about the task in question.

This Getting Started procedure will guide you through the processes necessary to perform the following tasks:

- Logging into your InfraStruXure Central server
- Becoming familiar with the InfraStruXure Central console
- Configuring Device Security Settings to enable mass configuration of NetBotz devices on your network
- Automatically discovering physical infrastructure devices on your network
- Creating device groups to simplify sorting and management of your physical infrastructure devices
- Creating user specific accounts that can be used to limit user access to InfraStruXure Central services or to specific device groups
- Configuring and using Sensor Imaging to simplify monitoring of your physical infrastructure devices

System and Web Browser Prerequisites

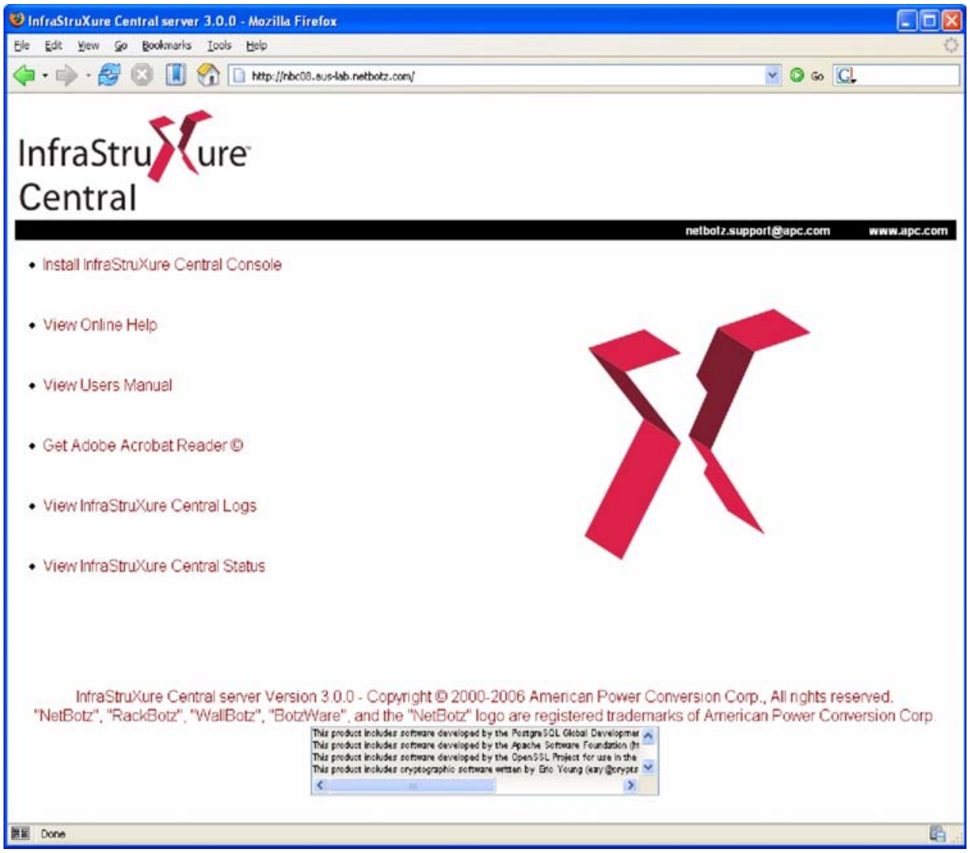
The InfraStruXure Central console is a stand-alone Java application that runs on systems that meet the following requirements:

- A PC with an 1 GHz or better AMD/Intel processor running Microsoft Windows (2000, XP SP1or SP2, or Vista) or Red Hat Enterprise Linux 4.
- Java Runtime Environment (JRE) 1.5.0_11
- 512MB RAM

Finally, your screen resolution should be set to at least 1024x768.

Logging Into InfraStruXure Central

Point your web browser at the IP address or hostname of the InfraStruXure Central server. You will see the InfraStruXure Central welcome screen.


InfraStruXure Central server 3.0.0 - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://nbc08.aus-lab.netbotz.com/
Go
InfraStruXure Central
netbotz.support@apc.com
www.apc.com
Install InfraStruXure Central Console
View Online Help
View Users Manual
Get Adobe Acrobat Reader ©
View InfraStruXure Central Logs
View InfraStruXure Central Status
Done

InfraStruXure Central server Version 3.0.0 - Copyright © 2000-2006 American Power Conversion Corp., All rights reserved.
"NetBotz", "RackBotz", "WallBotz", "BotzWare", and the "NetBotz" logo are registered trademarks of American Power Conversion Corp.

This product includes software developed by the PostgreSQL Global Developmer
This product includes software developed by the Apache Software Foundation (ht
This product includes software developed by the OpenSSL Project for use in the
This product includes cryptographic software written by Eric Young (eay@crypts

You can use the InfraStruXure Central welcome page to launch the InfraStruXure Central console, install the InfraStruXure Central console, view an online version of this User's Reference, view a list of help topics, view the InfraStruXure Central logs, or view the InfraStruXure Central server status. You can also install download and install the Adobe Acrobat Reader (required to view the online version of this User's Guide). If you haven't yet installed the InfraStruXure Central console application, click Install InfraStruXure Central console and install the application. After you have finished installing the application, click **Start > Programs >InfraStruXure Central Console > InfraStruXure Central Console** to start the application.

You will next be prompted to choose a InfraStruXure Central server to which you will log in. If you have previously logged into a InfraStruXure Central server using this console you can simply select the IP address or host name of the server from the Server selection box. Otherwise:

1. Type the IP address or host name of the InfraStruXure Central server in the **IP Address or Host Name** field.
2. If the server is configured to communicate on a port other than port 80, type the port number into the **Port** field.
3. If you will be using a SOCKS or HTTP proxy server to access your InfraStruXure Central server, click **Configure Proxy** and then provide the necessary information about the proxy in use. Click **OK** when you have finished entering proxy server information.
4. If you wish to use SSL for secure communications between the InfraStruXure Central server and

your console, check the **Connect Using SSL** check box.

5. Type in the **User** and **Password** fields the user ID and password for your InfraStruXure Central user account. If this is the first time you have used this InfraStruXure Central server and a InfraStruXure Central administrator has not created a user account for you to use, use the default User ID and Password as follows:

   User: apc

   Password: apc

   If a InfraStruXure Central administrator has created a user account for you, log in using the user ID and password that were assigned to you.

6. Check the **Save this Password** check box to save your user ID/password information.
7. Click **OK** to start the InfraStruXure Central console and to log into the server.

About the InfraStruXure Central Console

The InfraStruXure Central console is divided into three main regions, or panes. The upper-left corner pane is called the Group Navigation pane. The lower-left corner pane is called the Device Selection pane. Finally, the right-side pane is called the Action/Information pane.

The Group Navigation Pane

The Group Navigation pane displays a tree view of all device groups that are defined for use by this user account. The Group Navigation pane also functions as a basic status monitoring view. If a monitored device reports an alert the device group to which the device belongs turns red. If the device is included in multiple device groups, all groups of which it is included will turn red.

About Device Groups

Device groups contain monitored devices (such as NetBotz devices, camera pods, sensor pods, and other physical infrastructure devices). Device group definitions allow you to more easily manage devices by sorting them into smaller device groups, called “child groups.” Child groups are nested beneath their “parent group” in the Device Group selection tree. Device groups enable you to set security policies for your device groups by specifying what local user accounts or local user groups can access the device and group and usage privileges they have while doing so).

Child device groups automatically inherit the settings of their parent device group and can have additional settings as well. For example, if you create a child device group that contains only NetBotz 500s, and nest it inside a parent device group that includes only appliances with IP addresses in the 192.168.1.* subnet, your new child device group would include only NetBotz 500s with IP addresses in the 192.168.1.1-192.168.1.256 range.

The contents of a device groups can be dynamic or static. Static device groups do not change, even if new devices are discovered on the network which conform to the device groups settings, while dynamic device groups are automatically updated to include newly discovered devices that fit the device groups settings.

The Device Selection Pane

When you select a device group from the Group Navigation pane, all devices contained within the selected device group are displayed in the Device Selection pane. Depending on your Client Preferences each device will be identified by its IP address, Location value, MAC address, or Hostname.

The Device Selection pane functions as a status monitoring view for the currently selected device group. If a monitored device in the currently selected device group reports an alert, the device will turn red in the Device Selection pane. If the device has gone offline it will be “grayed out” and will have a large red X over its icon. This can be used to simplify troubleshooting and to quickly identify trouble spots.

The Device Selection pane also supports filters. You can use filters to quickly and easily limit the devices that are displayed in the Device Selection pane. Because the contents of the Device Selection pane determine what devices are displayed in the various Action/Information pane views (i.e. the Map, Table, Alert, Graph/Report, Mass Configuration, and Surveillance Views), by filtering the contents of the Device Selection pane you also filter the contents of all of the other panes as well.

The Action/Information Pane

Located on the right-hand side of the interface, the Action/Information pane contains a series of buttons that enable you to view information and perform mass configuration tasks on the devices in the currently selected device group, or the devices that are currently selected in the Device Selection pane. Also, if you have selected a filter from the Filters drop box in the Device Selection pane then the results will be further reduced according to the filter settings. Each button, when selected, presents a different view in the Action/Information pane. The Action/Information pane features 6 buttons:

Pane View	Description
Map View	Devices are displayed as icons. Current reading reported by a selected sensor is displayed for each appliance. The default sensor that is currently selected is shown above the Map View in the center of the Action/Information pane. Current status can also be indicated with sensor imaging. If you select one or more appliances from the Device Selection pane, the icons for the selected appliances are selected in the Map view as well.
Table View	Devices are displayed in a table. Problems, such as appliance outages or alert conditions are indicated by a user-defined color (red by default) in the appropriate field. If you select one or more devices from the Device Selection pane the entries for the selected appliances in the Table view are selected as well.
Alert View	Enables you to easily view all alerts that have been generated by devices in the currently selected device group. Alerts that contain picture data can also be viewed, provided that the alert has been posted to the InfraStruXure Central server using the device HTTP post support or by using the Send to InfraStruXure Central or Send HTTP Post alert actions, available using the Alert Action task. If you select one or more devices from the Device Selection pane any appliances from the device group to which the selected devices belong that have reported alerts on the date selected in the Alerts view will be listed in the Alerts View. If a device appears in the Alert View but cannot be selected (and is “grayed out”) then no alerts have been posted to or collected from the selected appliance on the selected date.

Pane View	Description
Graph/Report View	Enables you to generate reports, for a user-specified time period, from the data collected from the sensor data collected by one or more devices. The data can be plotted in a Graph view to simplify data collation and comparison, or it can be can be collated into a single report to simplify data collation, collection, and comparison. Report data (or from a selected portion of the report) can be exported to a server and saved for future reference. Report data can also be exported as a delimited value text file.
Mass Configuration	Provides complete mass device configuration functionality, enabling you to perform all of the tasks necessary for complete management of all of your devices, one at a time or all at once. The Mass Configuration panel is divided into two areas: Sensor & Alerts Settings and Management Device Settings. Each area features a number of icons that represent the mass configuration tasks that you can perform.
Surveillance View	A separately available license key-based upgrade designed for use with InfraStruXure Central. Surveillance View enables you to easily collate, index and view a summary of all surveillance event images that have been captured on a specified day or range of days. Surveillance events contain picture data that can be indexed and viewed as movie-like “clips,” enabling you to see the sequence of events that caused the Surveillance event to occur. For more information about the Surveillance View, see “Surveillance View” on page 267.

Predefined Groups

The first time you use the InfraStruXure Central console you will have one predefined device group in your Group Navigation pane: The All Devices device group. The All Devices device group includes all devices that have been added to or discovered by this InfraStruXure Central appliance and to which the currently logged in user account has access. Any device that appears in any other defined device groups will also appear in the All Devices device group. However, a device can appear in the All Devices device group even though it is not currently a member of any other defined device group. We’ll learn about creating device groups later (in “Creating Device Groups” on page 36) but for now the All Devices device group will suffice.

Setting Up Device Security Settings

Before you can manage your physical infrastructure devices, you will need to configure InfraStruXure Central to have Administrator level access to your APC NetBotz devices.

Note

These settings are used only when accessing your APC NetBotz devices. They have no effect on accessing any other supported physical infrastructure devices.

APC NetBotz devices feature user accounts, each of which has a specific User name and Password, as well as an account-specific Privilege Set. Each Privilege Set determines what device features the account can access.

By default, APC NetBotz devices come pre-configured with a Administrator user name (the default user name and password is apc/apc). However, you may have changed the user settings on your devices to enhance the security of your devices.

The Device Security Settings task enables you to configure InfraStruXure Central with the Supervisor/ Administrator User ID and Password to use when accessing your devices. Depending on your needs, you can specify a default User ID and Password to use for all of your devices, specify multiple User IDs and Passwords to use on devices that have an IP address that falls within a specified range of addresses, or specify multiple IP address-specific User IDs and Passwords.

Starting the Device Security Settings Task

To start the Security Settings task, select from the Tools pull-down menu **Server Administration > Device Security Settings**.

Creating Device Security Settings Configurations

By default, InfraStruXure Central comes pre-configured to access all NetBotz devices using the default Administrator User name/Password (apc/apc). If you haven't changed the Administrator User name/Password from the default, you can move on to the next Tutorial topic, Discovering Your Devices. However, if you have assigned a new Administrator User name/Password to some or all of your devices you will need to create additional Device Security Settings configurations for your devices. Before continuing, you should put together a list of the Administrator User name/Passwords you use for your devices.

For this example, we will assume you have devices installed in the 192.168.1.* and 192.168.2.* subnets of your network, and that you have specified a Administrator User name/Password of apc1/apc1 to all of the devices in the 192.168.1.* subnet and a Administrator User name/ Password of apc2/apc2 to all of the devices in the 192.168.2.* subnet.

Note

Obviously this probably does not accurately reflect your particular device configuration, but this example should provide you with a working understanding of the Device Security Settings task so that you can create Device Security Settings configurations that fit your needs.

To enable InfraStruXure Central to manage all of the devices, you will need to create two separate Device Security Manager configurations: one for the 192.168.1.* subnet and a second for the 192.168.2.* subnet.

1. Click **Create** and then create a Device Security Settings configuration for the devices 192.168.1.* subnet.
   a. The Create Security Entry window opens.
   b. Type in the **IP Range** field 192.168.1.*.
   c. If you are using a port other than port 80 for device network communications, type in the **Port** field the port number in use.
   d. Type in the **User ID** field apc1.
   e. Type in the **Password** field apc1.
   f. Click **OK** to save this configuration.
2. Click Create and then create a Device Security Settings configuration for the devices on the 192.168.2.* subnet.
   a. The Create Security Entry window opens.
   b. Type in the **IP Range** field 192.168.2.*.

c. If you are using a port other than port 80 for device network communications, type in the **Port** field the port number in use.

d. Type in the **User ID** field apc2.

e. Type in the **Password** field apc2.

f. Click **OK** to save this configuration.

3. Click the **X** in the upper right-hand corner of the window to close the Device Security Settings window.

Discovering Your Devices

InfraStruXure Central can automatically search a user-specified IP address range on your network for supported management and SNMP devices. If new devices are discovered, InfraStruXure Central will add them to the All Devices device group. Later, when you have defined additional device groups, discovered devices will be automatically added to any appropriate device groups. Before devices can be discovered, however, you must configure the InfraStruXure Central Discovery Settings.

Starting the Discovery Settings Task

To start the Discovery Settings task, select from the Tools pull-down menu **Server Administration > Discovery Settings**.

Configuring InfraStruXure Central Discovery Settings

For this example, we will assume you have management devices installed in the 192.168.1.* and 192.168.2.* subnets of your network, that all of the management devices on subnet 192.168.1.* are configured to use port 80 for network communications, that all of the management devices on subnet 192.168.2.* are configured to use port 100 for network communications, and that you want to discover management devices each Sunday at 5:00PM.

Note

Obviously this probably does not accurately reflect your particular device configuration, but this example should provide you with a working understanding of the Discovery Settings task so that you can create discovery configurations that fit your needs.

1. Click **Create** and then create a discovery configuration for devices on the 192.168.1.* subnet.

a. The Create Discovery Entry opens.

b. Select the **Management device** radio button and then click **Next**.

c. Type in the **IP Range** field 192.168.1.*.

d. Type in the **Port Range** field 80.

e. Specify **SSL Options**. By default, Do not use SSL is selected. If desired, you can configure the Discovery Settings to *use SSL if available*, *require SSL without verification*, or *require SSL with verification*.

f. Check the **Enable schedule** check box. If discovery is not enabled, the discovery settings are saved but no discovery functions are actually carried out.

g. Click **Sunday** in the **Days** check boxes. This is the day of the week the discovery process will run.

h. Use the **Time** controls to specify 5:00 PM. This is the time of day the discovery process will run.

i. Click **Finish** to save this configuration.

2. Click **Create** and then create a Discovery configuration for devices on the 192.168.2.* subnet.

a. The Create Discovery Entry opens.

   b. Select the **Management device** radio button and then click **Next**.
   c. Type in the **IP Range** field 192.168.2.*.
   d. Type in the **Port Range** field 100.
   e. Specify **SSL Options**. By default, Do not use SSL is selected. If desired, you can configure the Discovery Settings to *use SSL if available*, *require SSL without verification*, or *require SSL with verification*.
   f. Check the **Enable schedule** check box. If discovery is not enabled, the discovery settings are saved but no discovery functions are actually carried out.
   g. Click **Sunday** in the **Days** check boxes. This is the day of the week the discovery process will run.
   h. Use the **Time** controls to specify 5:00 PM. This is the time of day the discovery process will run.
   i. Click **Finish** to save this configuration.

3. Now, unless it's Sunday and about 4:55PM you probably don't want to wait for the discovery process to begin. You can use the **Start** button to instruct InfraStruXure Central to run any selected discovery configuration immediately. To run discovery on your subnets right now, select each discovery setting and then click **Start**.

4. Click the **X** in the upper right-hand corner of the window to close the Discovery Settings window.

Creating Device Groups

InfraStruXure Central makes it easy to organize and manage your physical infrastructure devices by enabling you to create device groups. Device group definitions enable you to more easily manage devices by sorting them automatically into smaller device groups. Device groups also enable you to set security policies for your device groups by specifying what local user accounts or local user groups can access the device and group and usage privileges they have while doing so.

The contents of your device groups can also be dynamic or static. Static device groups do not change, even if new devices are discovered on the network which conform to the device groups settings, while dynamic device groups are automatically updated to include newly discovered devices that fit the device groups settings.

Starting Device Group Administration

To start the Group Administration task, select from the Tools pull-down menu **Server Administration > Device Group Administration**. When you start the Device Group Administration task all currently defined device groups are displayed in a tree view. If you have not defined new device groups the only device group shown will be the All Devices group, which contains all devices that have been discovered on your network. To view the settings of a previously created device group select it from the tree view.

Creating New Device Groups

For this example, we will assume you want to create two new device groups: one device group that is for all management devices that are installed on the 192.168.1.* subnet, and a second device group that is only for NetBotz 500 management devices that are installed on the 192.168.2.* subnet. We will also assume that both of these device groups will be dynamic.

Note

Obviously this probably does not accurately reflect your particular device configuration, but this example should provide you with a working understanding of the Device Group Administration task so that you can create device groups that fit your needs.

1. Click **Create** and then create a new device group that will contain any NetBotz management

devices on the 192.168.1.* subnet.

a. Type in the **Label** field *Devices on 192.168.1.**.

b. Leave the **Parent** drop box set to *All Devices* (note that you can also nest device groups within other device groups, if desired).

c. Select the Dynamic tab and then use the controls at the bottom of the window to build rules for this device group.

d. Click **More** to add a new set of rules controls to the interface.

e. Select **IP address > equals** and then type *192.168.1.** in the rules field.

f. Select the Security tab. This pane displays a list of all local user accounts and local user groups that currently are permitted to access this device group, and also displays the Device privilege and Surveillance privilege settings for each local user account or local user group. We'll leave these settings unchanged for now.

g. Click **OK** to save this device group. Your new device group appears in the Device Group Navigation pane and any previously discovered devices that apply to these device groups are automatically added to your device groups.

2. Click **Create** and then create a new device group that will contain only NetBotz 500 model management devices on the 192.168.1.* subnet.

a. Type in the **Label** field *NetBotz 500 devices on 192.168.1.**.

b. Leave the **Parent** drop box set to *All Devices* (note that you can also nest device groups within other device groups, if desired).

c. Select the Dynamic tab and select the **Devices must match all of the following** radio button. Then use the controls at the bottom of the window to build rules for this device group.

d. Click **More** to add a new set of rules controls to the interface.

e. Select **IP address > equals** and then type *192.168.1.** in the rules field.

f. Click **More** to add a new set of rules controls to the interface.

g. Select **Model > equals > 500**.

h. Select the Security tab. This pane displays a list of all local user accounts and local user groups that currently are permitted to access this device group, and also displays the Device privilege and Surveillance privilege settings for each local user account or local user group. We'll leave these setting sun changed for now.

i. Click **OK** to save this device group. Your new device group appears in the Device Group Navigation pane and any previously discovered devices that apply to these device groups are automatically added to your device groups.

About Devices that Appear in Multiple Device Groups

Depending on your device group configuration, it is possible for individual devices to appear in multiple device groups. For example, if you have both an All Devices device group and a second device group that includes only rack model NetBotz devices, all of your rack model NetBotz devices will be included in both the RackBotz device group and the All Devices device group. This will have no effect on the size of your InfraStruXure Central database. Though devices can be included in multiple device groups, the data for each device is stored in the InfraStruXure Central database only once.

Creating User Accounts

Use the selections available from the User/Group Administration task to create or modify local user accounts and local user groups for your InfraStruXure Central server. Local user accounts on your InfraStruXure Central server are allowed access only to specified device groups User/Group Administration also enables you to create local user groups. Local user groups are collections of local user accounts. When local user accounts are added, you can simply add the new local user account to a previously defined local user group. You can also create local user groups that automatically enable full administrator privileges for any local users that are added to the group. If a user account or user group is not specifically created with administrator privileges, the user privileges will be determined by the Security settings of the device group to which they are added.

Starting User/Group Administration

To start the User/Group Administration task, select from the Tools pull-down menu **Server Administration > User/Group Administration**.

Creating New User Accounts

For this example, we will assume you want to create two new user accounts: one account (for User1) that will have Administrator access to InfraStruXure Central, and one account (for User2) that will have only the default access permitted by the device group to which it is later added.

Note

Obviously this probably does not accurately reflect your particular user account needs, but this example should provide you with a working understanding of the User/Group Administration task so that you can create user accounts that fit your needs.

After starting the User/Group Administration task, select the User Administration tab.

1. Click **Create** and then create a new user account that will enable User1 to log into the InfraStruXure Central server as a member of the Administrator user group. By default, members of the Administrators user group have View and Modify permissions on all InfraStruXure Central services.
   a. The Create User window opens. Select the **User Information** tab.
   b. Check the **Enabled** check box.
   c. Type User1 in the **User name** field.
   d. Type User1’s name in the **Full Name** field.
   e. Type a password for User1 in the **Password** and **Verify Password** fields.
   f. Type User1’s e-mail address in the **E-mail Address** field.
   g. If desired, type additional information in the **Description** field.
   h. Select the **User Roles** tab.
   i. Check the **InfraStruXure Central administrator** check box. Leave the **InfraStruXure Central Proxy Access** check box unchecked.
   j. Select the **User Group Membership** tab. The controls on this pane enable you to add the user account to one or more of the previously defined user groups. However, because this is a new user account, no user groups will be listed in this pane. Click **Add User Group**, then select Server Administrators from the list of available groups and click **OK**.
   k. Click **OK** to save this user account.
2. Click **Create** and then create a new user account that will enable User2 device group privileges that are defined by the Security settings of each device group on your server.

a. The Create User window opens. Select the **User Information** tab.
b. Check the **Enabled** check box.
c. Type User2 in the **User name** field.
d. Type User2’s name in the **Full Name** field.
e. Type a password for User2 in the **Password** and **Verify Password** fields.
f. Type User2’s e-mail address in the **E-mail Address** field.
g. If desired, type additional information in the **Description** field.
h. Select the **User Roles** tab.
i. Leave both the **InfraStruXure Central administrator** and the **InfraStruXure Central Proxy Access** check boxes unchecked.
j. Select the **User Group Membership** tab. The controls on this pane enable you to add the user account to one or more of the previously defined user groups. However, because this is a new user account, no user groups will be listed in this pane. Click **Add User Group**, then select Server Administrators from the list of available groups and click **OK**.
k. Click **OK** to save this user account.

3. Click the **X** in the upper right-hand corner of the window to close the User/Group Administration task. When User1 or User2 attempt to log into the InfraStruXure Central server, their user accounts will determine the level of access they have to your devices, device groups, and InfraStruXure Central services.

Creating and Editing Groups

You can use local user groups to quickly and easily organize your local user accounts into groups for simplified user account management. Local user groups can also be created that automatically enable full administrator access to all InfraStruXure Central functionality on all local user accounts that are added to the local user group.

To create a user group, or to edit a previously defined user group:

1. Start the User/Group Administration task and then select the Local User Groups tab. A list of all currently defined local user groups is displayed.

2. To create a new user group, click **Create**. To edit a previously defined user group select the user group and then click **Edit**.

3. The New User Group (or Edit User Group, if you are editing a previously created account) window appears. This window consists of 3 tabbed panes: The Group Information pane, the Group Roles pane, and the Group Members pane.

4. Select the **Group Information** pane and type in the **Group name** field a name that will be associated with this local user group.

5. Select the **Group Roles** pane. The controls on this pane enable you to configure the local group to automatically enable full administrator privileges and/or SOCKS proxy to access devices on both the public network and the internal DHCP LAN (or “private” LAN) when enabled for any local users that are added to the group. Leave both the **InfraStruXure Central administrator** check box and the **InfraStruXure Central Proxy Access** check box unchecked.

6. Select the **Group Members** pane. This pane features a list of local user accounts that are members of this local user group. To add a local user account to this local user group, click **Add User**, select one or more previously defined local user accounts from the **Choose User(s)** pane, and then click

OK.

7. Click **OK** to save your local user group settings.

Using Sensor Imaging

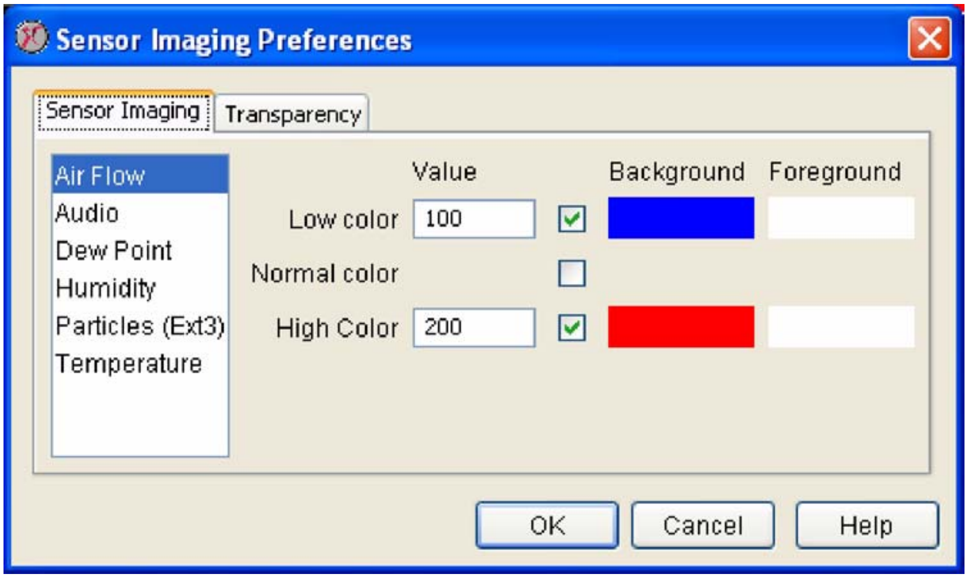
Sensor Imaging enables you to see at a glance the general state of each of your devices. Once you have defined a range of values for the currently selected Display Sensor, the color of the device icon will change to reflect where it's current sensor reading falls in the display imaging range. By setting imaging values that range from the optimal value to a value that equals the value at which an alert will be triggered you can use display imaging to spot “trouble spots” in your facilities before alerts start going off.

Sensor Imaging is enabled by default, with a default value range pre-configured for each of the device sensors. To enable or disable Sensor Imaging:

1. Right-click on the Map View. This will open a context menu.
2. Click **Use Sensor Imaging > On** (or **Off**).

Depending on your environment and needs, you may wish to change the Sensor Imaging values for your devices. To review or change your Sensor Imaging settings:

1. Right-click inside the Map View. This will open a context menu.
2. Click **Sensor Imaging Preferences**. The Sensor Imaging Preferences window opens.



Sensor Imaging Preferences

Sensor Imaging | Transparency

Air Flow
Audio
Dew Point
Humidity
Particles (Ext3)
Temperature

	Value		Background	Foreground
Low color	100	☑	🟦	
Normal color		☐		
High Color	200	☑	🟥	

3. Select a sensor from the **Sensor List** selection list to view its current Sensor Imaging configuration. Once you select a sensor, the high and low values used to define the Senor Imaging range for that sensor are displayed in the **Low Color** and **High Color** fields. Also, the colors that are currently defined for the Low, Normal, and High Sensor Imaging states are shown in the **Low Color**, **Normal Color**, and **High Color** drop boxes.

   If the sensor value that is reported by a device is less than the value you specify for the sensor in the **Low Value** field then a semi-transparent block of the **Low Color** will appear behind the device icon. If the sensor value that is reported by a device is higher than the value you specify for the sensor in the **High Value** field then a semi-transparent block of the **High Color** will appear behind the device icon. If the value falls between or equals either the **Low** and **High** values then a semi-transparent block of the **Normal Color** will appear behind the device icon.

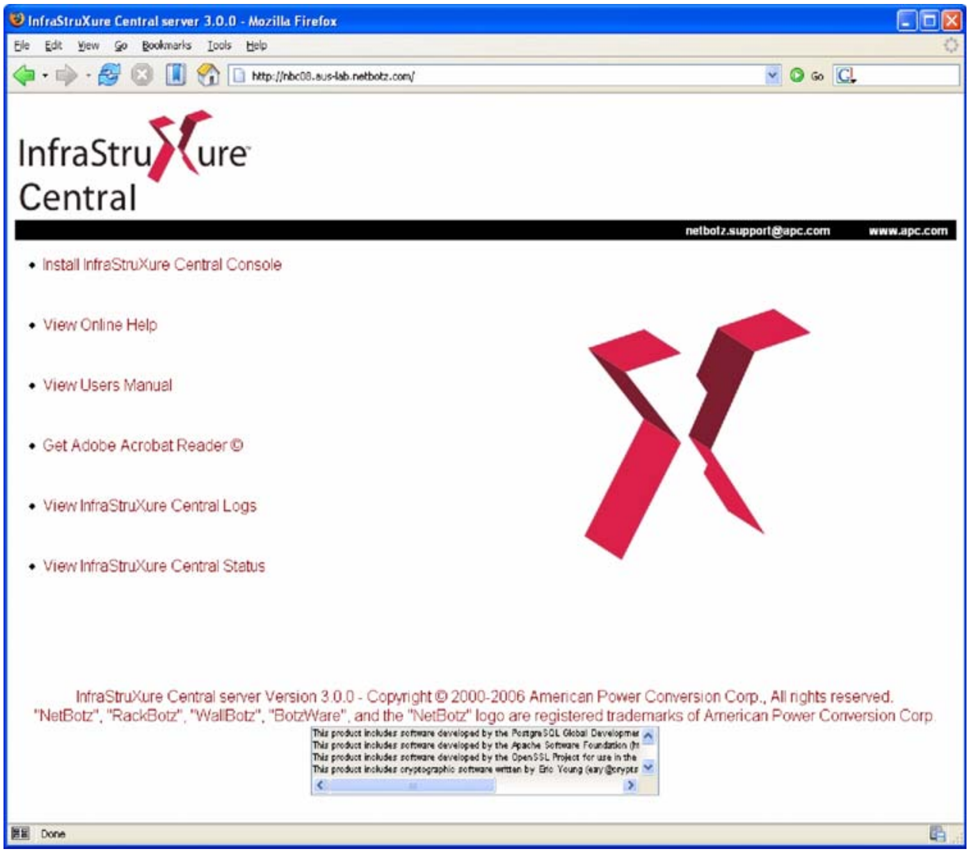
If you want to change any of these settings for a sensor, simply select the sensor, specify new low and/or high values, and select new **Sensor Imaging colors** as desired. You can also use the slider control in the **Transparency** tab to adjust the transparency of the Sensor Imaging color blocks that appears behind the icon in the Map view.

4. When you are finished, click **OK** to save your new Sensor Imaging configuration.

The InfraStruXure Central Console

The InfraStruXure Central console is a stand-alone Java application that is used to access and manage the InfraStruXure Central server. Before you can use the InfraStruXure Central console you must first install the application using your *InfraStruXure Central Installer* CD-ROM. If you have already installed the InfraStruXure Central console, click **Start > Programs > InfraStruXure Central Console > InfraStruXure Central Console** to start the application.

If you have not installed the application, use your *InfraStruXure Central Installer* CD-ROM to do so. Alternately, you can point your web browser at the IP address or hostname of the InfraStruXure Central server and install the InfraStruXure Central console from the server's welcome screen.


InfraStruXure Central server 3.0.0 - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://nbc08.aus-lab.netbotz.com/
Go
InfraStruXure Central
netbotz.support@apc.com
www.apc.com
Install InfraStruXure Central Console
View Online Help
View Users Manual
Get Adobe Acrobat Reader ©
View InfraStruXure Central Logs
View InfraStruXure Central Status
Done

InfraStruXure Central server Version 3.0.0 - Copyright © 2000-2006 American Power Conversion Corp., All rights reserved.
"NetBotz", "RackBotz", "WallBotz", "BotzWare", and the "NetBotz" logo are registered trademarks of American Power Conversion Corp.

This product includes software developed by the PostgreSQL Global Developmer
This product includes software developed by the Apache Software Foundation (ht
This product includes software developed by the OpenSSL Project for use in the
This product includes cryptographic software written by Eric Young (eay@crypts

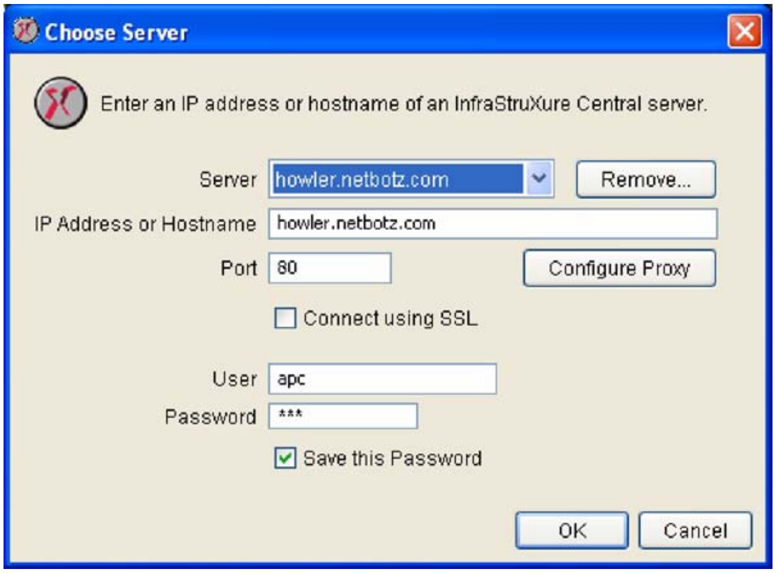
You can also use the InfraStruXure Central welcome screen to:

- Launch the InfraStruXure Central console (if it has been installed)
- View online help topics
- View the *InfraStruXure Central User's Reference* (this document) in PDF format
- Install Adobe Acrobat Reader

Click **Install InfraStruXure Central Console** to install the InfraStruXure Central console. After you have finished installing the application, click **Start > Programs >InfraStruXure Central Console > InfraStruXure Central Console** to start the application.

Logging Into InfraStruXure Central

You will next be prompted to choose a InfraStruXure Central server to which you will log in.



Enter an IP address or hostname of an InfraStruXure Central server.

Server: howler.netbotz.com

IP Address or Hostname: howler.netbotz.com

Port: 80

□ Connect using SSL

User: apc

Password: ***

☑ Save this Password

If you have previously logged into a InfraStruXure Central server using this console you can simply select the IP address or host name of the server from the **Server** selection box. Otherwise:

1. Type the IP address or host name of the InfraStruXure Central server in the **IP Address or Host Name** field.

2. If the server is configured to communicate on a port other than port 80, type the port number into the **Port** field.

3. If you will be using a SOCKS or HTTP proxy server to access your InfraStruXure Central server, click **Configure Proxy** and then provide the necessary information about the proxy in use. Click **OK** when you have finished entering proxy server information.

4. If your InfraStruXure Central server is configured to use SSL for secure communications between the InfraStruXure Central server and your console, check the **Connect Using SSL** check box. For information on how to configure your InfraStruXure Central server to use SSL, see “Using the Secure Sockets Layer (SSL) Pane” on page 101.

5. Type in the **User** and **Password** fields the user ID and password for your InfraStruXure Central user account. If this is the first time you have used this InfraStruXure Central server and a InfraStruXure Central administrator has not created a user account for you to use, use the default User ID and Password as follows:

   User Name: apc

   Password: apc

   If a InfraStruXure Central administrator has created a user account for you, log in using the User Name and Password that were assigned to you.

6. Check the **Save this Password** check box to save your user ID/password information.

7. Click **OK** to start the InfraStruXure Central console and to log into the server.

Interface Navigation

After you have logged in, you will see the InfraStruXure Central console. The InfraStruXure Central console is divided into three main regions, or panes. The upper-left corner pane is called the Device Group Navigation pane. The lower-left corner pane is called the Device Selection pane. Finally, the right-side pane is called the Action/Information pane.

Configuring Offline Devices

If a device goes offline, InfraStruXure Central will assume that the offline state is a temporary event. When a device is in an offline state you can still perform Mass Configuration tasks on the device. InfraStruXure Central will store these tasks in the Management Device Job Control queue, and will automatically perform the tasks as soon as the device comes back online.

The Device Group Navigation Pane

The Device Group Navigation pane displays a tree view of all device groups that are defined for this user account. The Device Group Navigation pane also functions as a basic status monitoring view. If a monitored device reports an alert the device group (or device groups, if the device is included in multiple device groups) to which the device belongs turns red.

About Device Groups

Device groups contain monitored devices (such as NetBotz devices, camera pods, sensor pods, and other physical infrastructure devices). Device group definitions allow you to more easily manage devices by sorting them into smaller device groups, called “child groups.” Child groups are nested beneath their “parent group” in the Device Group selection tree. Device groups enable you to set security policies for your device groups by specifying what local user accounts or local user groups can access the device and group and usage privileges they have while doing so.).

Child device groups automatically inherit the settings of their parent device group and can have additional settings as well. For example, if you create a child device group that contains only NetBotz 500s, and nest it inside a parent device group that includes only appliances with IP addresses in the 192.168.1.* subnet, your new child device group would include only NetBotz 500s with IP addresses in the 192.168.1.1-192.168.1.256 range.

The contents of a device groups can be dynamic or static. Static device groups do not change, even if new devices are discovered on the network which conform to the device groups settings, while dynamic device groups are automatically updated to include newly discovered devices that fit the device groups settings.

The Device Selection Pane

When you select a device group from the Group Navigation pane, all devices contained within the selected device group are displayed in the Device Selection pane. Depending on your Client Preferences (see “InfraStruXure Central Client Preferences” on page 61) each device will be identified by its IP address, Location value, MAC address, or Hostname.

The Device Selection pane functions as a status monitoring view for the currently selected device group. If a monitored device in the currently selected device group reports an alert, the device will turn red in the Device Selection pane. If the device has gone offline it will be “grayed out” and will have a large red X over its icon. This can be used to simplify troubleshooting and to quickly identify trouble spots.

The Device Selection pane also supports filters. You can use filters to quickly and easily limit the devices that are displayed in the Device Selection pane. Because the contents of the Device Selection pane determine what devices are displayed in the various Action/Information pane views (i.e. the Map, Table, Alert, Graph/Report, Mass Configuration, and Surveillance Views), by filtering the contents of the Device Selection pane you also filter the contents of all of the other panes as well.

The Action/Information Pane

Located on the right-hand side of the interface, the Action/Information pane contains a series of buttons that enable you to view information and perform mass configuration tasks on the devices in the currently selected device group, or the devices that are currently selected in the Device Selection pane. Each button, when selected, presents a different view in the Action/Information pane. The Action/Information pane features 6 buttons:

Action Pane View	Description
Map View	All devices in the selected device group are displayed as icons. Current reading reported by a selected sensor is displayed for each device. The default sensor that is currently selected is shown above the Map View in the center of the Action/ Information pane. Current status can also be indicated with sensor imaging. If you select one or more devices from the Device Selection pane, the icons for the selected devices are selected in the Map view as well.
Table View	Data about all devices in the selected device group are displayed in a table. Problems, such as device outages or alert conditions are indicated by a user-defined color (red by default) in the appropriate field. If you select one or more devices from the Device Selection pane the entries for the selected devices in the Table view are selected as well.
Alert View	Enables you to easily view all alerts that have been generated by NetBotz devices in the currently selected device group. Alerts that contain picture data can also be viewed from this pane if the alerts are posted to the InfraStruXure Central server using HTTP Post support (for more information, see “Creating a Send HTTP Post Alert Action” on page 239). If you select one or more devices from the Device Selection pane any devices from the device group to which the selected devices belong that have reported alerts on the date selected in the Alerts view will be listed in the Alerts view. If a device appears in the Alerts view but cannot be selected (and is “grayed out”) then no alerts have been posted to or collected from the selected device on the selected date.
Graph/Report View	Data about one or more selected sensors, for a user-specified time period, is collated and then either plotted in a color-coded line graph or used to generate a report. Data about multiple devices can be graphed in a single graph view to simplify data collation and comparison.
Mass Configuration	Provides complete mass device configuration functionality, enabling you to perform all of the tasks necessary for complete management of all of your devices, one at a time or all at once. The Mass Configuration panel is divided into two areas: Sensor & Alerts Settings and Host Device Settings. Each area features a number of icons that represent the mass configuration tasks that you can perform.

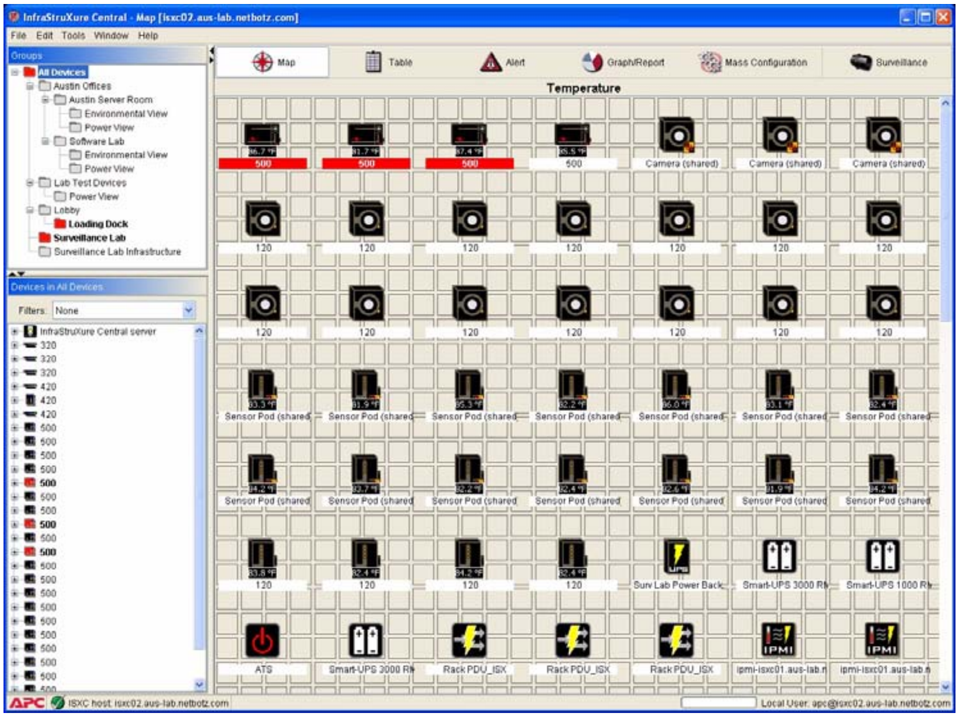
Action Pane View	Description
Surveillance View	A separately available license key-based upgrade designed for use with InfraStruXure Central. Surveillance View enables you to easily collate, index and view a summary of all surveillance event images that have been captured on a specified day or range of days. Surveillance events contain picture data that can be indexed and viewed as movie-like “clips,” enabling you to see the sequence of events that caused the Surveillance event to occur. For more information about the Surveillance View, see “Surveillance View” on page 267.

Predefined Device Groups

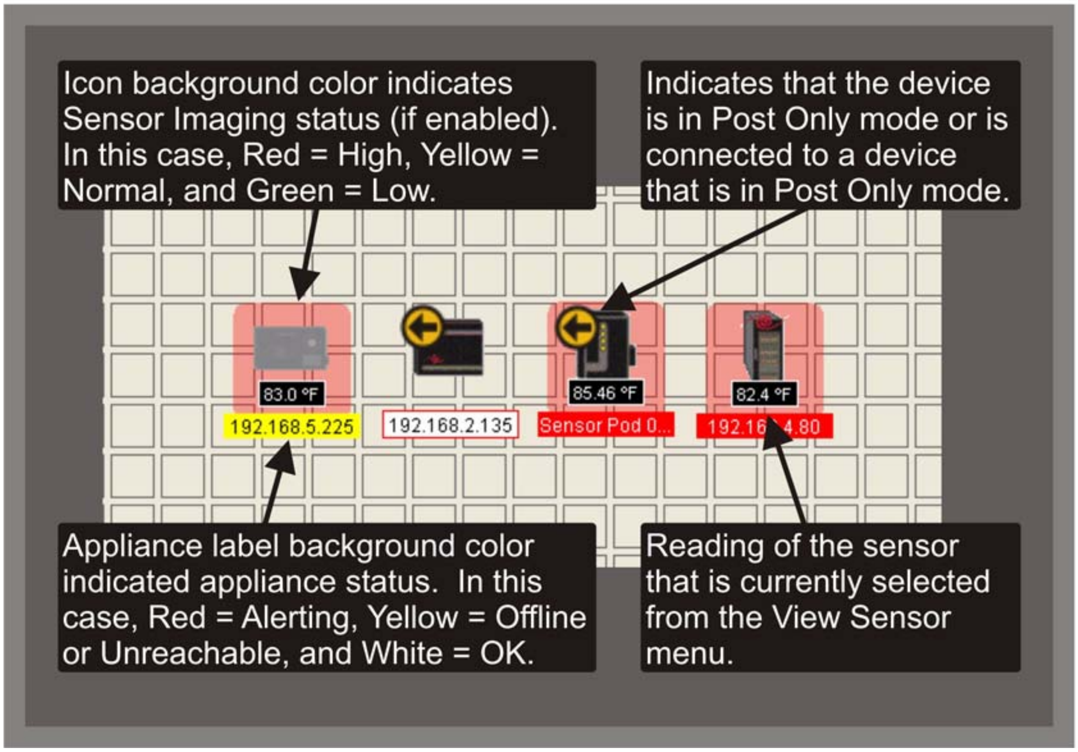
The first time you use the InfraStruXure Central console you will have one predefined device group in your Device Group Navigation pane: The All Devices device group. The All Devices device group includes all devices that have been added to or discovered by this InfraStruXure Central server and to which the currently logged in user account has access. Any device that appears in any other defined device groups will also appear in the All Devices device group. However, a device can appear in the All Devices device group even though it is not currently a member of any other defined device group.

Map View

The InfraStruXure Central Map View presents all devices in the currently selected device group in an easy-to-monitor graphic display. Colors are used to indicate the current state of each devices in the device group, alerts or network outages are easily noted, and the current reading of a selected sensor is displayed for all devices. You can also use custom background graphics and rearrange the contents of the device group to better represent the physical environment in which the devices are installed, making it easier to locate problem areas in your installation.



To use the Map view, select a device group from the Device Group Navigation pane and then click the Map tab. The devices that are part of the selected device group appear in the Map view window. Each device is shown as an icon, along with a display name (IP address, location value, or hostname, depending on your Client Preferences), and a current sensor reading. Also, any devices that are in Post Only mode, or that are connected to devices that are in Post Only mode, are indicated with a small yellow and black arrow icon as shown below:



Icon background color indicates Sensor Imaging status (if enabled). In this case, Red = High, Yellow = Normal, and Green = Low.

Indicates that the device is in Post Only mode or is connected to a device that is in Post Only mode.

Appliance label background color indicated appliance status. In this case, Red = Alerting, Yellow = Offline or Unreachable, and White = OK.

Reading of the sensor that is currently selected from the View Sensor menu.

The default sensor that is currently selected is shown above the Map view, in the center of the Action/ Information pane. If you select one or more devices from the Device Selection pane, the icons for the selected devices are selected in the Map view as well. To access other InfraStruXure Central Map View functions, right-click on the Map view to open the Map View context menu. The following selections are available from this context menu:

Context Menu Selection	Description
New...	Adds a user-specified management device or SNMP device. For more information, see “Adding New Devices” on page 111. **Note:** If the added device does not meet the configuration criteria for inclusion in the currently selected device group, the device group will not be shown. However, the device will be automatically added to any dynamically defined device groups with appropriate configuration criteria.

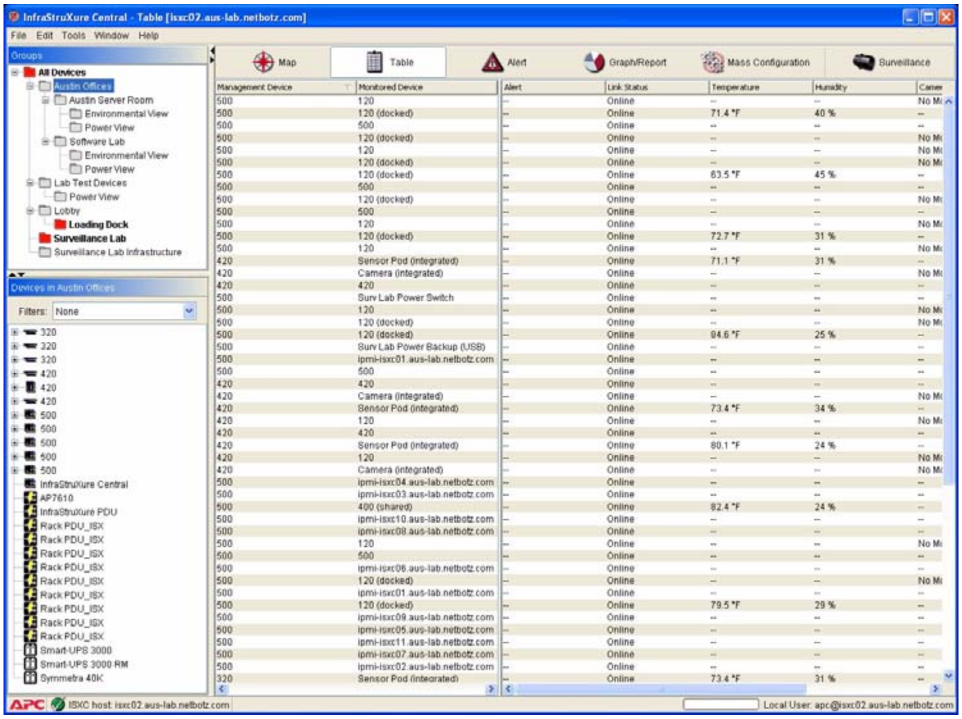
Context Menu Selection	Description
Delete device	Deletes all selected devices. **Note:** Deleting a device purges all data associated with the device from the InfraStruXure Central database and also deletes the device from any other device groups in which it exists, including other device groups to which you may not have access. Improper use of this function could result in loss of data and could also impact other InfraStruXure Central users.
Delete monitored device	Deletes all selected monitored devices (such as Sensor Pod 120s or Camera Pod 120s). **Note:** Deleting a monitored device purges all data associated with the monitored device from the InfraStruXure Central database and also deletes the monitored device from any other device groups in which it exists, including other device groups to which you may not have access. Improper use of this function could result in loss of data and could also impact other InfraStruXure Central users.
Find Device...	Simplifies finding specified devices. Type in the IP address, host name, or location information for the device you are trying to find. If it is located on the currently selected map it will be selected for you automatically.
Change Icon	Each device displayed in the Map View is represented by a default device type icon. If desired, you can use the Change Icon selection to specify a unique device-specific icon instead of the default icon.
Use Sensor Imaging	Use this control to enable or disable Map View sensor imaging.
Sensor Imaging Preferences	Use this control to specify sensor imaging settings. Sensor imaging enables you to see at a glance the general state of each of your devices. Once you have defined a range of values for the currently selected sensor, the background color behind a device icon will change to reflect where it's current sensor reading falls in the sensor imaging range. By setting imaging values that range from the optimal value to a value that equals the value at which an alert will be triggered you can spot "trouble spots" in your installations before alerts start going off.
Selection	Use this control to quickly select or un-select all devices in the Map View.
Sort by Alert	When enabled, the Sort by Alert function automatically sorts the devices in your map, displaying any devices that are offline first, followed by any devices that are reporting an alert, followed finally by device that are online and in a normal state.

Context Menu Selection	Description
Edit Map	Use the selections available from the Edit Map menu to create a custom map, delete a previously saved custom map, specify icon preferences, add a custom background image to your Map, and to specify sensor display preferences. For more information, see “Editing Map Settings” on page 252.
View Current Sensors	Opens a window that displays the current sensor readings and image capture for the selected device.
Launch Browser	Opens your system's web browser and directs it at the URL of the selected device.
Request Device Scan	Select this to cause InfraStruXure Central to initiate a scan of the selected SNMP device immediately.
Mass Configuration	Use this flyout menu to quickly select and start Mass Configuration tasks on the selected devices.
Filters	Enables you to create, edit, or delete filters. These filters are used to determine which devices are included in the Map and Table View. For more information, see “Creating or Editing Filters” on page 57.
Tutorial	Select Tutorial to display the InfraStruXure Central tutorial. Once you have opened the tutorial it will automatically start each time you start the InfraStruXure Central console until you un-check the **Show this at next startup** check box.
Help	Select Help to view the InfraStruXure Central online help.

For more information on the Map view, see “Using the Map View” on page 249.

Table View

The InfraStruXure Central Table view presents all devices in the currently selected device group in an easy-to-monitor and read table display. Colors are used to indicate the current state of each device in the device group making alerts or offline devices easy to spot. You can also use Table Preferences to specify the data that is displayed for each device.



Management Device	Monitored Device	Alert	Link Status	Temperature	Humidity	Camer
500	120	--	Online	--	--	No M
500	120 (docked)	--	Online	71.4 °F	40 %	--
500	500	--	Online	--	--	--
500	120 (docked)	--	Online	--	--	No M
500	120	--	Online	--	--	No M
500	120 (docked)	--	Online	--	--	No M
500	120 (docked)	--	Online	63.5 °F	45 %	--
500	500	--	Online	--	--	--
500	120 (docked)	--	Online	--	--	No M
500	500	--	Online	--	--	--
500	120	--	Online	--	--	No M
500	120 (docked)	--	Online	72.7 °F	31 %	--
500	120	--	Online	--	--	No M
420	Sensor Pod (integrated)	--	Online	71.1 °F	31 %	--
420	Camera (integrated)	--	Online	--	--	No M
420	420	--	Online	--	--	--
500	Surv Lab Power Switch	--	Online	--	--	--
500	120	--	Online	--	--	No M
500	120 (docked)	--	Online	--	--	No M
500	120 (docked)	--	Online	84.6 °F	25 %	--
500	Surv Lab Power Backup (USB)	--	Online	--	--	--
500	ipmi-isxc01.aus-lab.netbotz.com	--	Online	--	--	--
500	500	--	Online	--	--	--
420	420	--	Online	--	--	--
420	Camera (integrated)	--	Online	--	--	No M
420	Sensor Pod (integrated)	--	Online	73.4 °F	34 %	--
420	120	--	Online	--	--	No M
420	420	--	Online	--	--	--
420	Sensor Pod (integrated)	--	Online	80.1 °F	24 %	--
420	120	--	Online	--	--	No M
420	Camera (integrated)	--	Online	--	--	No M
500	ipmi-isxc04.aus-lab.netbotz.com	--	Online	--	--	--
500	ipmi-isxc03.aus-lab.netbotz.com	--	Online	--	--	--
500	400 (shared)	--	Online	82.4 °F	24 %	--
500	ipmi-isxc10.aus-lab.netbotz.com	--	Online	--	--	--
500	ipmi-isxc08.aus-lab.netbotz.com	--	Online	--	--	--
500	120	--	Online	--	--	No M
500	500	--	Online	--	--	--
500	ipmi-isxc06.aus-lab.netbotz.com	--	Online	--	--	--
500	120 (docked)	--	Online	--	--	No M
500	ipmi-isxc01.aus-lab.netbotz.com	--	Online	--	--	--
500	120 (docked)	--	Online	79.5 °F	29 %	--
500	ipmi-isxc09.aus-lab.netbotz.com	--	Online	--	--	--
500	ipmi-isxc05.aus-lab.netbotz.com	--	Online	--	--	--
500	ipmi-isxc11.aus-lab.netbotz.com	--	Online	--	--	--
500	ipmi-isxc07.aus-lab.netbotz.com	--	Online	--	--	--
500	ipmi-isxc02.aus-lab.netbotz.com	--	Online	--	--	--
320	Sensor Pod (integrated)	--	Online	73.4 °F	31 %	--

ISXC host: isxc02.aus-lab.netbotz.com

Local User: apc@isxc02.aus-lab.netbotz.com

To use the Table view, select a device group from the Device Group Navigation pane and then click the Table button. Data about all devices in the selected device group are displayed in a table. Problems, such as device outages or alert conditions, are indicated by a user-defined color (red by default; for information on how to change the default colors see “InfraStruXure Central Client Preferences” on page 61) in the appropriate field. If you select one or more devices from the Device Selection pane the entries for the selected devices in the Table view are selected as well.

To access other InfraStruXure Central Table view functions, right-click on the Table view to open the Table View context menu. The following selections are available from this context menu:

Context Menu Selection	Description
New...	Adds a user-specified management device or SNMP device. For more information, see “Adding New Devices” on page 111. **Note:** If the added device does not meet the configuration criteria for inclusion in the currently selected device group, the device group will not be shown. However, the device will be automatically added to any dynamically defined device groups with appropriate configuration criteria.

Context Menu Selection	Description
Delete Device	Deletes all selected devices from the current Map. **Note:** Deleting a device purges all data associated with the device from the InfraStruXure Central database and also deletes the device from any other device groups in which it exists, including other device groups to which you may not have access. Improper use of this function could result in loss of data and could also impact other InfraStruXure Central users.
Delete Monitored Device	Deletes all selected monitored devices (such as Sensor Pod 120s or Camera Pod 120s) from the currently selected group. **Note:** Deleting a monitored device purges all data associated with the monitored device from the InfraStruXure Central database and also deletes the monitored device from any other device groups in which it exists, including other device groups to which you may not have access. Improper use of this function could result in loss of data and could also impact other InfraStruXure Central users.
Table Preferences	Use this control to specify what device data will be displayed for each device in the Table view.
Export Table	Use this control to export the appliance data displayed in the table to a delimited value file.
View Current Sensors	Opens a window that displays the current sensor readings and image capture for the selected appliance.
Request Device Scan	Select this to cause InfraStruXure Central to initiate a scan of the selected SNMP device immediately.
Launch Browser	Opens your system's web browser and directs it at the URL of the selected device.
Filters	Enables you to create, edit, or delete filters. These filters are used to determine which devices are included in the Map and Table View. For more information, see “Creating or Editing Filters” on page 57.
Tutorial	Select Tutorial to display the InfraStruXure Central tutorial. Once you have opened the tutorial it will automatically start each time you start the InfraStruXure Central console until you un-check the **Show this at next startup check box.**
Help	Select Help to view the InfraStruXure Central online help.

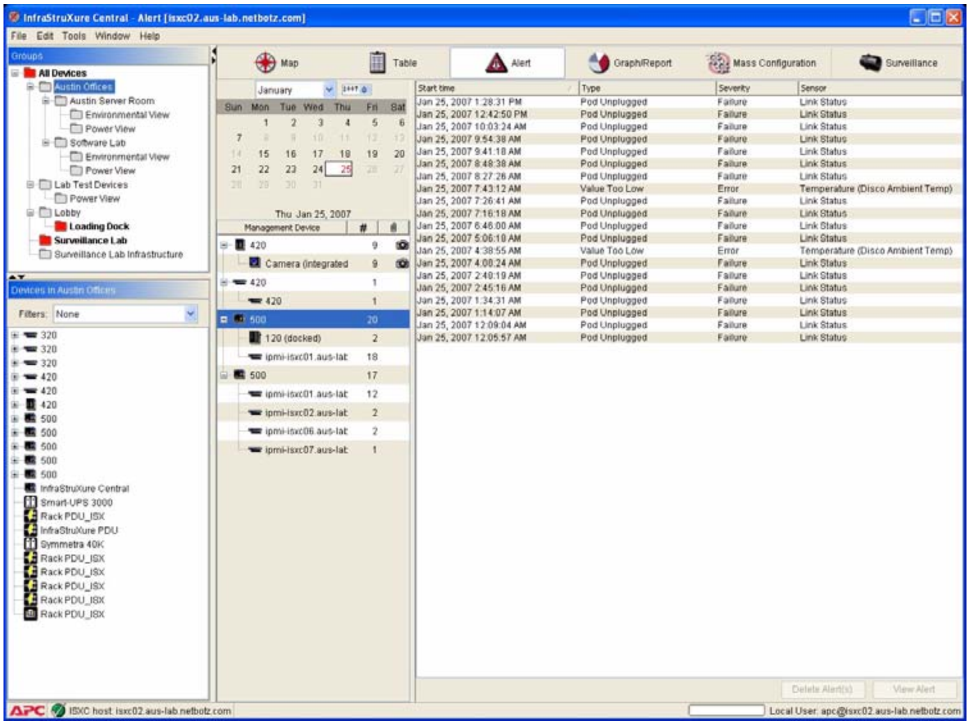
For more information on the Table view, see “Using the Table View” on page 255.

Alert View

The InfraStruXure Central Alert view enables you to easily view a summary of all alert events that were reported by any selected devices on a user-specified day. Any alert events that were active on the specified date as displayed, as are any alert events that were resolved on the selected date, regardless of when the alert event began. Alert events begin at the time a specified threshold is exceeded and end when the alerting sensor has returned to a “normal” state. Therefore, depending on the nature of the alert, an alert event can continue for more than one day.

Alerts that contain picture data can also be viewed, provided that the alert has been posted to the InfraStruXure Central server using the device HTTP Post support (see “Creating a Send HTTP Post Alert Action” on page 239 for more information) or the Send to InfraStruXure Central alert action.

If you select one or more devices from the Device Selection pane only the selected devices will be listed in the Alerts view. If a device is not selectable in the Alerts view (and is “grayed out”) then no alerts have been posted to or collected from the selected device on the selected date.


InfraStruXure Central - Alert [isxc02.aus-lab.netbotz.com]
File Edit Tools Window Help
Map
Table
Alert
Graph/Report
Mass Configuration
Surveillance
Delete Alert(s)
View Alert

Thu Jan 25, 2007

Management Device	#	
420	9	📷
Camera (integrated	9	📷
420	1	
420	1	
500	20	
120 (docked)	2	
ipmi-isxc01.aus-lat	18	
500	17	
ipmi-isxc01.aus-lat	12	
ipmi-isxc02.aus-lat	2	
ipmi-isxc06.aus-lat	2	
ipmi-isxc07.aus-lat	1	

Start time	Type	Severity	Sensor
Jan 25, 2007 1:28:31 PM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 12:42:50 PM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 10:03:24 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 9:54:38 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 9:41:18 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 8:48:38 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 8:27:26 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 7:43:12 AM	Value Too Low	Error	Temperature (Disco Ambient Temp)
Jan 25, 2007 7:26:41 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 7:16:18 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 6:46:00 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 5:06:10 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 4:38:55 AM	Value Too Low	Error	Temperature (Disco Ambient Temp)
Jan 25, 2007 4:08:24 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 2:49:19 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 2:45:16 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 1:34:31 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 1:14:07 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 12:09:04 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 12:05:57 AM	Pod Unplugged	Failure	Link Status

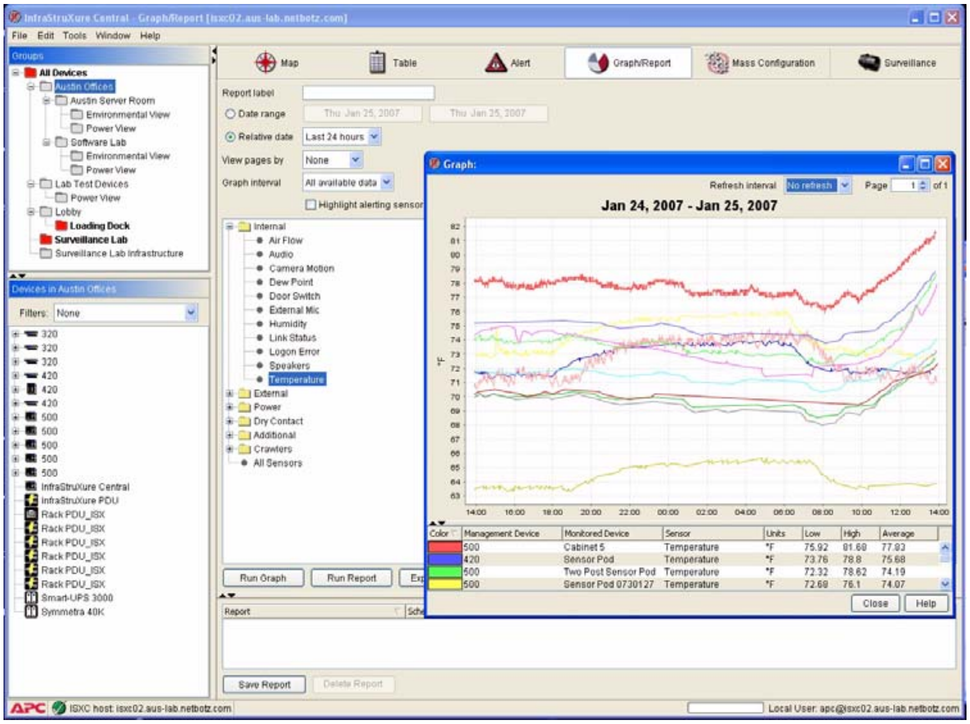
Note Only alerts that are generated by devices from which InfraStruXure Central collects data or that post their alert data to the InfraStruXure Central server using HTTP post support are available from the Alerts view. For more information of collecting data from your devices, see “Data Collection/Monitoring Settings” on page 75.

To see a summary of all alerts that were generated on a particular date, select that date using the calendar control in the Alerts view. Dates on which no alerts have been generated or for which there is no alert data are grayed out in the calendar.

For more information on the Alerts view, see “Using the Alert View” on page 257. For information on configuring your devices to generate alerts see “Mass Configuration: Sensor and Alert Settings” on page 113, “Alert Actions” on page 115, and “Alert Profile” on page 117. For information on configuring your devices to send HTTP Post data about alerts to your InfraStruXure Central server or an HTTP server see “Creating a Send HTTP Post Alert Action” on page 239 and “Creating a Send to InfraStruXure Central Alert Action” on page 225.

Graph/Report View

The InfraStruXure Central Graph/Report view enables you to generate reports, for a user-specified time period, from the data collected from the sensor data collected by one or more devices. The data can be plotted in a graph to simplify data collation and comparison, or it can be can be collated into a single report to simplify data collation, collection, and comparison. Report data (or from a selected portion of the report) can be exported to a server and saved for future reference. Report data can also be exported as a delimited value text file.



Report label

○ Date range Thu Jan 25, 2007 Thu Jan 25, 2007

● Relative date Last 24 hours

View pages by None

Graph interval All available data

□ Highlight alerting sensors

Filters: None

Refresh interval No refresh

Page 1 of 1

Color	Management Device	Monitored Device	Sensor	Units	Low	High	Average
🟥	500	Cabinet 5	Temperature	°F	75.92	81.68	77.83
🟦	420	Sensor Pod	Temperature	°F	73.76	78.8	75.68
🟩	500	Two Post Sensor Pod	Temperature	°F	72.32	78.62	74.19
🟨	500	Sensor Pod 0730127	Temperature	°F	72.68	76.1	74.07

To use the Graph/Report view:

1. Select a device group from the Group Navigation pane, or one or more devices from the device selection window, and then click the Graph/Report button.

2. If you would like to name this report so you can save it and re-run it later, type a name in the Report label field.

Note

You must provide a report label to save reports for use later.

3. Specify the time period for which the report will be run by selecting either the Date Range or Relative Date radio button.

   – If you select Date Range, and use the two calendar controls to specify the date range for the graph.

   – If you select Relative Date, select the time period prior to the present (Today, Last 24 Hours, Last Week, etc.) for which data will be collected.

4. Select from the View pages by drop box what portion of the total amount of data will be shown in

each page of the resulting report or graph.

5. Select from the Graph interval drop box the time interval for which data will be included in the resulting report or graph.
6. Select from the Sensor tree the sensors for which data will be included in the resulting report or graph and then click the right arrow button to add the sensors to the list on the right. To remove sensors from the list, select them and then click the left arrow button.
7. Check the Highlight alerting sensors check box to highlight the names of sensors that are reporting alerts in the graph or report. In a graph, the sensors that are reporting an error will be shown with a heavier line. In a report, the entries in the report that correspond to alert states will be highlighted.
8. Check the Only show alert and clear check box to include only the alert and alert cleared values for the selected sensors. This option is used only when generating a report and has no effect on graphs that are generated using the Graph view.
9. Click the button that corresponds to the graphing or reporting function you wish to perform.
   – Click Run Graph to generate a graph of the collected data.

   – Click Run Report to generate a report from the collected data.

   – Click Export Report to export and save the collected data as a delimited text file.

Each line that is shown in the graph corresponds to a single sensor on a single selected device. A table showing which line color corresponds to which device and sensor appears at the bottom of the Graph/ Report window.

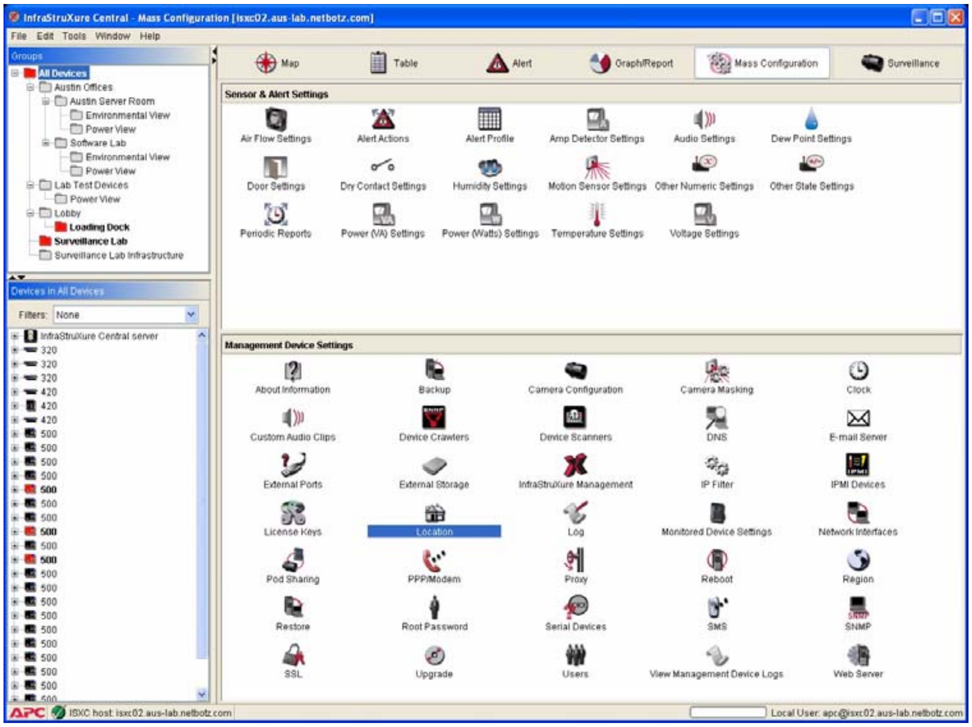
To select a portion of a graph and display only the selected data click and drag a box around the portion of the graph that you want to view. The data points from the selected area of the graph will then be re-graphed. To restore the full graph, right-click on the graph and select **Zoom Out**.

The graph can be saved as a graphic file (JPG or BMP format). To save the graph as a graphic file, right-click on the graph and select Save Graph.

For more information about the Graph/Report view, see “Using the Graph/Report View” on page 259.

Mass Configuration View

The InfraStruXure Central Mass Configuration view provides complete mass device configuration functionality, enabling you to perform all of the tasks necessary for complete management of all of your devices, one at a time or en masse. The Mass Configuration panel is divided into two areas: Sensors Settings and Device Settings. Each area features a number of icons that represent the mass configuration tasks that you can perform.



To perform a mass configuration task, first select a device group from the Device Group Navigation pane and then double-click on the appropriate mass configuration icon. For detailed information about the various mass configuration tasks that can be performed, see “Mass Configuration: Sensor and Alert Settings” on page 113 and “Mass Configuration: Device Settings” on page 159.

About Deleting Devices

Depending on your device group configuration, it is possible for individual devices to appear in multiple device groups. For example, if you have both an All Devices device group and a second device group that includes only rack-model devices, all of your rack-model devices will be included in both the rack-model devices group and the All Devices device group. Though devices can be included in multiple device groups, the data for each device is stored in the InfraStruXure Central database only once.

Deleting a device also purges all data associated with the device from the InfraStruXure Central database. As a result, when you delete a device from a device group the device is also deleted from any other device groups in which it exists, including other device groups to which the user may not have access.

For more information, see “User/Group Administration” on page 106.

Using Filters

You can use filters to quickly and easily limit the devices that are displayed in the Device Selection pane. Because the contents of the Device Selection pane determine what devices are displayed in the various Action/Information pane views (i.e. the Map, Table, Alert, Graph/Report, Mass Configuration, and Surveillance Views), by filtering the contents of the Device Selection pane you also filter the contents of all of the other panes as well.

By default, the contents of the Device Selection groups are unfiltered. This means that when a Device Group is selected from the Group Selection pane, the Device Selection pane will include the following devices if they are present in the selected groups:

- Management devices with docked pods
- Management devices without docked pods
- Other physical devices that are connected to the management devices via a USB port (such as Sensor Pod 120s, Camera Pod 120s, CCTV Adapter Pods, and 4-20 mAmp Sensor Pods)
- Other devices that are connected to the management devices via your network (such as SNMP-based devices that have been configured for use with the Device Crawlers or Device Scanners tasks, or IPMI-based devices that have been configured for user with the IPMI Devices task)

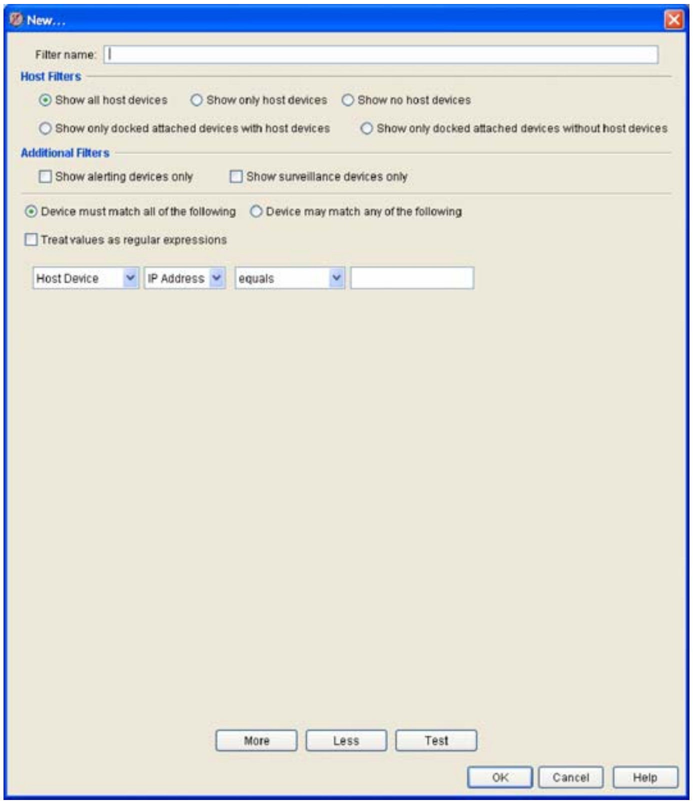
You can use filters to easily limit which of these devices are displayed, enabling you to more easily manage your devices.

Creating or Editing Filters

To create or edit a filter:

1. Right-click in either the Device Selection pane or the Action/Information pane and select Filters....
2. The Filters... window opens. To create a new filter, click Add. To edit a previously created filter,

select the desired filter and then click Edit.


New...
Filter name:
Host Filters
● Show all host devices
○ Show only host devices
○ Show no host devices
○ Show only docked attached devices with host devices
○ Show only docked attached devices without host devices
Additional Filters
□ Show alerting devices only
□ Show surveillance devices only
● Device must match all of the following
○ Device may match any of the following
□ Treat values as regular expressions
Host Device
IP Address
equals
More
Less
Test
OK
Cancel
Help

3. The Add or Edit Filter window opens. This window contains the following controls:

Field	Description
Filter name	The name that you will use to describe this filter.

Field	Description
Management device display filters	These controls determine how management devices will be displayed in the filtered results.You can select from the following options: • Show all management devices: All management devices will be included in the filtered results. Docked pods, undocked pods, and devices connected to management devices via USB or network connections are shown. • Show no management devices: Management devices are filtered from the results. Docked pods, undocked pods, and devices connected to management devices via USB or network connections are shown. • Show only docked pods with management devices: Only management devices to which a Sensor Pod 120, Camera Pod 120, or CCTV Adapter Pod has been docked will be shown in the filtered results. Undocked pods, devices connected to management devices via USB or network connections, and management devices to which pods have not been docked are automatically filtered from the results. • Show only docked pods without management devices: Only the pods that are docked with management devices are show. The management devices to which the pods are docked, undocked pods, devices connected to management devices via USB or network connections, and management devices to which pods have not been docked are automatically filtered from the results.
Show only alerting devices	Any devices that are not currently reporting an alert state are filtered from the results.
Show Surveillance	Shows only devices that have been licensed for use with Surveillance.
Additional Filters controls	Click More to add another set of filter controls to the window. Use these controls to add additional filters that will further limit the devices that are included in the filtered results.

4. Select a Management device display filter.
5. If desired, check the Show alerting devices and/or Show Surveillance check boxes.
6. If desired, use the Additional Filters controls to further refine the results. Additional filters enable you to limit your filtered results to specific management devices or monitored devices that fit user-specified criteria. To define an additional filter:
   a. Select the Device must match all of the following or Device may match any the following radio button.
      - If you select Device must match all of the following and you define 2 or more Additional Filters, only devices that meet the conditions specified in all of the Additional Filters will be included in the results.
      - If you select Device may match any of the following and you define 2 or more Additional Filters, only devices that meet the conditions specified in 1 or more of the Additional Filters will be included in the results.

  b. Check the Treat values as regular expressions check box to enable greater control of wildcard value definitions in the additional filter controls.
  c. Define the filter.
     i. First select the type of device to which the filter applies (Management Device or Monitored Device).
     ii. Select the value that will be used to determine whether the device is included in the filtered results. You can choose to filter devices based on IP address, Hostname, Type, Model, Location or Other. If you select Other you must also provide the name of the qualifying value.
     iii. Specify whether the device will be included in the filtered results if the value equals, does not equal, contains, or does not contain the discerning value information that is contained in the last field.
     iv. Either select from or type in the last field the discerning value that will be used to determine whether or not devices are filtered from the results.
  d. To add another Additional Filter definition, click More. To remove the last Additional Filter definition from the list, click Less. To test the results of the current filter definitions click Test.

7. When you've finished defining your filter, click OK to save the filter. Click Cancel to close this window without saving the filter definition.

Once you've defined a filter, it appears in the Filter drop box, located at the top of the Device Selection pane. To filter your Device Selection pane contents, select the desired filter from the Filter drop box.

InfraStruXure Central Client Preferences

Client preferences are configured using the Client Preferences interface, available using the **Edit>Preferences** menu selection. Use the Client Preferences interface to configure the following client settings:

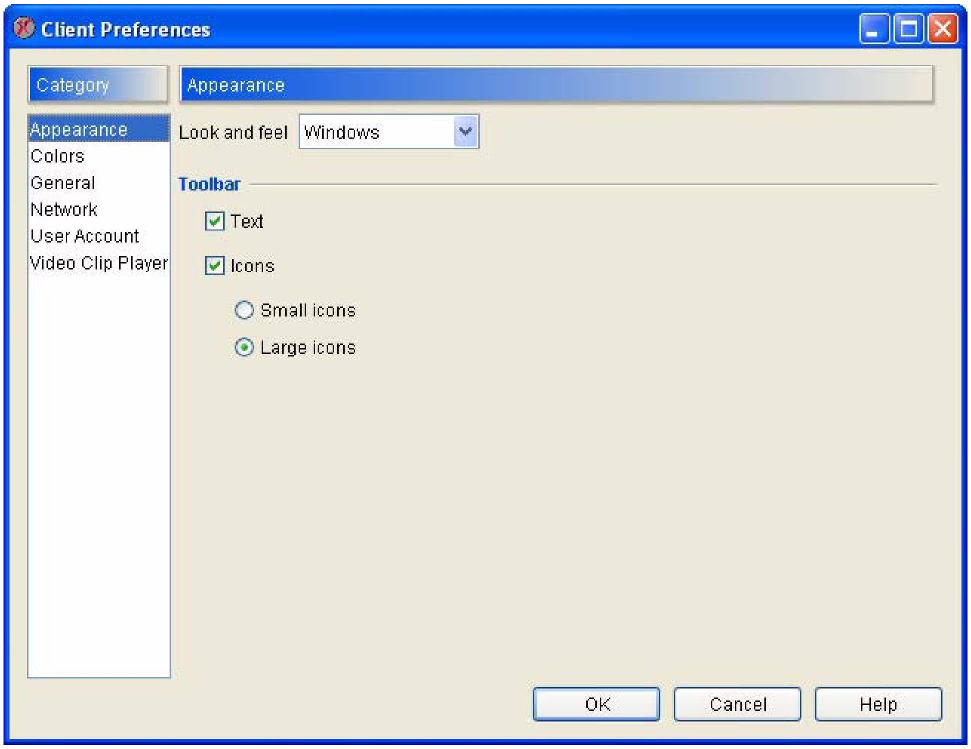
- Appearance
- Colors
- General
- Network
- User Account
- Video Clip Player

Note that these settings apply only to the currently logged in user account, and will not affect other user accounts or any global InfraStruXure Central settings.

Configuring Client Appearance Preferences

Enables you to change the appearance of your InfraStruXure Central console. Use the controls to specify the following client preferences:

- Look and Feel: Controls the basic appearance of the interface and the interface controls (buttons, menus, drop boxes, etc.). You can choose CDE/Motif, Kunststoff, Metal, Windows, or Windows Classic.
- Toolbar: Controls the appearance of items in the InfraStruXure Central toolbar. You can choose to use text, icons, or both to identify toolbar selections. If using icons, you can choose to use small or large icons.



Look and feel: Windows

Toolbar

☑ Text

☑ Icons

○ Small icons

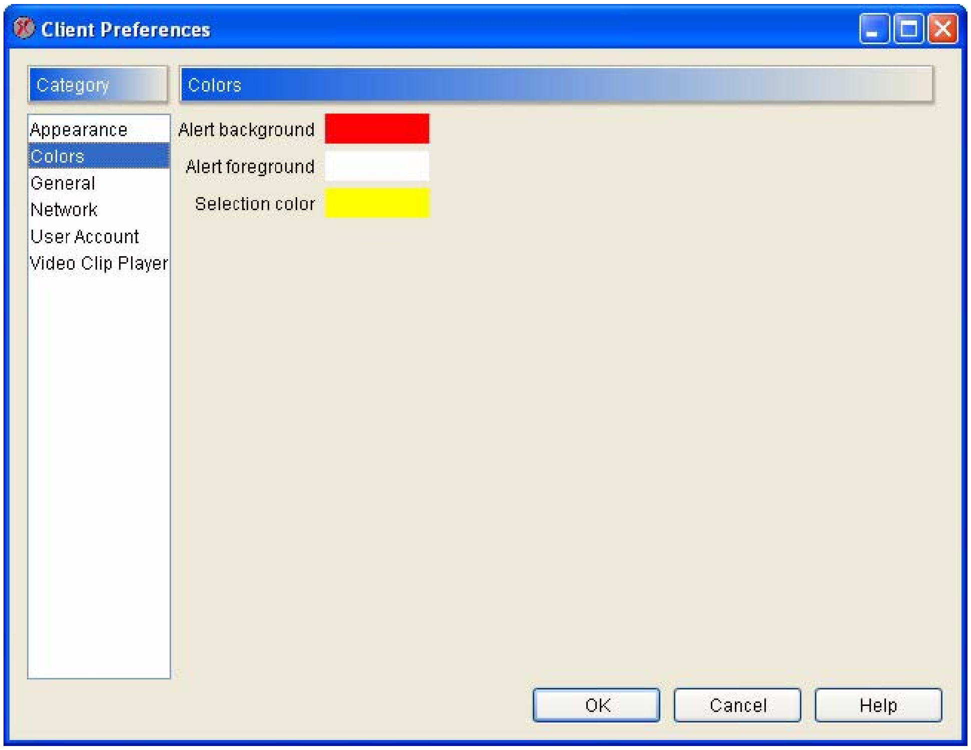
● Large icons

When you're finished configuring your client appearance, click **OK** to save your settings.

Configuring Color Preferences

Enables you to configure the colors that will be used to indicate alert states on devices in the Map and Table view. Use the controls to specify the following client preferences:

- Alert Background and Alert Foreground: Set the background and foreground colors that are used, in the Map and Table views, to indicate that a device has reported an alert from one of its sensors. The manner in which the selected colors are used depends on the view in question:
  - In the Map view, the Display Name for the device will be shown using the Alert Foreground for the text of the Display Name and the Alert Background color for the background behind the Display Name.
  - In the Table view, the table cell that corresponds to the device that reported the alert and the sensor that the alert pertains to will be displayed using the Alert Foreground for the cell text and the Alert Background color for the cell background.



Client Preferences

Category: Appearance, Colors, General, Network, User Account, Video Clip Player

Colors

Alert background 🟥

Alert foreground ⬜

Selection color 🟨

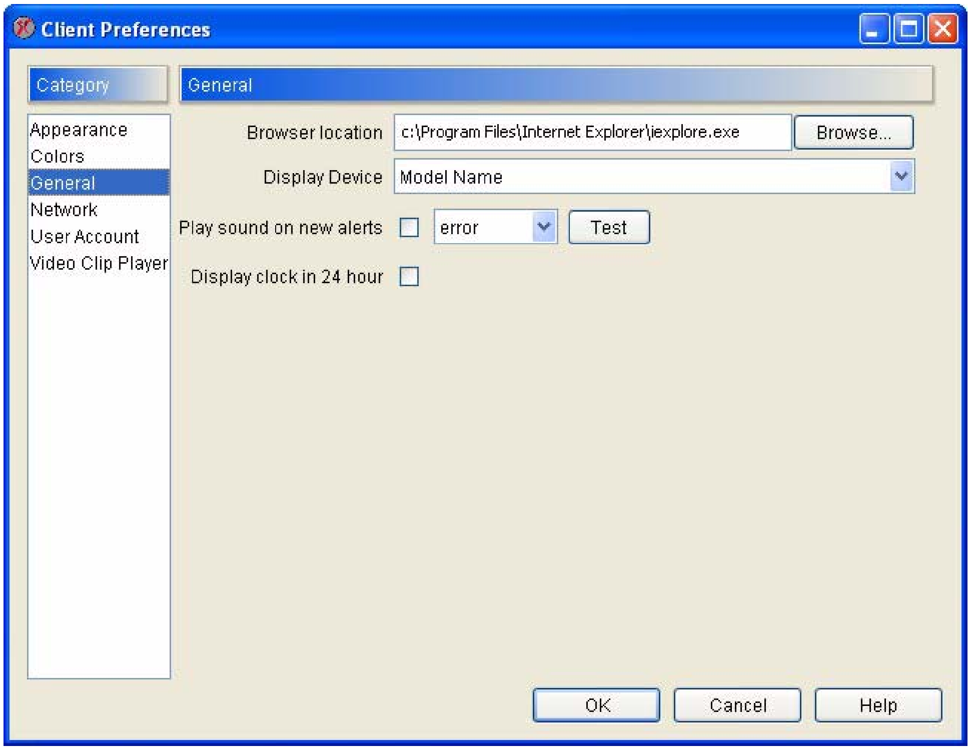
- Selection Color: Sets the color used to indicate selected devices or areas in the interfaces and, in the Surveillance view (if the Surveillance add-on application has been installed and licensed for use), as a frame around any surveillance images in which motion has been detected.

Click **OK** to save your settings.

Configuring General Client Preferences

Enables you to specify a variety of general console settings. Use the controls to specify the following client preferences:

- To specify the location in which your system's web browser is installed, type in the **Browser location** field (or use click **Browse** and navigate to) the drive, directory, and executable name of your web browser.
- To specify whether devices will be identified in the InfraStruXure Central interfaces using their host name, IP address, location value, or MAC address select Host name, IP address, Location, or MAC address from the **Display device** selection list.



Browser location: c:\Program Files\Internet Explorer\iexplore.exe

Display Device: Model Name

Play sound on new alerts □ error

Display clock in 24 hour □

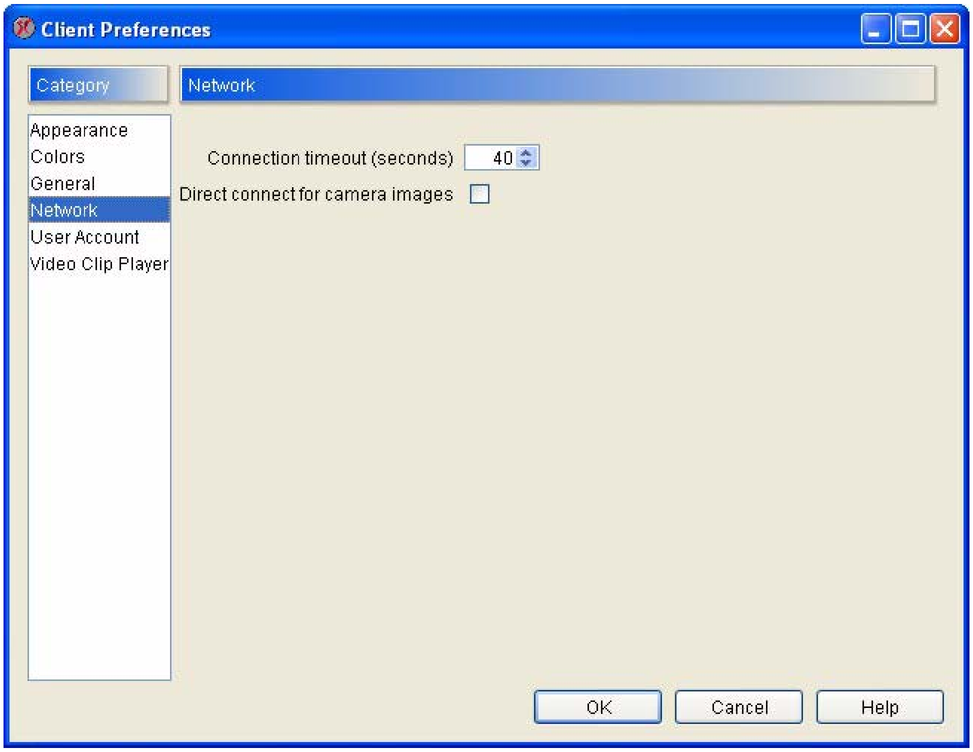
- To configure the InfraStruXure Central console to play a sound when alerts are detected, check the **Play sound on new alerts** check box.
- To display time in the console using a 24 hour clock style, check the **Display clock in 24 hour** check box.

Click **OK** to save your settings.

Configuring Client Network Preferences

Enables you to set the client network timeout setting and to enable or disable direct connection to managed devices gathering camera images. Note that Direct connection for camera images must be checked to enable Two-Way Audio functionality (see "Two-Way Audio Functionality" on page 274).

Type in the Connection timeout field the amount of time that the InfraStruXure Central console should wait when attempting to connect to the InfraStruXure Central server before giving up, and check the Direct connect for camera images check box if desired.



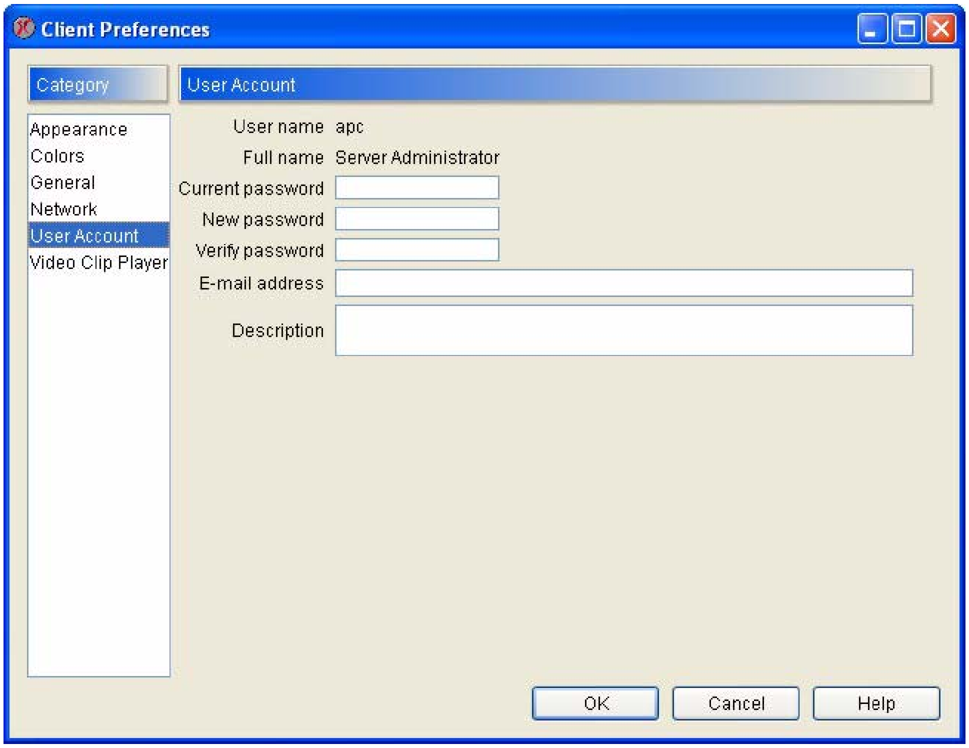
Connection timeout (seconds) 40

Direct connect for camera images □

Click **OK** to save your settings.

Configuring User Account Preferences

Enables you to specify the password, e-mail address, and description that will be used for the InfraStruXure Central server's administrator account. The user name for this account is always “apc.” The default password is “apc” as well.



User name apc

Full name Server Administrator

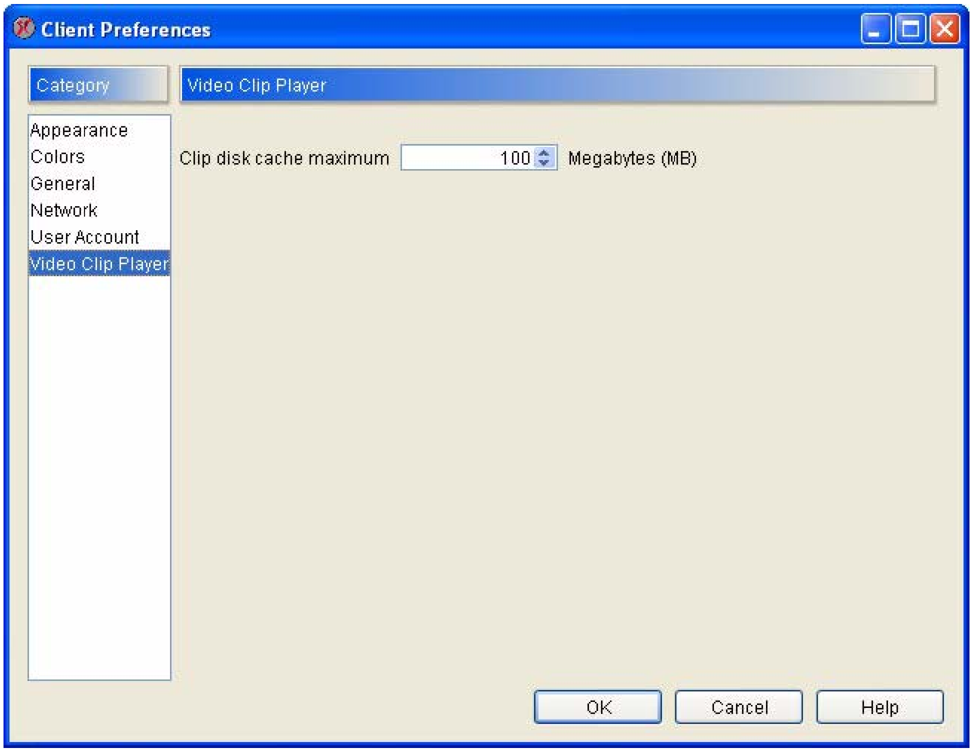
To change the password:

1. Type in the **Current password** field the password that is currently assigned to the administrator account.
2. Type in the **New password** field the new password that will be used for the administrator account.
3. Type the new password again in the **Verify password** field.
4. Click **OK** to save the new password.

Be sure to type in the E-mail address field an administrator e-mail address: Important system e-mail notifications will be automatically sent to this address when necessary.

Configuring Video Clip Player Preferences

Enables you to specify how many MB of disk space should be reserved for use with the built-in video clip player.



Clip disk cache maximum 100 Megabytes (MB)

Click **OK** to save your settings.

InfraStruXure Central Tools Menu

The selections available from the Tools menu enable you to view InfraStruXure Central server messages, configure settings on the InfraStruXure Central server, configure user accounts, configure network settings, and perform maintenance tasks on the server. Individual tasks are divided into one of the following submenus: Messages, Server Administration, Server Control, and Server Messages.

Messages

Select Messages from the Tools pull-down menu to view information generated by the InfraStruXure Central console application. These messages are generated primarily for logging and debugging purposes, and may be useful if you should need to contact support.

Server Administration

Use the selections available from the Server Administration submenu to configure settings on the InfraStruXure Central server, configure user accounts, and perform maintenance tasks on the server. The following tasks are available from this submenu:

- Backup/Restore Administration
- Data Collection/Monitoring Settings
- Device Group Administration
- Discovery Settings
- Disk Array Management
- Export Administration
- Management Device Job Control
- Management Device Security Settings
- Management Device Timeout Settings
- Install/Upgrade Management
- License Keys
- Server Settings
- Storage Repositories
- Surveillance Administration
- User/Group Administration

For complete information on Server Administration tasks see “Server Administration Tasks” on page 71.

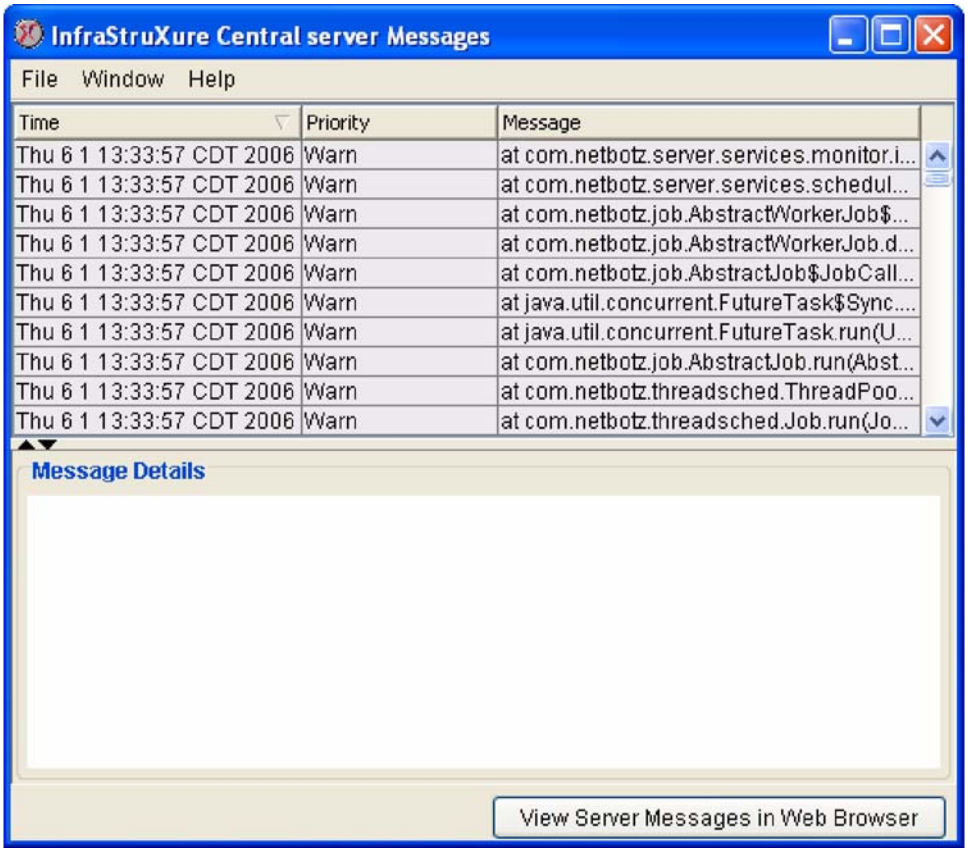
Server Control

Use the selections available from the Server Control submenu to restart the InfraStruXure Central application and device, or to shutdown and power off the device. You can choose from the following three selections:

- Restart InfraStruXure Central Software: Shuts down and restart the InfraStruXure Central application on the InfraStruXure Central server.
- Restart InfraStruXure Central Hardware: Shuts down the InfraStruXure Central application, cycles the power on the device, and restarts the InfraStruXure Central application.
- Shutdown/Power-Off InfraStruXure Central Hardware: Shuts down the InfraStruXure Central application, then shuts down the device as well.

Server Messages

Select Server Messages from the Tools pull-down menu to view log file entries generated by the InfraStruXure Central server. These logs contain information about all of the processes the InfraStruXure Central server performs, such as device discovery, sensor data monitoring and collection, and user administration. These messages are generated primarily for logging and debugging purposes, and may be useful if you should need to contact support.


InfraStruXure Central server Messages
File
Window
Help
Message Details
View Server Messages in Web Browser

Time	Priority	Message
Thu 6 1 13:33:57 CDT 2006	Warn	at com.netbotz.server.services.monitor.i...
Thu 6 1 13:33:57 CDT 2006	Warn	at com.netbotz.server.services.schedul...
Thu 6 1 13:33:57 CDT 2006	Warn	at com.netbotz.job.AbstractWorkerJob$...
Thu 6 1 13:33:57 CDT 2006	Warn	at com.netbotz.job.AbstractWorkerJob.d...
Thu 6 1 13:33:57 CDT 2006	Warn	at com.netbotz.job.AbstractJob$JobCall...
Thu 6 1 13:33:57 CDT 2006	Warn	at java.util.concurrent.FutureTask$Sync....
Thu 6 1 13:33:57 CDT 2006	Warn	at java.util.concurrent.FutureTask.run(U...
Thu 6 1 13:33:57 CDT 2006	Warn	at com.netbotz.job.AbstractJob.run(Abst...
Thu 6 1 13:33:57 CDT 2006	Warn	at com.netbotz.threadsched.ThreadPoo...
Thu 6 1 13:33:57 CDT 2006	Warn	at com.netbotz.threadsched.Job.run(Jo...

The messages that are displayed in the InfraStruXure Central Server Messages window correspond to the contents of nbc.xml, the primary InfraStruXure Central log file. Only the 150 most recent entries are displayed in this window, and no messages with a DEBUG priority are displayed, regardless of the Server Administration Log Level setting (configured using the Log Management task. For more information, see “Log Settings” on page 97). However, complete nbc.xml contents, as well as additional package and process-specific log files, can be accessed by clicking View Server Messages in Web Browser.

When you click View Server Messages in Web Browser you are prompted to log in using your InfraStruXure Central account User ID and Password. Once logged in, click on the log that you wish to view.

Note

Aside from the nbc.xml log, the log files are primarily for use by APC support staff.

Server Administration Tasks

Use the selections available from the Server Administration submenu to configure settings on the InfraStruXure Central server, configure user accounts, and perform maintenance tasks on the server. The following tasks are available from this submenu:

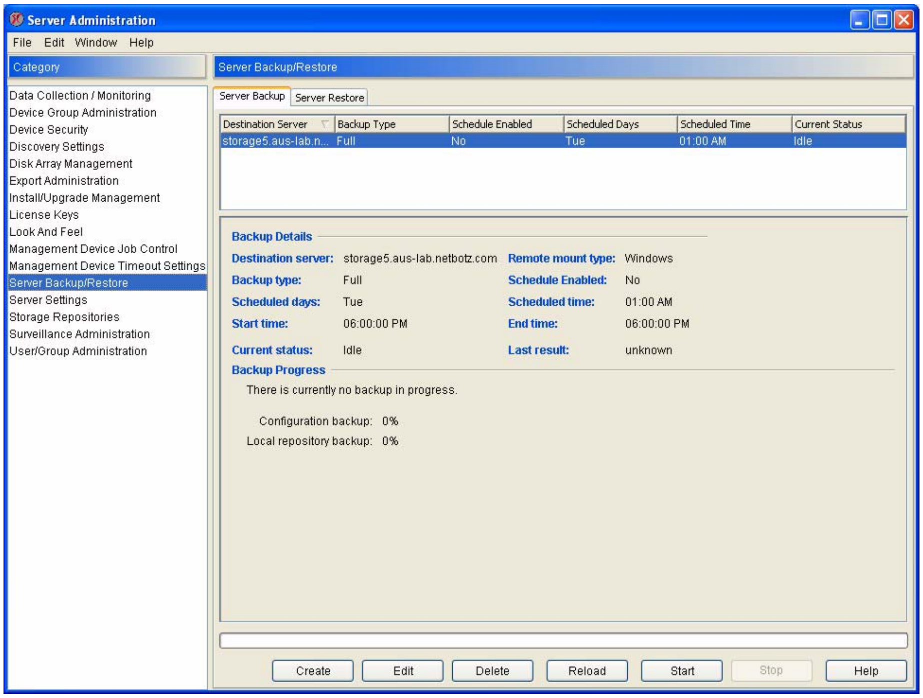
- Backup/Restore Administration
- Data Collection/Monitoring Settings
- Device Group Administration
- Discovery Settings
- Disk Array Management
- Export Administration
- Install/Upgrade Management
- License Keys
- Management Device Job Control
- Management Device Security Settings
- Management Device Timeout Settings
- Server Settings
- Storage Repositories
- Surveillance Administration
- User/Group Administration

Backup/Restore Administration

Use the Backup/Restore task to save a copy of your InfraStruXure Central server configuration and data to a remote network-attached storage system or to restore your InfraStruXure Central configuration and data using a previously saved configuration backup file stored on a remote network-attached storage system. The Backup/Restore window consists of 2 panes: The Server Backup pane, which is used to backup the server configuration and data; and the Server Restore pane, which is used to restore the server's configuration and data using previously created backup files.

Server Backup

The Server Backup pane contains a list of previously created backups entries. For detailed information about each of the previously created backup entries, select the backup entry file form the Backups selection list and then refer to the Backup Information data beneath the selection list.



Destination Server	Backup Type	Schedule Enabled	Scheduled Days	Scheduled Time	Current Status
storage5.aus-lab.n...	Full	No	Tue	01:00 AM	Idle

Backup Details

Destination server:	storage5.aus-lab.netbotz.com	**Remote mount type:**	Windows
Backup type:	Full	**Schedule Enabled:**	No
Scheduled days:	Tue	**Scheduled time:**	01:00 AM
Start time:	06:00:00 PM	**End time:**	06:00:00 PM
Current status:	Idle	**Last result:**	unknown

Backup Progress

There is currently no backup in progress.

Configuration backup: 0%
Local repository backup: 0%

To create a new Backup entry, or to edit a previously created Backup entry:

1. Select the Server Backup pane and then click Create to add a new Backup entry. To edit a previously created entry, select the desired Backup entry from the selection list and then click Edit.
2. The Create/Edit Backup Entry window opens. This window contains the following fields:

Field	Description
Backup type	Select the type of backup that will be performed. You can select: • Full backup: Creates a new backup file containing a complete backup of all server data every time • Synchronization: Performs a backup of all data the first time it is run, and then backs up only new or changed data on all subsequent backups • Configuration: Creates a backup file that contains all server configuration data (device names and addresses, device groups, user accounts, and so forth) but which does not include the data repository
Remote mount type	Select the type of file system used by the remote network-attached storage system. You can choose either NFS or Windows. Note that the mount type you select alters the contents of this window.
Server hostname or IP	Type in this field the hostname or IP address used by the remote system.

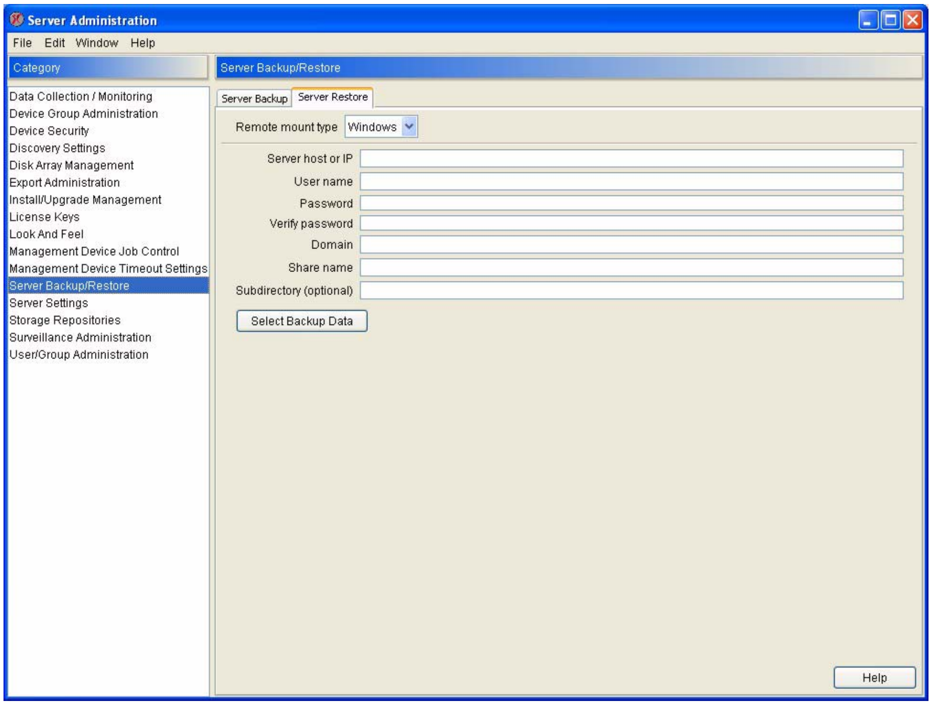
Field	Description
User name — Windows systems only	Type in this field the user name that will be used to access the remote system.
Password/Verify password — Windows systems only	Type in these fields the password that will be used to access the remote system.
Domain — Windows systems only	Type in this field the name of the domain on which the remote system that will be used to store the backup file resides.
Share name — Windows systems only	Type in this field the name of the share on the remote system on which the backup file will be stored.
Share path — NFS mounts only	The share path of the NFS mount.
Subdirectory (optional)	If desired, enter the name of a subdirectory on the share in which the backup file will be stored.
Test Mount	After specifying a remote file system, host, drive, and directory, click Test Mount to ensure that InfraStruXure Central can access the remote system.
Day/Time controls	If desired, use these controls to specify days and times at which backups will occur automatically.
Enable schedule	Check this check box to enable the Backup job to run according to your specified schedule settings.

3. When you've finished specifying the needed information, click OK to save your backup entry and return to the Server Backup pane.

To backup your server immediately, select a Backup entry and then click Start. To halt a backup that is currently in progress, select the entry that corresponds to the Backup and then click Stop.

Server Restore

Use the Server Restore pane to restore your InfraStruXure Central configuration and data using a previously created InfraStruXure Central backup file stored on a remote network-attached storage system.



Remote mount type: Windows

To restore your InfraStruXure Central server:

1. Select the Server Restore pane. This pane contains the following fields:

Field	Description
Remote mount type	Select the type of file system used by the remote network-attached storage system. You can choose either NFS or Windows. Note that the mount type you select alters the contents of this window.
Serve hostname or IP address	Type in this field the hostname used by the remote system.
User name — Windows systems only	Type in this field the user name that will be used to access the remote system.
Password/Verify password — Windows systems only	Type in these fields the password that will be used to access the remote system.
Domain — Windows systems only	Type in this field the name of the domain on which the remote system that contains the database backup file resides.
Share name — Windows systems only	Type in this field the name of the share on the remote system on which the backup file is stored.
Share path — NFS mounts only	The share path of the NFS mount.
Subdirectory (optional)	If necessary, enter the name of a subdirectory on the share in which the backup file will be stored.

2. Fill in the necessary fields, and then click Select Backup Data to specify what portion of the InfraStruXure Central data stored in the backup file you wish to restore to your server.

Note

Any users that are logged into InfraStruXure Central will be automatically logged out during the Database Restore process and will be unable to log back in until the Database Restore process is completed.

Data Collection/Monitoring Settings

Use the Data Collection/Monitoring task to:

- View, modify, add, or delete data collection settings for your InfraStruXure Central device groups. InfraStruXure Central uses the Data Collection settings to determine at what time intervals it should gather data from all devices that are included in specific device groups.
- Specify the device monitoring settings. Device monitoring determine how often InfraStruXure Central checks to ensure that the device is responding and available

This task consists of two panes: The Data Collection Settings pane and the Monitor Settings pane.

The Data Collection Settings Pane

Use the Data Collection pane to view, modify, add, or delete data collection settings for your InfraStruXure Central device groups. The InfraStruXure Central server uses the Data Collection settings to determine at what time intervals it should gather data from all devices that are included in specific device groups. Each InfraStruXure Central device groups can have its own Data Collection settings and schedule.

Avoiding Redundant Data Collection

All data collection is performed on a device group-by-device group basis. Therefore, devices that appear in multiple device groups could have data collected from them at multiple times, depending on the Data Collection settings for each device group to which they belong. For example, if you create a device group that includes all rack model devices in your network, and you configure Data Collection settings for both your rack model device group and for your default All Devices device group, data will be gathered from all of your rack model devices twice, periodically. While this does not increase the size of your InfraStruXure Central database, it will increase network traffic.

When you select the Data Collection pane a table is displayed that contains all currently defined data collection settings. The table contains the following information about each device group for which you have defined data collection settings:

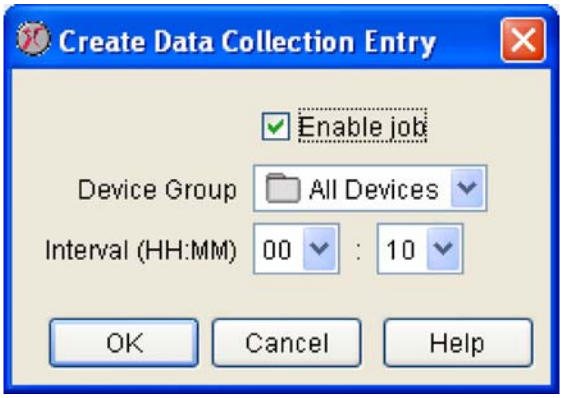
Field	Description
Device Group	The name of the device group to which these data collection settings apply.
Interval (HH:MM)	The amount of time, in hours:minutes, that must pass after a data collection process has completed before InfraStruXure Central will initiate another data collection process.
Enabled	The current state of data collection for this device group. If data collection is not enabled, the data collection settings are saved but no data is collected from the device group.

Note

If you have not defined any data collection settings for any of your device groups then no table will be displayed.

To edit previously defined data collection settings, or to configure new data collection settings for your device groups:

1. Click Create (or, select a previously defined data collection setting from the Data Collection table and then click Edit).



Create Data Collection Entry

☑ Enable job

Device Group: All Devices

Interval (HH:MM): 00 : 10

2. The Create Collection window opens (or, if you are editing a previously defined data collection

settings, the Edit Collection window opens). This window contains the following controls:

Field	Description
Device Group	Select from this drop box the name of the device group to which these data collection settings will apply. If you are editing a previously defined data collection setting the name of the device group to which the settings apply will appear in this field.
Interval (HH:MM)	Use the drop boxes to specify the number of hours and minutes that must pass between data collection operations.
Enabled	Check this check box to enable data collection of this device group. If this check box is not checked, the data collection settings will be saved but data collection will not be performed.

3. Use the controls to set the data collection settings.
4. When you are finished, click OK to save this data collection setting.
5. To begin collecting data from a device group immediately, select a device group and then click Start. To abort a currently occurring data collection process, select the device group from which data is being collected and then click Stop. To delete data collection settings for a device group, select the device group and then click Delete.

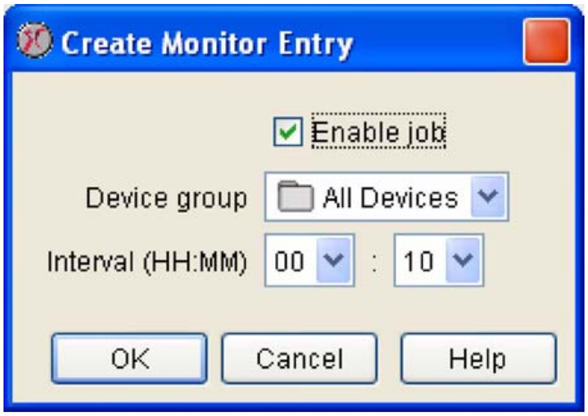
The Monitor Settings Pane

Use the Monitor Settings pane to specify the device monitoring settings. Once a device is discovered or added to InfraStruXure Central, the server periodically checks the device to ensure that it is responding and available. If the device is not available, InfraStruXure Central will change its state to Offline in the Map and Table views, and will gray the device out in the Group Navigation pane.

When you select the Monitor Settings pane a table is displayed that contains all currently defined device monitoring configurations. By default, the All Devices group is configured with default monitoring settings. However, you can modify the default values, or you can create additional device monitoring configurations that are group-specific.

To edit previously defined monitoring configurations, or to configure new monitoring settings:

1. Click Create (or, select a previously defined configuration from the table and then click Edit).



☑ Enable job

Device group: All Devices

Interval (HH:MM): 00 : 10

2. The Create Device Monitor Entry window opens (or, if you are editing a previously defined device

group, the Edit Device Monitor Entry window opens). This window contains the following controls:

Field	Description
Device Group	Select from this drop box the name of the device group to which these device monitoring settings will apply. If you are editing a previously defined device monitoring configuration the name of the device group to which the settings apply will appear in this field.
Interval	Use the drop boxes to specify the number of hours and minutes that must pass between device monitoring operations.
Enabled	Check this check box to enable data collection of this device group. If this check box is not checked, the data collection settings will be saved but data collection will not be performed.

3. Use the controls to set the settings.
4. When you are finished, click Apply to save this configuration.

Device Group Administration

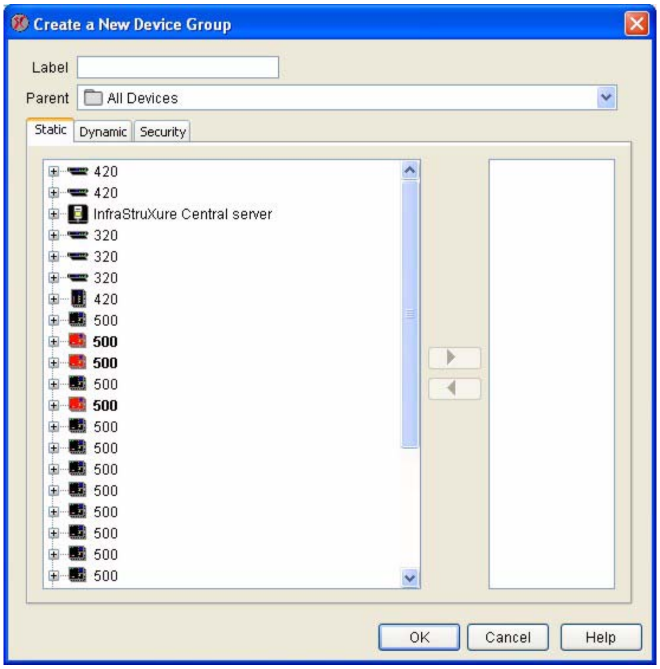
Use the Device Group Administration task to add, delete, or modify device groups. Device group definitions enable you to more easily manage devices by sorting them automatically into smaller device groups. Device groups also enable you to set security policies for your device groups by specifying what local user accounts or local user groups can access the device and group and usage privileges they have while doing so.

The contents of your device groups can also be dynamic or static. Static device groups do not change, even if new devices are discovered on the network which conform to the device groups settings, while dynamic device groups are automatically updated to include newly discovered devices that fit the device groups settings.

When you start the Device Group Administration task all currently defined device groups are displayed in a tree view. If you have not defined new device groups the only device group shown will be the All Devices group, which contains all devices that have been discovered on your network. To view the settings of a previously created device group select it from the tree view.

To edit previously defined device groups, or to configure new device group:

1. Click Create (or, select a previously defined device group from the tree view and then click Edit).



Create a New Device Group

Label:

Parent: All Devices

2. Type in the Label field a name for this device group.
3. Select from the Parent drop box the previously created device group that will be the parent of the new device group. Note that nested device groups inherit the security privileges of their parents.
4. Select the Static or the Dynamic tab (select Static if you want the devices contained within the device group to remain unchanged even if new devices are discovered on the network which conform to the device groups settings; select Dynamic if you want the contents of the device group to be automatically updated to include newly discovered devices that fit the device groups settings).
   – If you selected Static, use the controls to select the devices that will be included in the device group from the list of available devices. All management devices are displayed in the list, with any managed devices (such as Camera Pods, Sensor Pods, or SNMP devices) that are associated with each management device nested beneath the management device with which they are associated. Use the arrow controls to move devices between the Available Devices selection list and the Selected Devices selection list. Only devices that are located in the Selected Devices list will be included in the resulting device group.

     Note

     If you add a management device to the Selected Devices list all managed devices associated with that management device (such as Camera Pods, Sensor Pods, or SNMP devices) are added to the Selected List as well. However, once you add a management device to the Selected Device list you cannot remove any managed devices associated with it without removing the management device itself. This will remove all other managed devices associated with that management device. To add some -- but not all -- managed devices that are associated with a management device, expand the management device's tree, select one of more managed devices, and then add them to the Selected Devices list.

   – If you selected Dynamic, use the controls at the bottom of the window to build rules for this device group. Use the first drop box to specify what type of value (IP Address, Model, Type, Location, Host Name) will be used to determine if an appliance belongs in the defined device group. Use the second drop box to define whether the selected value must equal or must not equal a selected or user-specified value for the appliance to be included in the device group. Finally, use the last control (an entry field or a drop box, depending on what value type you selected) to specify the value that InfraStruXure Central will check on the appliance to determine whether or not the appliance belongs in the device group. If you have more than one rule an AND/OR selection list appears before each rule after the first, enabling you to build more complex rules-based device groups.

5. Select the Security tab. This pane displays a list of all local user accounts and local user groups that currently are permitted to access this device group, and also displays the Device privilege and Surveillance privilege settings for each local user account or local user group.

   Note that any local user accounts or local user groups that were permitted access to the parent of the selected device group (if any) are automatically added to the list of authorized users for this device group. Local users and local user groups automatically inherit all privileges that were granted in the parent group, and can be configured to allow additional privileges if desired. However, local users and local user groups that are inherited by child device groups cannot be configured to have fewer privileges than they had in the parent group.

6. To enable additional local user and local user group access, click Add User or Add User Group. To edit a previously configured local user or local user group entry, select the entry and click Edit Entry. To delete a previously configured local user or local user group entry, select the entry and click Remove Entry.

7. If you are adding or editing a local user or local user group, specify the Device privilege and Surveillance privilege settings for the local user or local user group. There are four device privilege levels and four surveillance privilege levels.

   The available device privilege levels are:

   – No access: The local user account or local user group are not permitted to access devices in this group.

   – View access: The local user account or local user group are permitted to view data generated by the devices in this group, but cannot configure, access, or trigger output control actions on the devices.

   – View & Control access: The local user account or local user group are permitted to view data generated by the devices in this group and can also trigger output control actions that have been defined for the devices, but cannot otherwise configure or access the devices.

   – Administrator access: The local user account or local user group are permitted to view data generated by the devices in this group, and also have complete access to all management and configuration tasks on the devices.

   The available Surveillance privilege levels are:

   – No access: The local user account or local user group are not permitted to access Surveillance data in this group.

   – View access: The local user account or local user group are permitted to view Surveillance data generated by the devices in this group, but cannot tag clips and cannot access the Surveillance Administration task or other surveillance-related tasks.

   – View & Tag access: The local user account or local user group are permitted to view Surveillance data generated by the devices in this group and can also tag resulting surveillance clips, but cannot access the Surveillance Administration task or other surveillance-related tasks.

- Administrator access: The local user account or local user group are permitted to view Surveillance data generated by the devices in this group, and also have complete access to all Surveillance configuration tasks on the devices.

> **Note**
>
> The Device and Surveillance privilege levels specify the default access privileges for local users or local user groups that can access this device group. However, the InfraStruXure Central administrator check box (available when using User/Group Administration to create or edit a local user account) and the Group members are InfraStruXure Central administrators check box (available when using User/Group Administration to create or edit a user group) override any device group-specific privileges you set using the Device Group Administration.

8. Select one of more local user accounts or local user groups and then click OK to enable them to access this device group.

9. Click Apply to save these settings.

Discovery Settings

Use the Discovery Settings task to configure the InfraStruXure Central automatic device discovery settings. InfraStruXure Central can automatically search a user-specified IP address range on your network for management devices or supported SNMP devices. If new devices are discovered, InfraStruXure Central will add them to the appropriate device groups automatically.

When you start the Discovery Settings task a table is displayed that contains all currently defined discovery settings. The table contains information about each device group for which you have defined discovery settings, including the IP range that will be searched, the type of devices that are searched, and the days and time at which discovery attempts are made.

To edit previously defined discovery settings, or to configure new discovery settings:

1. Click Create (or select a previously defined discovery setting from the Discovery table and then click Edit).

2. The Create Discovery Entry window opens (or, if you are editing previously defined discovery settings, the Edit Discovery Entry window opens). Select the radio button that corresponds to the type of devices you wish to discovery using this Discovery Entry (Management devices or SNMP) and then click Next.

– Management devices: If you are creating a Management device discovery entry, the following controls are displayed in the Management device discovery definition window:

Field	Description
IP range	The range of IP addresses that will be searched periodically for devices. An IP address range is defined by either using an asterisk to indicate a wildcard portion of the IP address (for example, 192.168.1.* means that you want InfraStruXure Central to periodically check for the presence of a device on all IP addresses between 192.168.1.1 through 192.168.1.255) or by using a hyphenated value to define a specific range of values for part of the IP address (for example, 192.168.1.1-20 means that you want InfraStruXure Central to periodically check for the presence of a device on all IP addresses between 192.168.1.1 through 192.168.1.20, while 192.168.1-20.* checks for devices on all addresses between 192.168.1.1 through 192.168.20.255). **Note:** Use asterisks as a wildcard value only for whole portions of the IP address. Wildcard values must be used to represent the entire range of addresses in each portion of the IP address. For example, 192.168.1.* will work, but 192.168.1.1* will not.
Port range	The TCP/IP ports that will be checked on each IP address.
SSL options	Select from this drop box the selection that corresponds to the SSL communication options that you want to apply to communications when attempting to discover devices. You can choose the following options: • Do not use SSL: Do not use SSL • Use SSL if available: Attempt to use SSL, but proceed with un-encrypted delivery otherwise. If SSL is used, no certificate verification is required. This is the default. • Require SSL: No verification: Require SSL support on the server (do not deliver without it), but accept any certificate provided by the server (i.e. self signed certificates will be allowed). • Require SSL - verify certificate: Require SSL support (do not communicate without it), and only accept certificates signed by a trusted certificate authority (i.e. self signed certificates will not be allowed, but Verisign and the like certificates will be accepted even if the hostname does not match the host in the certificate).
Enable schedule	The current state of this discovery setting schedule. If this check box is not enabled, the discovery settings are saved but scheduled discovery functions will not occur automatically. Instead, discovery functions will occur only when initiated by the user.
Days	The day or days of the week on which the discovery function will be performed.
Time	The time of day at which the discovery function will be performed.

– SNMP devices: If you are creating an SNMP device discovery entry, the following controls are displayed in the SNMP device discovery definition window:

Field	Description
IP range	The range of IP addresses that will be searched periodically for SNMP devices. An IP address range is defined by either using an asterisk to indicate a wildcard portion of the IP address (for example, 192.168.1.* means that you want InfraStruXure Central to periodically check for the presence of an SNMP device on all IP addresses between 192.168.1.1 through 192.168.1.255) or by using a hyphenated value to define a specific range of values for part of the IP address (for example, 192.168.1.1-20 means that you want InfraStruXure Central to periodically check for the presence of an SNMP device on all IP addresses between 192.168.1.1 through 192.168.1.20, while 192.168.1-20.* checks for devices on all addresses between 192.168.1.1 through 192.168.20.255). **Note:** Use asterisks as a wildcard value only for whole portions of the IP address. Wildcard values must be used to represent the entire range of addresses in each portion of the IP address. For example, 192.168.1.* will work, but 192.168.1.1* will not.
Port	The TCP/IP port that will be checked on each IP address.
Timeout	The number of seconds that InfraStruXure Central will wait for a response from a target IP address before either retrying communications or considering the target to be unresponsive. The default value is 30 seconds.
Retries	The number of times that InfraStruXure Central will retry communications with target IP address that is not responding before considering the IP address to be unresponsive and moving on to the next IP address in the IP address range.
Enable schedule	The current state of this discovery setting schedule. If this check box is not enabled, the discovery settings are saved but scheduled discovery functions will not occur automatically. Instead, discovery functions will occur only when initiated by the user.
Days	The day or days of the week on which the discovery function will be performed.
Time	The time of day at which the discovery function will be performed.
Version	The version of SNMP that will be used to communicate with the target. You can select version 1, 2c, or 3.
Read community	The read only community string used for SNMP communications on the target. The default value is public.

3. Type in the required information, and then click Finish to create the discovery entry.

Running Discovery Processes

Discovery processes run automatically according to the schedule you define. However, if you want to run a discovery process right away, select the discovery setting from the Discovery task window and then click Start. To halt a currently running discovery process, select the entry that corresponds to the discovery process and then click Stop.

DHCP LAN Discovery

Note

The DHCP LAN pane is enabled only if the internal DHCP LAN functionality has been enabled on your server. Once enabled, if internal DHCP LAN functionality is later disabled then DHCP LAN discovery will automatically be disabled as well.

When enabled DHCP LAN discovery will automatically search the internal DHCP LAN for management devices or supported SNMP devices. If new devices are discovered, InfraStruXure Central will add them to the appropriate device groups automatically.

To enable DHCP LAN discovery, check the Enable internal DHCP LAN discovery check box. By default, the discovery process will attempt to use the default SNMP read community string “public” when discovering and communicating with any supported SNMP-based devices on the internal DHCP LAN. If necessary, you can add additional read community strings that will be used when attempting to communicate with SNMP devices on the internal DHCP LAN. To add a community string type the new string in the text entry field located beneath the SNMP Read Communities selection list and then click Add.

InfraStruXure Central will also automatically discover the following APC protocol PDU devices if they are connected to the internal DHCP LAN:

- 3 Phase Power Distribution Units:
  - AP7601
  - AP7601J
  - AP7601X135
  - AP7602
  - AP7602X135
  - AP7608
  - AP7610
  - AP7651
  - AP7652
  - AP7658
- 1 Phase Power Distribution Units:
  - AP7611
  - AP7620
  - AP7621
  - AP7622

- – AP7622N
- – AP7626
- – AP7640
- – AP7641

Note: APC protocol PDU devices will be discovered only if they are connected to the internal DHCP LAN. APC protocol PDU devices that are connected to a public LAN will not be discovered.

Disk Array Management

Use the Disk Array Management task to check the status of the RAID array (included with Enterprise Edition InfraStruXure Central). The current status of the following components of your disk array are displayed:

- Disk array controller status
- Disk array status
- Disk array type
- Individual drive status

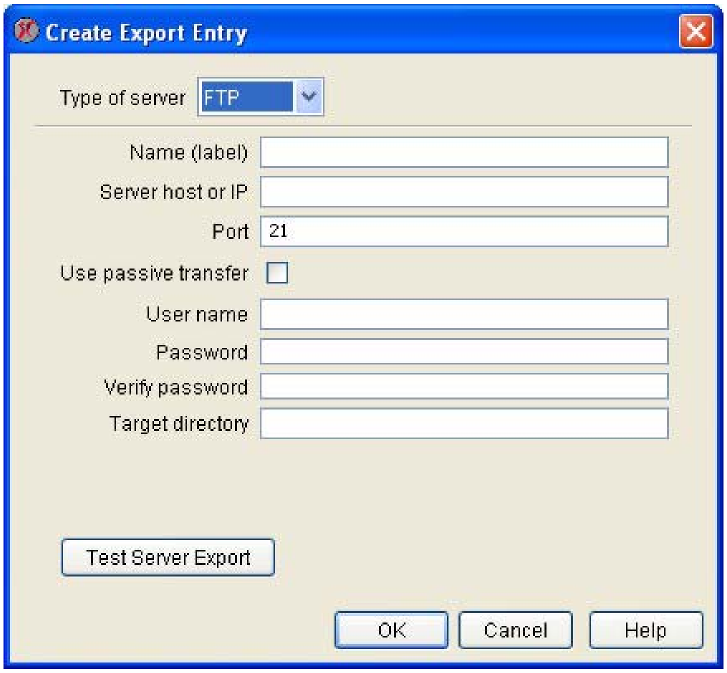
Note: This task will be available only when using the InfraStruXure Central console to manage an Enterprise Edition InfraStruXure Central server.

Export Administration

Use the Export Administration task to specify servers to which reports (generated using the Report View) can be saved for future reference. To create or edit an export entry:

1. Launch the Export Administration task and then click Create. To edit a previously created Export entry, select the desired entry and then click Edit.

2. The Create/Edit window opens. Type in the Name (label) field a name for the export entry.



3. Select from the Type of server drop box that type of server to which data will be saved. You can select FTP, E-mail, HTTP, Windows, or NFS.

4. Fill in the server-type specific data fields. The fields that appear in the rest of the window depend on what server type has been selected from the Type of server drop box.

- If you select FTP from the Type of server drop box the following fields are available:

Field	Description
Server hostname or IP	The hostname or IP address of the server to which the data will be saved.
Port	The TCPIP port that is used by the server for FTP communications.
Use passive transfer check box	Check this check box to use passive FTP transfers when communicating with the FTP server. This can be useful if your InfraStruXure Central server is communicating across a firewall.
User name	The user name that will be used, along with the password, to gain access to the specified FTP server.
Password/Verify password	The password that will be used, along with the user name, to gain access to the specified FTP server.
Target directory	The relative directory path to be used for storing the data on the FTP server. This should always be a path relative to the default directory associated with the user ID used to log on to the FTP server. If the directories on the path do not exist they will be created automatically. The Target Directory field accepts macros.

- If you select E-mail from the Type of server drop box the following fields are available:

Field	Description
Subject of message	The subject of the e-mail message that will be generated and sent.
Body of message	The body of the message e-mail message that will be generated and sent.
E-mail addresses	E-mail addresses to which the e-mail message that will be generated and sent. To add e-mail addresses click Add. To remove previously added e-mail addresses select an address and then click Remove.

Note

The SMTP server that is used to e-mail saved report data is defined using the Server Settings task.

- If you select HTTP from the Type of server drop box the following fields are available:

Field	Description
Target URL for POST	The URL to which the data will be POSTed.
Server requires authentication check box	Check this check box if the HTTP server requires a user name and password for access.
User name	The user name that will be used, along with the password, to gain access to the specified HTTP server.
Password/Verify password	The password that will be used, along with the user name, to gain access to the specified HTTP server.
SSL options	Select from this drop-box the SSL options that will be used for this post.

- If you select Windows from the Type of server drop box the following fields are available:

Field	Description
Server IP or host	The hostname or IP address of the Windows share.
User name	The user name required to access the Windows share.
Password/Verify password	The password that is required to access the Windows share.
Domain	The domain to which the Windows share is connected.
Share name	The name of the Windows share.
Subdirectory (optional)	The subdirectory in the Windows share that will be used to store data. If no subdirectory is specified, data will be stored in the root directory of the share.

- If you select NFS from the Type of server drop box the following fields are available:

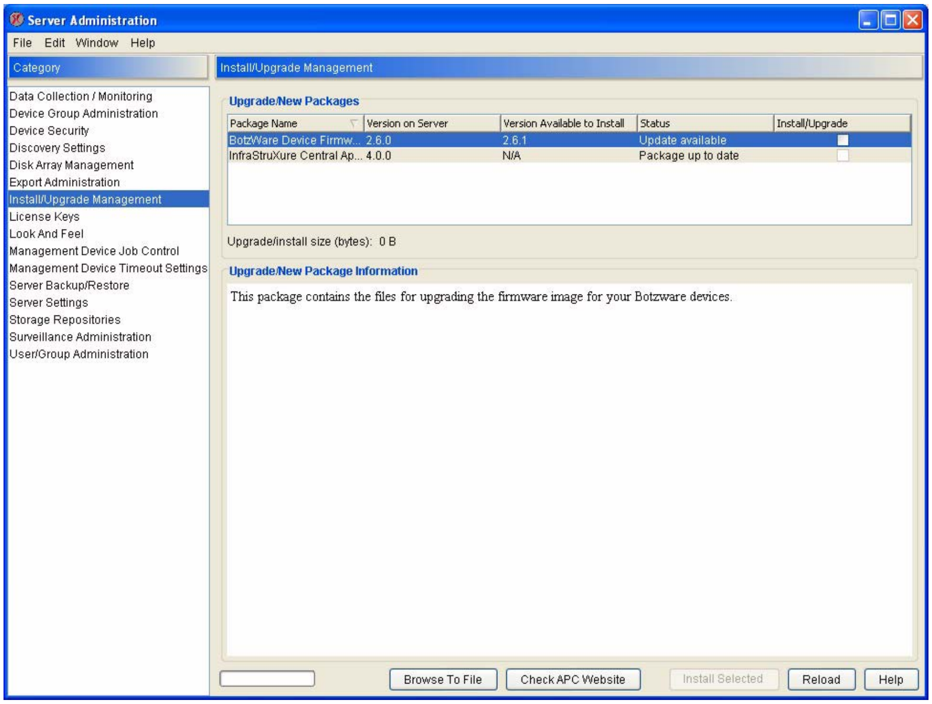
Field	Description
Server hostname or IP	The hostname or IP address of the NFS mount.
Share path	The path for the NFS share.
Subdirectory (optional)	The subdirectory in the NFS mount that will be used to store data. If no subdirectory is specified, data will be stored in the root directory of the mount.

5. When you have finished entering the required values, click Test Server Export to ensure that the server can be accessed.
6. Click OK to save your export entry.

Install/Upgrade Management

Use the Install/Upgrade Management task to check for and apply any upgrades that are available for the various applications used by the InfraStruXure Central server. This task also enables you to manage the BotzWare images that are stored on your InfraStruXure Central server for use with the Mass Configuration Upgrade task.

The Upgrade/New Packages selection list displays a list of upgrades or new software packages that are available for use with your InfraStruXure Central server and managed devices. Upgrades can be obtained using CDs or from the APC web site. Using this pane, you can check for upgrades and install them if needed.



Package Name	Version on Server	Version Available to Install	Status	Install/Upgrade
BotzWare Device Firmw...	2.6.0	2.6.1	Update available	□
InfraStruXure Central Ap...	4.0.0	N/A	Package up to date	□

Upgrade/install size (bytes): 0 B

This package contains the files for upgrading the firmware image for your Botzware devices.

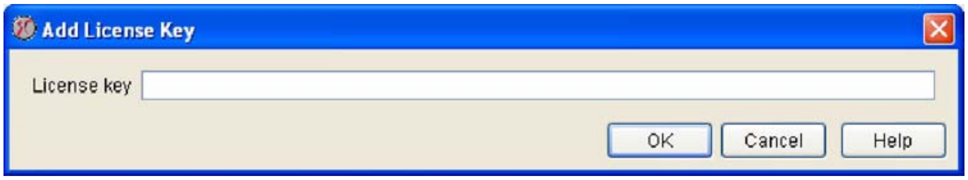
To determine if upgrades are available for any of the package names listed in this pane, select the source from which upgrades and packages will be installed.

- To compare the version of package names available from a CD against those that are available from your InfraStruXure Central server, click Browse to File and select the CD-ROM drive that contains your CD. Then, select the directory that contains the master.release file and click Open.
- To compare the version of packages available for download from the APC web site against those that are available from your InfraStruXure Central server, click Check APC Website.

The version of each package that is currently installed appears in the Version on Server column, while the versions available for upload from your selected source appear in the Version Available to Install column. The message in the Status column notifies you if an Update to the package is available from the selected source. To upload and install an available update select the package and then click Install Selected.

License Keys

Use the License Keys task to display and modify the license key information for your InfraStruXure Central server. Information displayed includes currently implemented license keys and functions, as well as unlicensed functions that are available for use on your server (if any).



To use License Key task to add a new license key click Add and then type in the License Key field the license key that you wish to add, and then click OK. To remove a previously added license key, select the license key you wish to remove from your server and then click Delete.

Look and Feel

Use the Look and Feel task to specify the image that is displayed on the InfraStruXure Central server's web page, the image that is displayed in the logon prompt window, and the status logo image that is displayed in lower left-hand corner of the InfraStruXure Central interface.

To select an image, select the Browse button that corresponds to the image type you want to specify and then use the interface to the desired image file.

- The image that is displayed on the home page cannot be larger than 514 pixels in width or 118 pixels in height.
- The image displayed in the logo prompt window cannot be larger than 64 pixels in width or height.
- The image displayed for the status logo cannot be larger than 106 pixels in width or 26 pixels in height.

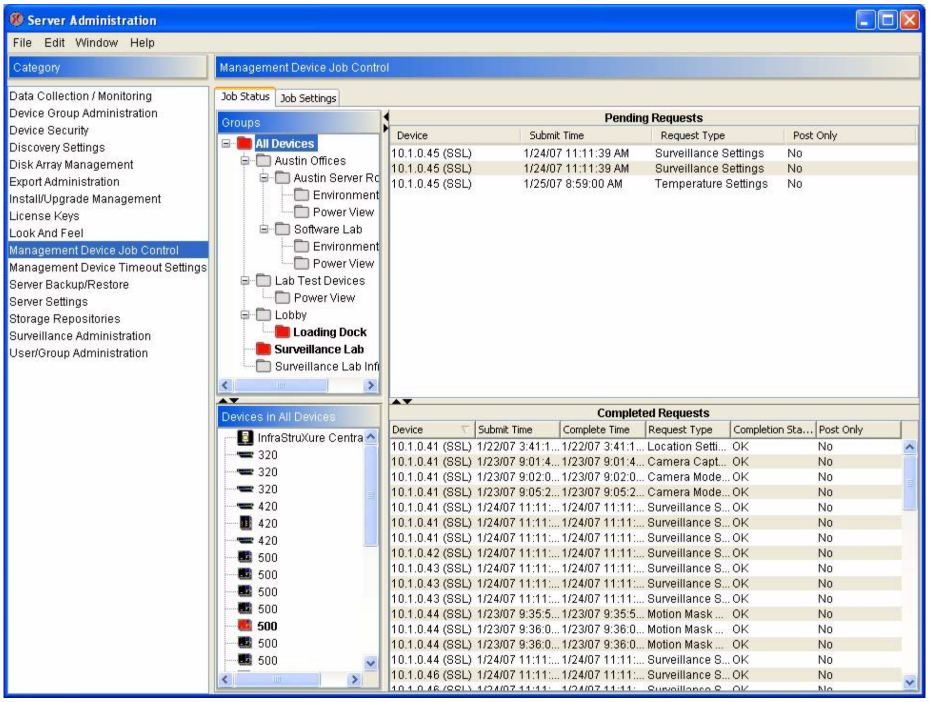
If desired, you can restore the default image for any of the images by selecting the appropriate Restore Default button.

Management Device Job Control

Use the Management Device Control task to view a list of tasks that are currently pending against offline or Post Only devices; to view a list of previously pending tasks that have been completed; and to configure a variety of Management Device Job Control settings, including the length of time for which information about completed job will be stored and the frequency with which camera images from Post Only clients will be posted to InfraStruXure Central. The Device Job Control task window consists of 2 panes: Job Status and Job Settings.

Using the Job Status Pane

If InfraStruXure Central attempts to configure a device that is in Post Only mode or that is presently offline or unreachable, the task will be placed in a pending state and will appear in the Pending Requests list. Jobs that were previously in a pending state but which have since been successfully completed appear in the Completed Requests list. Completed jobs will remain in the Completed Requests list for the period of time specified by the Job complete history (days) setting in the Job Settings pane, after which they will not longer be listed.



Pending Requests

Device	Submit Time	Request Type	Post Only
10.1.0.45 (SSL)	1/24/07 11:11:39 AM	Surveillance Settings	No
10.1.0.45 (SSL)	1/24/07 11:11:39 AM	Surveillance Settings	No
10.1.0.45 (SSL)	1/25/07 8:59:00 AM	Temperature Settings	No

Completed Requests

Device	Submit Time	Complete Time	Request Type	Completion Sta...	Post Only
10.1.0.41 (SSL)	1/22/07 3:41:1...	1/22/07 3:41:1...	Location Setti...	OK	No
10.1.0.41 (SSL)	1/23/07 9:01:4...	1/23/07 9:01:4...	Camera Capt...	OK	No
10.1.0.41 (SSL)	1/23/07 9:02:0...	1/23/07 9:02:0...	Camera Mode...	OK	No
10.1.0.41 (SSL)	1/23/07 9:05:2...	1/23/07 9:05:2...	Camera Mode...	OK	No
10.1.0.41 (SSL)	1/24/07 11:11:...	1/24/07 11:11:...	Surveillance S...	OK	No
10.1.0.41 (SSL)	1/24/07 11:11:...	1/24/07 11:11:...	Surveillance S...	OK	No
10.1.0.41 (SSL)	1/24/07 11:11:...	1/24/07 11:11:...	Surveillance S...	OK	No
10.1.0.42 (SSL)	1/24/07 11:11:...	1/24/07 11:11:...	Surveillance S...	OK	No
10.1.0.43 (SSL)	1/24/07 11:11:...	1/24/07 11:11:...	Surveillance S...	OK	No
10.1.0.43 (SSL)	1/24/07 11:11:...	1/24/07 11:11:...	Surveillance S...	OK	No
10.1.0.43 (SSL)	1/24/07 11:11:...	1/24/07 11:11:...	Surveillance S...	OK	No
10.1.0.44 (SSL)	1/23/07 9:35:5...	1/23/07 9:35:5...	Motion Mask ...	OK	No
10.1.0.44 (SSL)	1/23/07 9:36:0...	1/23/07 9:36:0...	Motion Mask ...	OK	No
10.1.0.44 (SSL)	1/23/07 9:36:0...	1/23/07 9:36:0...	Motion Mask ...	OK	No
10.1.0.44 (SSL)	1/24/07 11:11:...	1/24/07 11:11:...	Surveillance S...	OK	No
10.1.0.46 (SSL)	1/24/07 11:11:...	1/24/07 11:11:...	Surveillance S...	OK	No
10.1.0.46 (SSL)	1/24/07 11:11:...	1/24/07 11:11:...	Surveillance S...	OK	No

Removing Pending Requests

If you wish to remove a job from the Pending Requests list (and therefore prevent the pending job from being completed on the device), right-click on the desired task and the select Remove Pending Request from the pop-up menu. Note that if there is more than one job for a given device currently listed in Pending Requests list and you remove a request, any subsequent pending requests for that device will automatically be removed from the list as well.

Using the Job Settings Pane

Use the Job Settings pane to specify the number of days for which completed tasks will be displayed in the Completed Tasks list on the Job Status pane and to configure device-specific camera image posting settings for Post Only clients. These settings determine how often camera images that are stored on devices will be posted to the InfraStruXure Central database.

To configure the Job History settings, use the spin buttons to specify the number of days for which completed job will be displayed and then click Apply to save your settings.

To set the Post Only Camera Settings, select the radio button that corresponds to the frequency with which management devices in Post Only mode should send camera images. The available settings are:

- Send camera images whenever posting to InfraStruXure Central: Images are posted every time InfraStruXure Central communicates with the device. This is the default setting.
- Never send camera images when posting to InfraStruXure Central: Images are never posted to InfraStruXure Central.
- Send camera images when posting to InfraStruXure Central using the following interval: Images are posted to InfraStruXure Central at the specified interval. For example, if you set this value to 3 then images are posted during one communication, and are not posted again until 3 successive communications between the device and InfraStruXure Central have occurred.

When you have finished selecting a Post Only Camera Setting click Apply to save your settings.

Management Device Security Settings

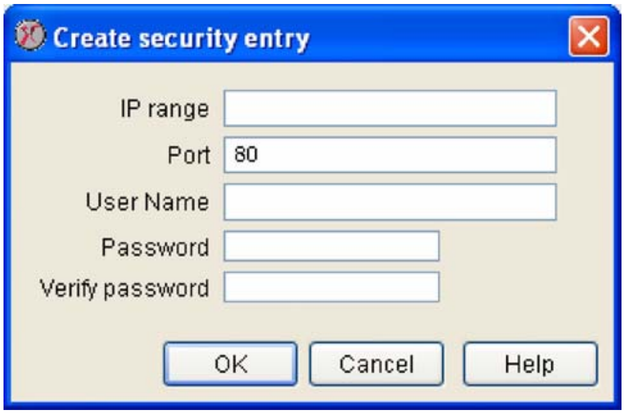
Use the Management Device Security Settings task to specify the user names and passwords that InfraStruXure Central will use to monitor and manage your devices. By default, InfraStruXure Central will attempt to use the default supervisor (administrator) user name and password (netbotz/netbotz) to access and manage devices when performing configuration tasks. If you have changed the administrator password on your devices, you must use the Management Device Security Settings task to specify the user name and password that will enable InfraStruXure Central to access your devices.

Note

If InfraStruXure Central is not configured to have administrator-level access to your devices you will not be able to perform configuration tasks on the devices.

To edit previously defined device security settings, or to configure new security settings:

1. Click Create (or, select a previously defined setting from the table and then click Edit).



Port 80

2. The Create Security Entry window opens (or, if you are editing a previously defined user group, the

Edit Security Entry window opens). This window contains the following controls:

Field	Description
IP range	The IP address or IP address range for this security setting. The user name and password will be used only for devices that are connected to your network at the specified IP address or at an IP address that falls within the specified range. To specify an IP address range, use the asterisk as a wildcard value in the IP address (for example, specifying an IP address of 192.168.1.* will result in this security entry being used whenever InfraStruXure Central attempts to log into and manage any device with an IP address of 192.168.1.1 through 192.168.1.255) or use a hyphenated value to define a specific range of values for part of the IP address (for example, 192.168.1.1-20 means that you want InfraStruXure Central to periodically check for the presence of a device on all IP addresses between 192.168.1.1 through 192.168.1.20).
Port	The IP port used to communicate with devices in the specified IP Range.
User name	The user name that will be used when attempting to manage a device with the IP address specified.
Password	The password that will be used when attempting to manage a device with the IP address specified.

3. Use the controls to set the security entry settings.
4. When you are finished, click OK to save this configuration.

Management Device Timeout Settings

Use the Management Device Timeout Settings task to specify the timeout settings that InfraStruXure Central will use when attempting to communicate with devices on your network. InfraStruXure Central comes pre-configured with timeout settings that will work for most networks. However, depending on your network topology and architecture, you might need to create IP address-specific or IP address range-specific timeout settings.

When you start the Management Device Timeout Settings task a table is displayed that contains all currently defined timeout settings. The table contains the following information about each timeout setting:

Field	Description
IP range	The range of IP addresses that the timeout settings apply to. An IP address range is defined by either using an asterisk to indicate a “wildcard” portion of the IP address (for example, 192.168.1.* means that the timeout settings apply to devices on all IP addresses between 192.168.1.1 through 192.168.1.255) or by using a hyphenated value to define a specific range of values for part of the IP address (for example, 192.168.1.1-20 means that the timeout settings apply to all devices on all IP addresses between 192.168.1.1 through 192.168.1.20).

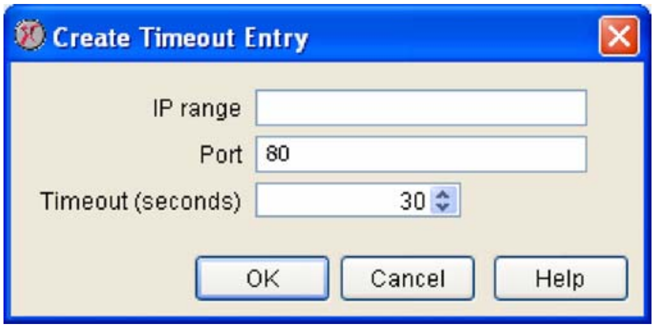
Field	Description
Port	Type in this field the TCPIP port number for which these device timeout settings apply.
Timeout	Type in this field the amount of time that InfraStruXure Central should wait when attempting to connect to or obtain data from a device in the specified IP address range before declaring it unreachable.

Note

Use asterisks as a wildcard value only for whole portions of the IP address. Wildcard values must be used represent the entire range of addresses in each portion of the IP address. For example, “192.168.1.*” will work, but “192.168.1.1*” will not.

To edit previously defined timeout settings, or to configure new timeout settings:

1. Click Create (or select a previously defined timeout setting from the Device Timeout Settings table and then click Edit).
2. The Create Timeout Entry window opens (or, if you are editing previously defined discovery settings, the Modify Timeout Entry window opens). Use the controls in the window to specify the IP range, port, and timeout value.



IP range
Port 80
Timeout (seconds) 30

3. Click OK to save this entry.

Server Settings

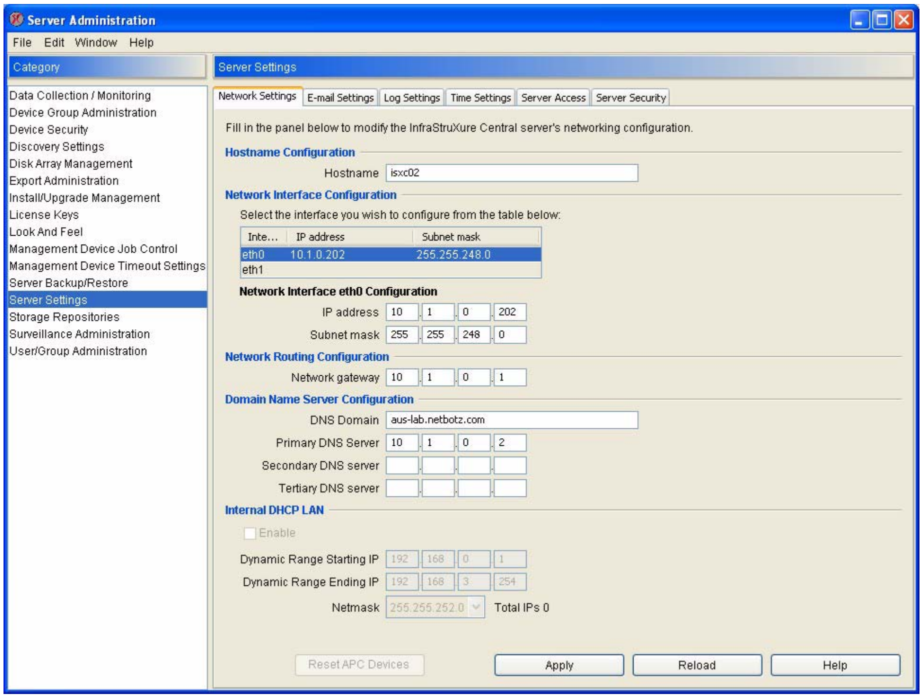
Use the Server Settings task to configure a variety of InfraStruXure Central server access and configuration tasks, including:

- Network Settings
- E-mail Settings
- Log Settings
- Time Settings
- Server Access
- Server Security

Network Settings

Use the Network Settings pane to configure the InfraStruXure Central server network settings for your server network interfaces. You can configure the following settings:

- Hostname
- Network interface configuration
- Network routing configuration
- Domain name server configuration
- Internal DHCP LAN



Fill in the panel below to modify the InfraStruXure Central server's networking configuration.

Hostname Configuration

Hostname: isxc02

Network Interface Configuration

Select the interface you wish to configure from the table below:

Inte...	IP address	Subnet mask
eth0	10.1.0.202	255.255.248.0
eth1		

Network Interface eth0 Configuration

IP address: 10 . 1 . 0 . 202

Subnet mask: 255 . 255 . 248 . 0

Network Routing Configuration

Network gateway: 10 . 1 . 0 . 1

Domain Name Server Configuration

DNS Domain: aus-lab.netbotz.com

Primary DNS Server: 10 . 1 . 0 . 2

Secondary DNS server: . . .

Tertiary DNS server: . . .

Internal DHCP LAN

□ Enable

Dynamic Range Starting IP: 192 . 168 . 0 . 1

Dynamic Range Ending IP: 192 . 168 . 3 . 254

Netmask: 255.255.252.0 Total IPs 0

To configure the device's network settings, provide the following information:

Field	Description
Hostname	The hostname assigned to the server.
IP address	The IP address being used by your server.
Subnet mask	The subnet mask for your network.
Gateway	The IP address of the gateway in your network.
DNS domain	The name of the DNS domain to which the InfraStruXure Central server belongs.
Primary DNS server	The IP address of the primary domain name server.
Secondary DNS server	The IP address of the secondary domain name server.
Tertiary DNS server	The IP address of the tertiary domain name server.

Field	Description
Enable Internal DHCP LAN check box	Check this check box to enable internal DHCP-based LAN support. **Important:** When enabling the internal DHCP LAN, the private LAN connection must be connected to LAN Port 2 on your InfraStruXure Central appliance. Once this feature is enabled, ensure that LAN Port 2 is NOT connected to a public LAN. Enabling this functionality on an InfraStruXure Central with LAN Port 2 connected to a public LAN will result in serious network connectivity issues.
Internal DHCP LAN Dynamic Range Starting IP and Internal DHCP LAN Dynamic Range Ending IP	Specify the first and last IP addresses in the IP address range that will be assigned to devices connected to the internal DHCP LAN. **Important:** The IP address range specified for use by the internal DHCP LAN must not overlap with the IP addresses used for devices on the public LAN. IP addressing overlaps between the public LAN and devices on the internal DHCP LAN will result in network connectivity and communication errors.
Internal DHCP LAN Netmask	Specify the netmask value that will be used for the Internal DHCP LAN.
Reset APC Devices	When the internal DHCP LAN is enabled, resets any SNMP-based APC devices or APC protocol PDU devices connected to the internal DHCP LAN. Resetting these devices will force them to request a new IP address from the DHCP LAN server. **Notes:** • You will need to provide the Write community name to reset SNMP-based devices. • The write community names used to reset your APC devices are not saved on the InfraStruXure Central server. You will need to re-enter the write community names each time you choose to reset your APC devices. • Be sure to reset your SNMP-based APC devices and APC protocol PDU devices whenever you make changes to the internal DHCP LAN dynamic IP range or netmask settings.

When you have finished providing the required information, click Apply to save your network settings.

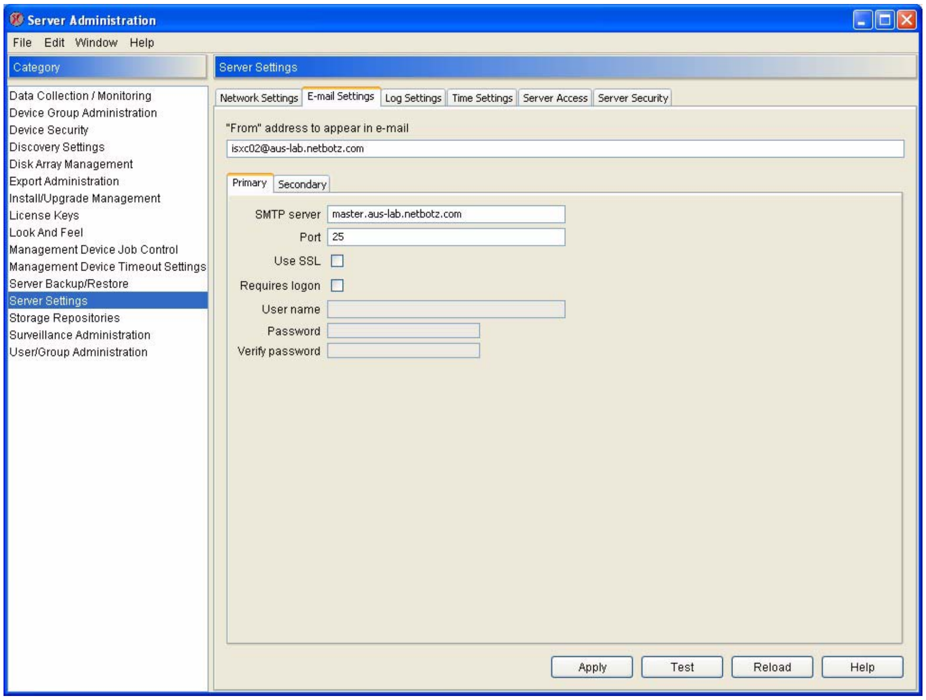
E-mail Settings

Use the E-mail Settings pane to specify the e-mail address that will appear in the “From” field of any e-mails generated by the InfraStruXure Central server and to specify primary and secondary mail servers that will be used to deliver any e-mail notifications. This window contains the following fields:

Field	Description
From address	The e-mail address that will appear in the “From” field of any e-mail generated by the InfraStruXure Central server.
SMTP server	The IP address of the SMTP server.
Port	The IP port on the e-mail server used for SMTP communications.

Field	Description
Requires logon check box	Check this check box if the server requires you to log in to send e-mail.
User name	Provide a User ID that will be accepted by the SMTP server when sending e-mail.
Password/Verify password	Provide a password that will be accepted by the SMTP server when sending e-mail.

All settings except the From address field are available for both a Primary and Secondary e-mail server.



"From" address to appear in e-mail: isxc02@aus-lab.netbotz.com

SMTP server: master.aus-lab.netbotz.com

Port: 25

Use SSL □

Requires logon □

User name

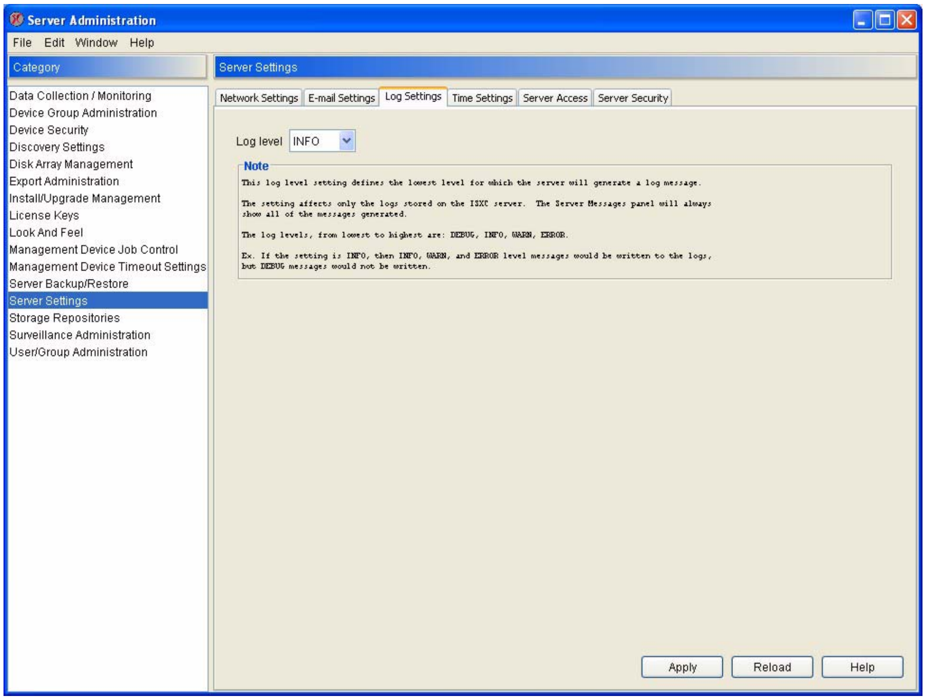
Password

Verify password

The secondary server is used if the InfraStruXure Central server is unable to connect to the primary e-mail server. To change the InfraStruXure Central server E-mail Server settings, type the new values in the appropriate fields. When you are finished, click Apply to save any changes to the server. Click Test to test your e-mail server settings. Click Cancel to close this window without saving any changes.

Log Settings

Use the Log Management pane to specify the log level filter for use with the InfraStruXure Central server log. The log level value determines what the minimum priority value of a InfraStruXure Central log message must be for that message to be stored in the Server Messages logs. Only messages that are of the selected log level priority or higher will be stored.



Log level: INFO

Note

This log level setting defines the lowest level for which the server will generate a log message.

The setting affects only the logs stored on the ISXC server. The Server Messages panel will always show all of the messages generated.

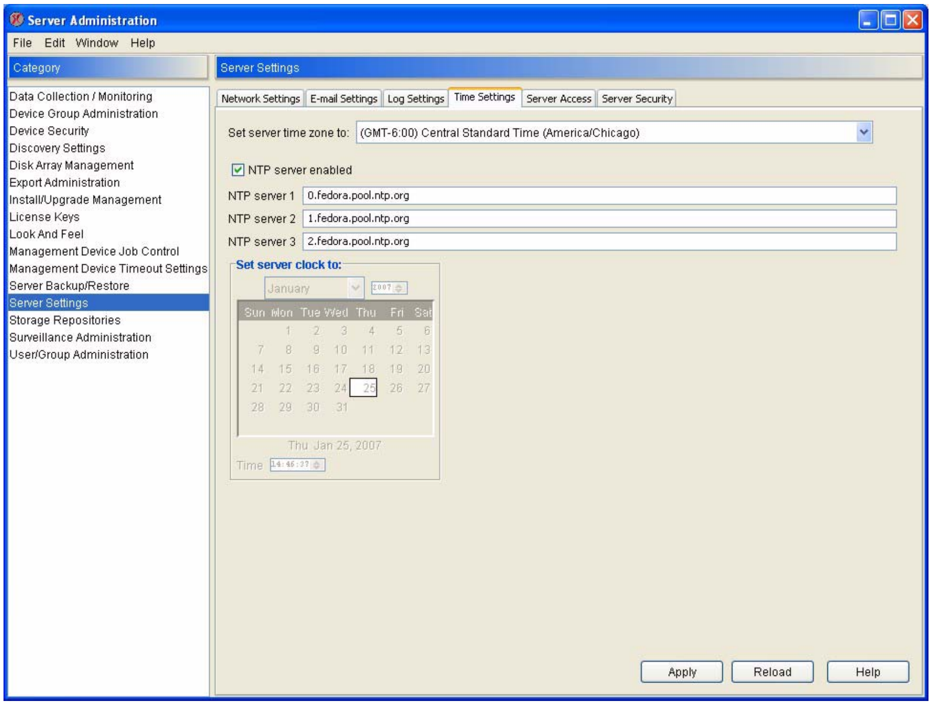
The log levels, from lowest to highest are: DEBUG, INFO, WARN, ERROR.

Ex. If the setting is INFO, then INFO, WARN, and ERROR level messages would be written to the logs, but DEBUG messages would not be written.

There are four log level values: DEBUG, INFO, WARNING, and ERROR (in order of increasing priority). The default Log Level value is INFO, meaning that messages that have a priority value of DEBUG are not stored in the logs, while all other messages are stored. To change the log level value, select from the Log level drop box the desired log level value and then click Apply.

Time Settings

Use the Time Configuration pane to specify the date and time that are configured on the InfraStruXure Central server's internal clock, or to configure your server to obtain and synchronize its clock settings from an NTP server.



Set server time zone to: (GMT-6:00) Central Standard Time (America/Chicago)

☑ NTP server enabled

NTP server 1: 0.fedora.pool.ntp.org

NTP server 2: 1.fedora.pool.ntp.org

NTP server 3: 2.fedora.pool.ntp.org

Set server clock to:

January 2007

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Thu Jan 25, 2007

Time 14:46:37

The following controls are available from the Time Configuration pane:

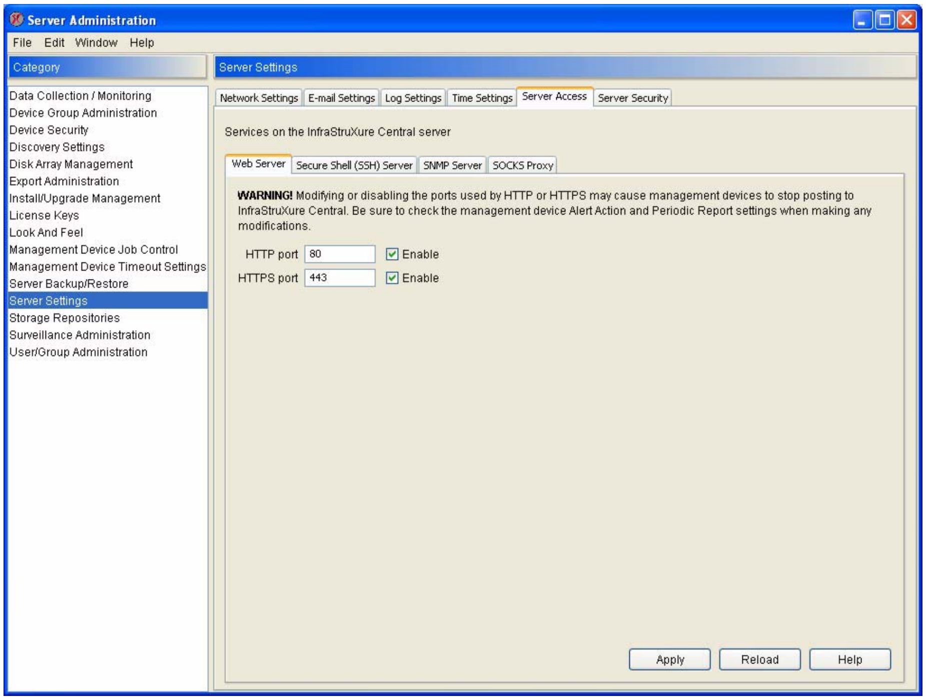
Field	Description
Locale	Select from the list the location in which the InfraStruXure Central server is located.
Set server time zone to	Select from this drop box the time zone used in the InfraStruXure Central server’s location.
Use 24 hour time	Select to configure the InfraStruXure Central server to report time using a 24-hour clock (for example, 1430).
Enable NTP check box	Check this check box to enable the NTP functionality. Un-check this check box to enable the clock and calendar controls on this pane.
Primary, Secondary, and Tertiary NTP Servers	IP address or hostnames of NTP servers for use in automatically setting the server clock.
Date/Time Controls	Use the arrows in the Time field, the Month drop box, the arrows in the Year field, and the Calendar control to manually configure the day, date, and time used by your server’s internal clock.

To specify the date on time manually, uncheck the NTP server enabled check box and then use the controls to specify the time zone in which the server resides, as well as a month, year, day, and time. Click Apply to save these settings.

To configure your server to automatically obtain date and time settings from one or more NTP servers, check the NTP server enabled check box and then provide one or more NTP server IP addresses or hostnames in the appropriate fields. Click Apply to save these settings.

Server Access

Use the Server Access pane to enable, disable, and configure settings associated with the different network-accessible processes running on your server. These processes include the web server, the SSH daemon, the SNMP daemon, and the SOCKS proxy. Each of these processes has its own sub-pane in the Server Access pane.



WARNING! Modifying or disabling the ports used by HTTP or HTTPS may cause management devices to stop posting to InfraStruXure Central. Be sure to check the management device Alert Action and Periodic Report settings when making any modifications.

HTTP port 80 ☑ Enable

HTTPS port 443 ☑ Enable

The Web Server Pane

Use the Web Server pane to view or change the IP ports through which your InfraStruXure Central server performs HTTP and HTTPS web server communications.

Note

Enabling and disabling HTTP or HTTPS access, or changing the IP ports used for these communications, can prevent devices from posting data to your InfraStruXure Central server. Be sure to check the Alert Action and Periodic Report settings of your devices before making changes to the Web Server settings.

The Web Server pane contains the following fields:

Field	Description
HTTP port	The IP port through which HTTP communications are performed.
HTTPS port	The IP port through which HTTPS communications are performed.
HTTP port/HTTPS port Enable check boxes	Check the check box to enable the corresponding web server port.

Note

IP ports 1 - 65535 are valid, with the exception of ports 20, 21, 22, 23, 25, 123, 161, and 389. These ports are reserved for use by the NetBotz appliance, and using them would create a conflict and would result in operational difficulties.

Type in the desired values and then click Apply to save any changes to the server.

Click Cancel to close this window without saving any changes.

The Secure Shell (SSH) Control Pane

Secure shell (SSH) is a program that enables you to log into your InfraStruXure Central server over a network, from a command line, and to execute commands on the device. It provides strong authentication and secure communications over insecure channels. Your InfraStruXure Central server supports SSH connections, but this support is primarily intended for use with APC support guidance in troubleshooting device issues. You can use the Secure Shell (SSH) Control pane, to enable or disable the SSH support on the device.

Using this pane you can specify whether or not SSH is currently running, and also specify whether or not you want SSH started automatically at device startup. Select the appropriate radio buttons and then click Apply to save your settings.

The SNMP Server Pane

Use the SNMP Server pane to view or change the SNMP communications settings on your InfraStruXure Central server. The SNMP pane contains the following fields:

Field	Description
Enable SNMP agent check box	Check this check box to enable the SNMP agent on your device.
Read-only community	Type in this field the read-only community name for SNMP read requests.
Confirm community	When updating or changing the SNMP read-only community name, type the new community name in this field as well.
SNMP read/write community	Type in this field the read/write community name for SNMP read requests.
Confirm community	When updating or changing the SNMP read/write community name, type the new community name in this field as well.
Port	Type in this field the port number to be used for SNMP communications. The default value is 161.

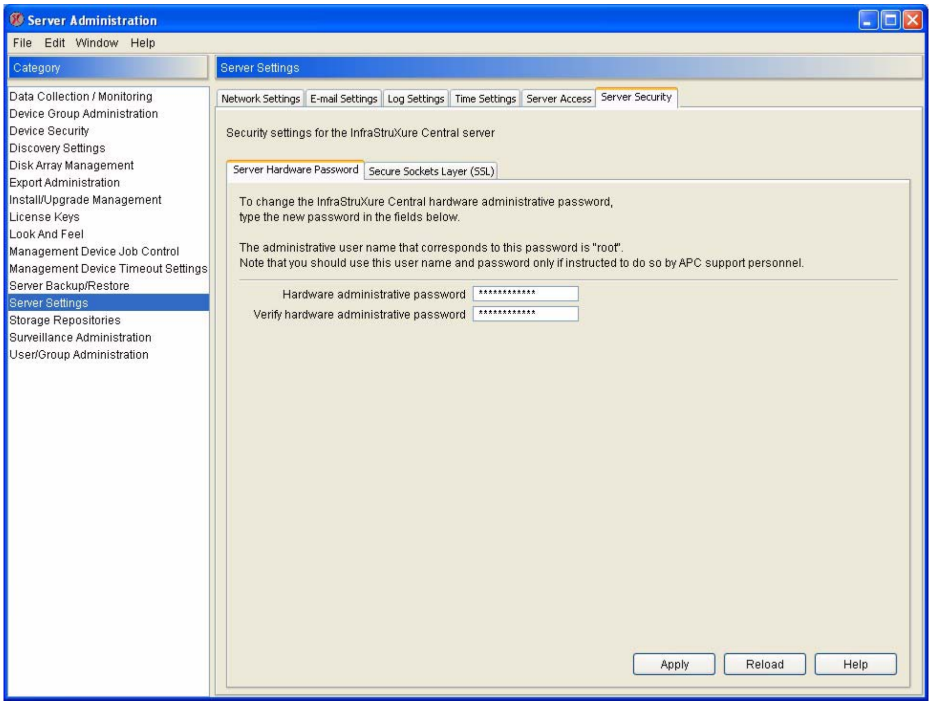
Type in the desired values and then click Apply to save any changes to the server. Click Cancel to close this window without saving any changes.

SOCKS Proxy Pane

Use the SOCKS Proxy pane to enable or disable InfraStruXure Central's built-in SOCKS v5 proxy server. Once enabled, users with proxy access will be able to connect to the server using a SOCKS client, and will also be able to access devices that reside on the internal DHCP LAN from the public LAN. The SOCKS v5 server uses port 1080.

Server Security

Use the Server Security pane to specify the security features of your InfraStruXure Central server. Using this pane, you can change the Server Hardware Password and configure your InfraStruXure Central server to communicate with InfraStruXure Central consoles using a Secure Sockets Layer (SSL) certificate.



Security settings for the InfraStruXure Central server

To change the InfraStruXure Central hardware administrative password, type the new password in the fields below.

The administrative user name that corresponds to this password is "root". Note that you should use this user name and password only if instructed to do so by APC support personnel.

Hardware administrative password ************

Verify hardware administrative password ************

The Server Security pane consists of two sub-panes: The Server Hardware Password pane and the Secure Sockets Layer (SSL) pane.

Using the Server Hardware Password Pane

The Server Hardware Password is the password needed to access the server when communicating with it using the serial port. Your InfraStruXure Central server comes with a pre-configured root account. The root account is used only for server communications that are performed using the serial port, such as when you use the Serial Configuration Utility to specify network settings. The user name and password for this pre-configured account are:

User name: root

Password: apc

You cannot change the root account user name. However, to ensure security, be sure to use the Server Hardware Password pane to change the default root account password. To change the hardware password, type a new password in both the Hardware administrative password and Verify hardware administrative password fields and then click Apply.

Using the Secure Sockets Layer (SSL) Pane

Use the Secure Sockets Layer (SSL) pane to configure your InfraStruXure Central server to use SSL encryption for all network communication between web browsers using the InfraStruXure Central console and the InfraStruXure Central server. You can use this pane to Install an SSL certificate, to examine a previously installed SSL certificate and its Private Key, and to uninstall a previously installed SSL certificate.

To install a certificate, click Install Certificate and then provide the SSL certificate data.

- If you have submitted your key to a certification authority and have received your signed certificate, copy and paste the signed certificate into the Install certificate field.
- If you received a Privacy Enhanced Mail (PEM) file from your certification authority, click Import Certificate, select the PEM file, and then click OK to import the contents of the PEM file into the Install certificate field.

When you have finished, click Apply to install the certificate.

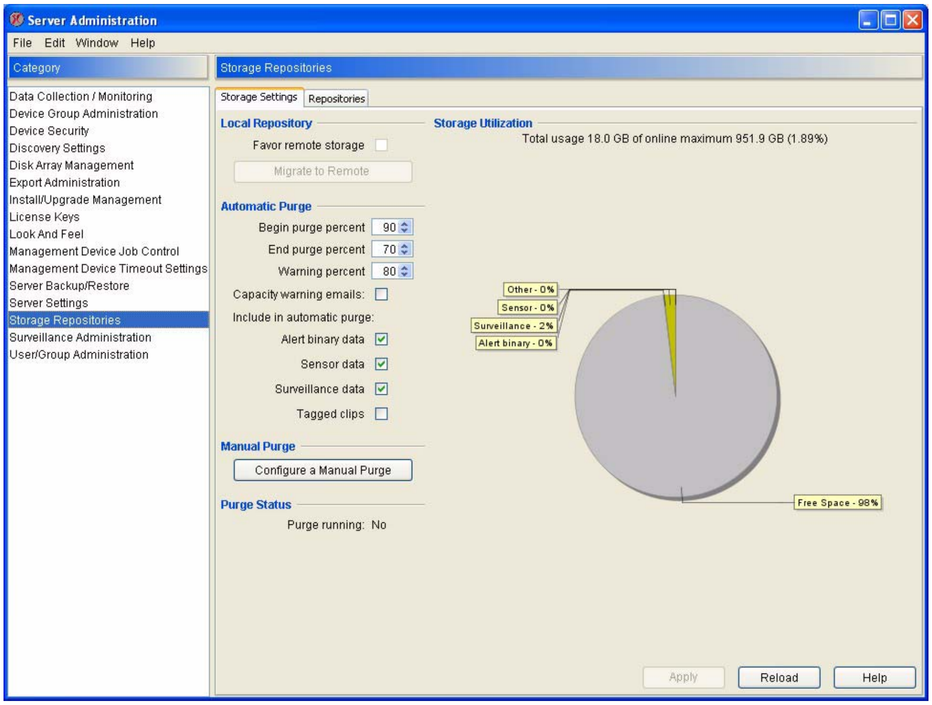
Note

After creating a certificate signing request be sure to save a copy of your server's private key before installing the certificate you receive. Should you ever need to re-install your certificate on a replacement server, you'll need both the private key and the certificate you bought.

To remove a previously installed certificate, click Remove Certificate.

Storage Repositories

Use the Storage Repositories task to monitor the status of storage repositories that have been defined for use with your InfraStruXure Central server, to configure the automatic disk space management system or to manually purge data from the database to free up disk space. InfraStruXure Central's disk management system monitors the size of your InfraStruXure Central database and will automatically purge older data when repository space is running low. The Storage Repository task also enables you to specify automatic e-mail notifications when a user-defined percentage of your disk space has been utilized, enabling you to schedule a database backup or manually purge data from the database. Finally, the Storage Repositories task enables you to specify network attached storage for use as remote storage repositories for InfraStruXure Central data.



Local Repository

Favor remote storage □

Automatic Purge

Begin purge percent 90

End purge percent 70

Warning percent 80

Capacity warning emails: □

Include in automatic purge:

Alert binary data ☑

Sensor data ☑

Surveillance data ☑

Tagged clips □

Manual Purge

Purge Status

Purge running: No

Storage Utilization

Total usage 18.0 GB of online maximum 951.9 GB (1.89%)

The Storage Repositories task window consists of two panes: The Storage Settings pane and the Repositories pane.

The Storage Settings Pane

The Storage Settings pane features a pie chart that shows you the percentage of your storage repositories that is currently being used. The pie chart includes sections for the following types of data that are stored in the repository:

- Alert binary: All binary data associated with alert events
- Surveillance: All data associated with Surveillance events
- Sensor: All sensor data
- Other: Indexing and miscellaneous non-InfraStruXure Central data that is associated with the repository mount point
- Free space: Repository space that is currently unused

This interface also includes the following controls:

Field	Description
Favor remote storage check box	When checked, InfraStruXure Central will store data on remote storage repositories unless none are available.
Migrate to Remote	Click Migrate to Remote to migrate all data that is currently stored in the local repository to remote storage repositories.
Begin purge percent	Use this control to specify the disk utilization percentage at which Automatic Purge begins.
End purge percent	Use this control to specify the disk space utilization percentage at which Automatic Purge will cease.
Warning percent	Use this control to specify the percentage of disk utilization at which the InfraStruXure Central server will send an e-mail notification to all InfraStruXure Central users that have administrator access advising them that the repository space available to this InfraStruXure Central server is getting low. **Note:** Warning e-mails will be sent only if the **Capacity warning** e-mails check box is checked.
Capacity warning e-mails check box	When checked, the InfraStruXure Central server will send e-mail notifications to all InfraStruXure Central users that have administrator access informing them of the current capacity status of the server repository whenever it exceeds the disk space utilization specified by the **Warning percent** setting.
Include in purge check boxes	Check the check boxes that correspond to the data types that will be purged during automatic purge. The available data types are: Alert binary data, Sensor data, Surveillance data, and Tagged clips. Only selected data types will be purged automatically. You must select at least one purge option data type.
Configure a Manual Purge button	Click this to manually purge data from the repository.
Purge status	Shows whether a purge is currently being initiated.

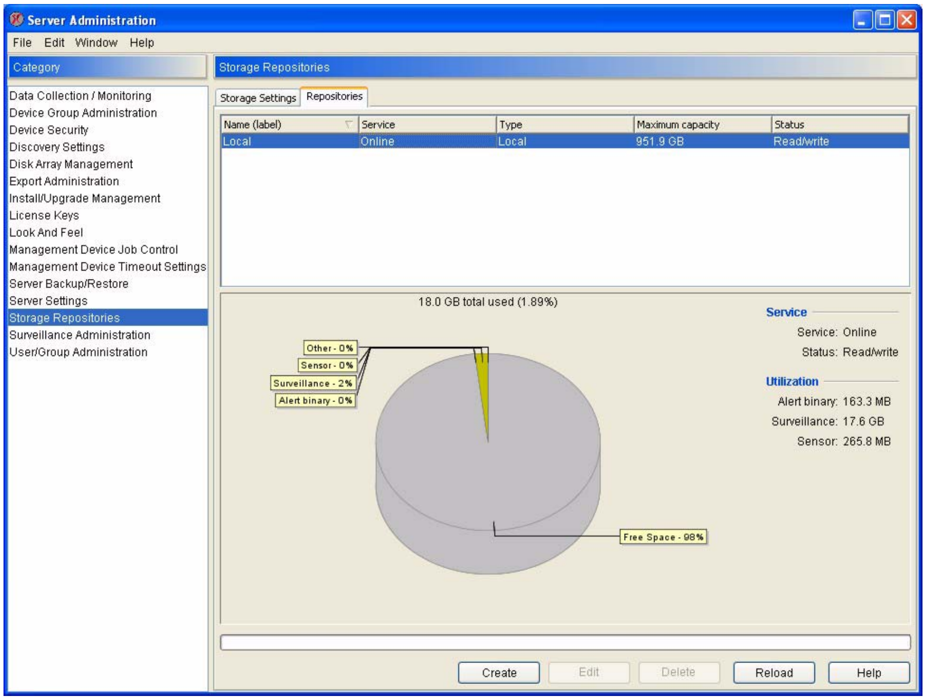
Purging Data Manually

To manually purge data from the InfraStruXure Central database, click on the Configure a Manual Purge button to open the Purge Data window. When the Purge Data window opens, use the calendar controls to specify a date range for which data will be purged, and then check the check boxes that correspond to the data types that will be purged during manual purge. The available data types are: Alert binary data, Sensor data, Surveillance data, and Tagged clips. Only selected data types will be purged. You must select at least one purge option data type. Then, click Run Purge to purge the data from the repository.

After data is deleted the Purge Data window will close and the disk space utilization values in the Storage Settings pane window will be updated.

The Repositories Pane

The Repositories pane features a list of all currently defined storage repositories. Initially only one entry, Local, will appear in this list. The Local repository corresponds to the on-board hard drive storage that is included with your InfraStruXure Central server. However, you can add additional remote storage repositories using network attached storage (such as an NFS mount or Windows share).



Name (label)	Service	Type	Maximum capacity	Status
Local	Online	Local	951.9 GB	Read/write

Service

Service: Online
Status: Read/write

Utilization

Alert binary: 163.3 MB
Surveillance: 17.6 GB
Sensor: 265.8 MB

To add a remote repository (or edit a previously created share):

1. Click Create (or select a previously created share and click Edit).
2. Select the type of repository you would like to create. You can choose either Unix/NFS or Windows.

- If you selected Unix/NF, provide the following information to define the NFS mount:

Field	Description
Name (label)	A name that will be used to identify this repository in the Storage Repository task interface.
Server host name or IP	The hostname or IP address of the NAS.
Share path	The name of the NFS mount on the NAS.

Field	Description
Subdirectory (optional)	The subdirectory in the NFS mount that will be used to store data. If no subdirectory is specified, data will be stored in the root directory of the mount.
Enabled check box	Check this check box to enable this remote repository for use with your InfraStruXure Central server.
Read-only check box	Check this check box to set this repository to read-only. Data will not be written to repositories that are set to read-only.
Maximum capacity	Use the controls to specify the maximum size of the remote repository.

- If you selected Windows, provide the following information to define the Windows share:

Field	Description
Name (label)	A name that will be used to identify this repository in the Storage Repository task interface.
Server host name or IP	The hostname or IP address of the Windows share.
User name	The user name required to access the Windows share.
Password / Verify password	The Password that is required to access the Windows share.
Domain	The domain to which the Windows share is connected.
Remote share name	The name of the Windows share.
Subdirectory (optional)	The subdirectory in the Windows share that will be used to store data. If no subdirectory is specified, data will be stored in the root directory of the share.
Enabled check box	Check this check box to enable this remote repository for use with your InfraStruXure Central server.
Read-only check box	Check this check box to set this repository to read-only. Data will not be written to repositories that are set to read-only.
Maximum capacity	Use the controls to specify the maximum size of the remote repository.
Use all available space check box	If checked, the device will not delete data from the share until all available space on the share has been exhausted. If unchecked, use the Limit space to (MB) and Allocation Unit controls to specify how much space on the share will be allocated for use by the device.

3. If you wish to test the share settings, click Test.

Note When editing a previously created share, the Test button will be grayed out unless the share has been disabled. You must first disable the share (select the share, click Edit, uncheck the Enabled check box, and click OK) before you will be able to test any changes made to the share settings without saving them.

4. Click OK to save your repository.

Surveillance Administration

The Surveillance Administration task enables you to license (or unlicense) devices for use with Surveillance, specify general Surveillance settings, and configure Surveillance Activation settings (such as Surveillance Capture Mode, Capture Rate, and Surveillance Event Duration settings). You can also configure motion masks and block out masks for licensed devices that support these features. For complete information on Surveillance, see “Surveillance View” on page 267.

User/Group Administration

Use the selections available from the User/Group Administration task to create or modify local user accounts and local user groups for your InfraStruXure Central server, to configure your InfraStruXure Central server to connect with use an external LDAP server, and to view a list of users that are currently logged into the InfraStruXure Central server. Local user accounts on your InfraStruXure Central server are allowed access only to specified device groups

User/Group Administration also enables you to create local user groups. Local user groups are collections of local user accounts. When local user accounts are added, you can simply add the new local user account to a previously defined local user group. You can also create local user groups that automatically enable full administrator privileges for any local users that are added to the group, or that enable users to use a SOCKS proxy to access devices on both the public network and the internal DHCP LAN (or “private” LAN) when enabled.

InfraStruXure Central’s built-in LDAP support enables you to configure your InfraStruXure Central server to connect with an LDAP server (such as MicroSoft Active Directory) and automatically access and set permissions for LDAP user accounts.

Creating and Editing Local User Accounts

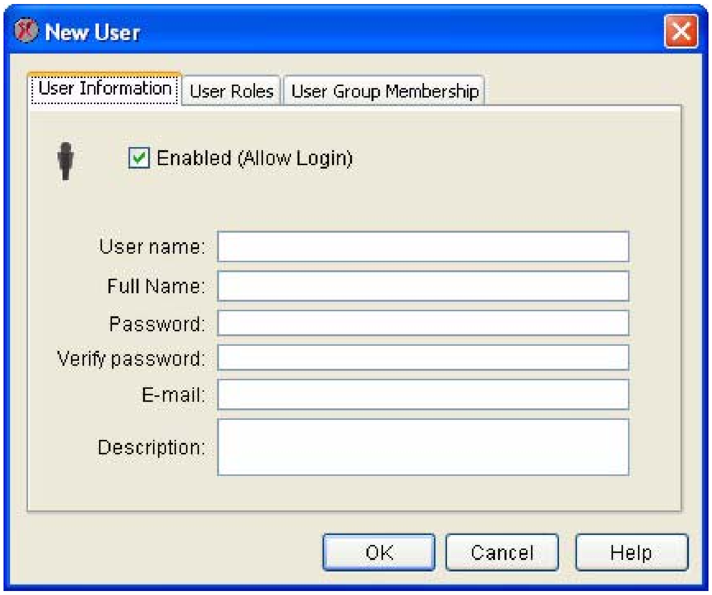
To create a new local user account, or to edit a previously defined local user account:

1. Start the User/Group Administration task and then select the Local Users tab. A list of all currently defined local user accounts is displayed, featuring the User Name, Full Name, and e-mail address associated with each account.

2. To create a new user account, click Create. To edit a previously defined user account select the account and then click Edit.

3. The Create User (or Edit User, if you are editing a previously created account) window appears. This window consists of 3 tabbed panes: The User Information pane, the User Roles pane, and the

User Group Membership pane.



4. Select the User Information tab. The fields in this pane enable you to define the user account login and identification information. This pane features the following fields:

Field	Description
Enabled check box	Check this check box to enable this local user account. Accounts that are disabled will not able to log into the InfraStruXure Central server.
User name	The user name that will be used to log into the InfraStruXure Central server.
Full name	The full name of the person to whom this user account is assigned.
Password/Verify password	The password that will be used, along with the user name, to log into the appliance.
E-mail address	The e-mail address of the user to whom this user account is assigned.
Description	A description of the local user account.

5. Select the User Roles tab. The controls on this pane enable you to enable full administrator privileges and/or SOCKS proxy to access devices on both the public network and the internal DHCP LAN (or “private” LAN) when enabled for this local user account. This pane features two

controls:

Field	Description
InfraStruXure Central administrator check box	Check this check box to give this local user account full administrator access to the InfraStruXure Central server. Administrators have complete monitoring and management access to all InfraStruXure Central server functionality. **Note:** This setting overrides any device group-specific privileges you may have set for local user accounts using the Device Group Administration task.
InfraStruXure Central proxy access check box	Check this check box to enable SOCKS proxy to access devices on both the public network and the internal DHCP LAN (or “private” LAN) -- when enabled -- for this user account. **Note:** This role is only used when your InfraStruXure Central is configured to use its built-in internal DHCP LAN with physical infrastructure devices that are connected to a private LAN. This functionality is enabled with the Server Settings task. **Important:** When enabling the internal DHCP LAN, the private LAN connection must be connected to LAN Port 2 on your InfraStruXure Central appliance. Once this feature is enabled, ensure that LAN Port 2 is NOT connected to a public LAN. Enabling this functionality on an InfraStruXure Central with LAN Port 2 connected to a public LAN will result in serious network connectivity issues.

6. Select the User Group Membership tab. The controls on this pane enable you to add the user account to one or more of the previously defined user groups. If this is a new user account, no user groups will be listed in this pane. If you are editing a previously created user account, this window will display a list of all user groups of which this user account is a member.
   – To add this user account to a previously defined user group, click Add User Group and select the desired user group from the Add User Group Access window, and then click OK.
   – To remove this user account from a user group to which it was previously added, select the user group from which you want to remove this user account and then click Remove User Group.
7. Click OK to finish creating or editing this local user account.

Creating and Editing Groups

You can use local user groups to quickly and easily organize your local user accounts into groups for simplified user account management. Local user groups can also be created that automatically enable full administrator access to all InfraStruXure Central functionality on all local user accounts that are added to the local user group.

To create a user group, or to edit a previously defined user group:

1. Start the User/Group Administration task and then select the Local User Groups tab. A list of all currently defined local user groups is displayed.
2. To create a new user group, click Create. To edit a previously defined user group select the user group and then click Edit.
3. The New User Group (or Edit User Group, if you are editing a previously created account) window appears. This window consists of 3 tabbed panes: The Group Information pane, the Group Roles

pane, and the Group Members pane.

4. Select the Group Information pane and type in the Group name field a name that will be associated with this local user group.
5. Select the Group Roles pane. The controls on this pane enable you to configure the local group to automatically enable full administrator privileges and/or SOCKS proxy to access devices on both the public network and the internal DHCP LAN (or “private” LAN) when enabled for any local users that are added to the group. This pane features two controls:

Field	Description
InfraStruXure Central administrator check box	Check this check box to give members of this user group full administrator access to the InfraStruXure Central server. Administrators have complete monitoring and management access to all InfraStruXure Central server functionality. **Note:** This setting overrides any device group-specific privileges you may have set for local user accounts using the Device Group Administration task.
InfraStruXure Central proxy access check box	Check this check box to enable SOCKS proxy to access devices on both the public network and the internal DHCP LAN (or “private” LAN) -- when enabled -- for any local users that are added to the group. **Note:** This role is only used when your InfraStruXure Central is configured to use its built-in internal DHCP LAN with physical infrastructure devices that are connected to a private LAN. This functionality is enabled with the Server Settings task. **Important:** When enabling the internal DHCP LAN, the private LAN connection must be connected to LAN Port 2 on your InfraStruXure Central appliance. Once this feature is enabled, ensure that LAN Port 2 is NOT connected to a public LAN. Enabling this functionality on an InfraStruXure Central with LAN Port 2 connected to a public LAN will result in serious network connectivity issues.

6. Select the Group Members pane. This pane features a list of local user accounts that are members of this local user group. To add a local user account to this local user group, click Add User, select one or more previously defined local user accounts from the Choose User(s) pane, and then click OK.
7. Click OK to save your local user group settings.

Using Remote Authentication Server Support

InfraStruXure Central features support for using LDAP servers in your network to define InfraStruXure Central user accounts. To add a remote LDAP server:

1. Select the Remote Authentication tab and then click Create. You will need to provide the following

information about the LDAP server:

Field	Description
Server label	The name that will be used when referring to this Remote Remote Authentication entry.
LDAP server type	Select the type of LDAP server you will be using from the drop box. You can select Active Directory or Open LDAP.
Server hostname	The hostname or IP address of the LDAP server.
Port	The port number used for communications with the LDAP server. The default port number for LDAP is 389.
Use SSL check box	Check to enable SSL communications between the console and the LDAP server.

2. When you have finished entering data, click Next to continue configuring the Remote Authentication settings. The following fields appear in the next window:

Field	Description
Bind user DN	The user DN required to bind to the LDAP server.
Bind password/Verify bind password	The password required to bind to the LDAP server.
Search Base	To narrow the search scope and decrease directory lookup time, provide an LDAP search base, if possible.

3. When you have finished entering data, click Next to continue configuring the Remote Authentication settings.
4. Next, specify which LDAP authorized users and user groups can access InfraStruXure Central. When you have finished click Finish.

Monitoring Currently Logged-In Users

To view a list of all InfraStruXure Central users that are currently logged into the InfraStruXure Central server, click the Logged In Users tab. This pane features a list of all currently logged in user accounts, as well as the full name associated with each account, the time at which the account logged into the appliance, and the DNS name or IP address from which the account is logged in.

Adding New Devices

Use the **Add...** selection in the Map and Table view context menus to add management devices and SNMP devices to your device groups.

Adding a Management Device

To add a new management device, select **New -> Management device** from the Map or Table view context menu. Then, provide the IP address or the hostname of the device you wish to add and the TCP/IP port number to be used when communicating with the management device, and check the **Connect using SSL** check box if you wish to use SSL when communicating with the management device. When you have finished specifying this information, click **OK** to add the management device.

Adding an SNMP Device

To add a new SNMP device (which will be monitored using the Device Scanner functionality), select New -> SNMP device from the Map or Table view context menu. Then, provide the following information about the SNMP device:

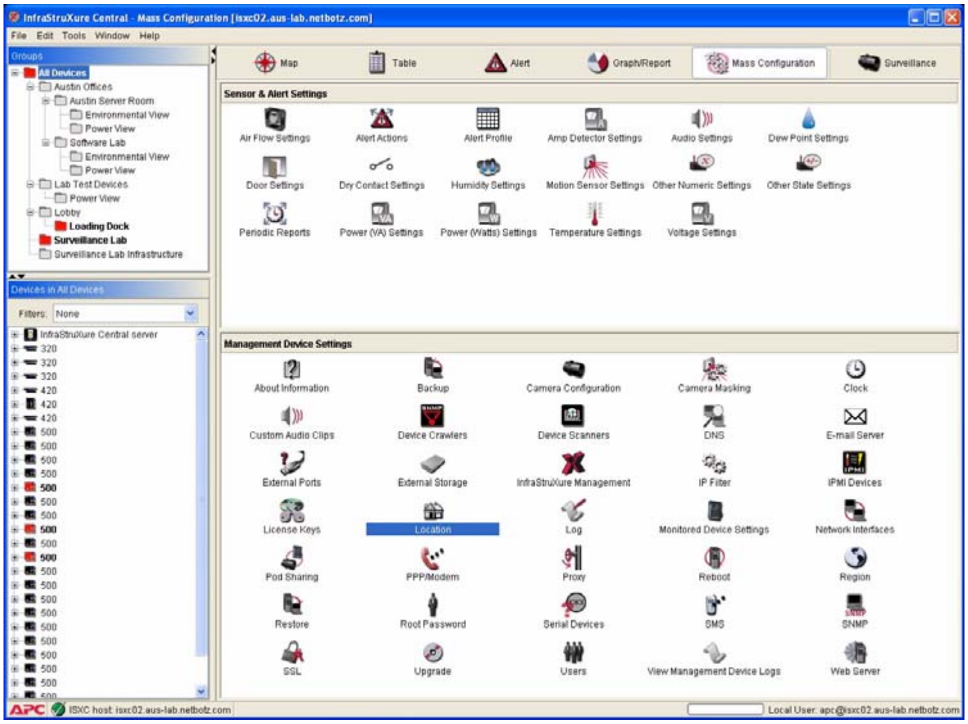
Field	Description
Hostname/IP address	Type in this field the hostname or IP address of the SNMP target.
Alert profile	Specify the Alert Profile that will be used to determine what alert notification actions will be taken in response to this threshold. By default, the Default Alert Profile is used for all thresholds. However, if you have created additional Alert Profiles you can specify that a threshold use an Alert Profile other than Default. **Note:** The Alert Profile drop box will appear in the Advanced tab only if additional Alert Profiles have been created.
Scan interval	Use this control to specify a device-specific scan interval for this device. The scan interval is the number of minutes that must pass between Device Scanner target queries. The default scan interval for all Device Scanner operations is specified using the Device Scanner Global SNMP Settings. For infomration Device Scanner Global SNMP Settings, see “Specifying Global SNMP Settings” on page 180.
Port	Type in this field the port number used for SNMP communications on the target. The default value is 161.
Timeout in seconds	Select the number of seconds that Device Scanner will wait for a response from a target before Device Scanner either retries communications or considers the target to be unresponsive. The default value is 30 seconds.
Retries	Select the number of times Device Scanner will retry communications with an SNMP target that is not responding before considering the target to be unresponsive and moving on to the next target.

Field	Description
Delete SNMP sensors if not found on crawled device	When checked, automatically removes previously defined SNMP-based sensors on a target when, after a successful scan, the sensors are found to no longer be present (no longer defined, unavailable, and so forth). If the sensors are not deleted, they will be displayed with sensor reading values of “N/A” or “null.”
Include network interface status	Check this check box to include the network status of the SNMP target in the list of sensors that are available for use on the target device.
Include network interface performance	If checked, Device Scanner will include network interface performance data in the list of sensors that are available for use on the target device.
SNMP Version	Select the version of SNMP that will be used to communicate with the target. You can select version 1, 2c, or 3.
Read community	Type in this field the read only community string used for SNMP communications on the target. The default value is public.

When you have finished specifying this information, click **OK** to add the SNMP device.

Mass Configuration: Sensor and Alert Settings

The selections available from the Mass Configuration view enable you perform mass configuration tasks on the NetBotz devices installed on your network. Use Mass Configuration tasks to set NetBotz device configuration settings, enable license-key based functionality to your devices, enable and disable alerts, set threshold values, configure device web interfaces, and to configure the alert actions and policies that will be used when alerts are reported by the sensors that are built into or connected to your devices. The individual tasks are divided into *Sensor and Alert Settings* and *Device Settings*. This chapter covers only the Sensor and Alert Settings tasks. For information regarding Device Settings tasks see “Mass Configuration: Device Settings” on page 159.



The tasks available from the Sensors and Alert Settings portion of the Mass Configuration panel enable you to configure the sensors that are built into or connected to your NetBotz devices and devices. Detailed information about the tasks available from the Sensors and Alert Settings portion of the Configuration panel follows.

Configuring Offline Devices

If a device goes offline, InfraStruXure Central will assume that the offline state is a temporary event. When a device is in an offline state you can still perform Mass Configuration tasks on the device. InfraStruXure Central will store these tasks in the Management Device Job Control queue, and will automatically perform the tasks as soon as the device comes back online.

Whenever you start a Mass Configuration task, the first window that is displayed shows a table of devices on which the selected task can be performed. This table features a Status column, in which the current status of each device is displayed. If a device is currently in an offline state the Status field for the device will read “Offline,” but you will still be able to enact Mass Configuration tasks on the device, just as if the device were online. When a Mass Configuration task is enacted against an offline device, the Status field will show that the task did not complete and is being retired automatically, and a small image of a clock is displayed to indicate that the configuration request against this device is currently in a pending state.

If InfraStruXure Central is unable to carry out a mass configuration task because a device is in an Offline state, it adds the task to the Pending Requests list (“Management Device Job Control” on page 89).

Managing BotzWare Version 1.x Devices

The Pod Sharing task enables you to use NetBotz 500 devices to receive data from legacy NetBotz devices running BotzWare 1.x (including RackBotz and WallBotz 300, 303, 310, 400, and 410 devices). Once a NetBotz 500 is configured to access these legacy models they are treated exactly like other shared pods or devices, providing alert and sensor data exactly as if they were directly connected to the NetBotz 500. For more information on Pod Sharing, see “Pod Sharing” on page 206.

About Sensor and Alert Settings Tasks

The majority of tasks that are available from the Sensor & Alert Settings pane enable you to configure the sensors that are built into or connected to your NetBotz devices. Each sensor threshold configuration task is named for the type of sensor with which the sensor will be used (temperature, air flow, humidity, and so forth).

The sensors used by your devices fall into two categories: Numeric sensors and state sensors. Numeric sensors report sensor readings as a current value within a broad range of potential values defined by a minimum and maximum value, such as temperature or humidity readings. State sensors, on the other hand, report sensor readings as one of two mutually exclusive states, such as a door being “open” or “closed” or motion being “detected” or “not detected.” Due to the differences in the kind of data reported by these two sensor types, the thresholds that can be applied to each sensor type differ greatly.

Each sensor threshold configuration task is named either a) for the type of sensor with which the sensor will be used (temperature, air flow, humidity, and so forth) or b) with a general name that describes the sort of sensor that is configured using the task. The sensor configuration tasks are:

- Air Flow Settings (to configure air flow sensors integrated with your devices)
- Amp Detector Settings (to configure amp detector sensors connected your devices)
- Audio Settings (to configure audio sensors integrated with your devices)
- Dew Point Settings (to configure dew point sensors integrated with your devices)
- Door Settings (to configure door switch sensors connected to your devices)
- Dry Contact Settings (to configure dry contact sensors connected to your devices)
- Humidity Settings (to configure humidity sensors integrated with or connected to your devices)
- Motion Sensor Settings (to configure the camera motion sensors integrated with your devices)
- Power (VA) Settings: Use the Power (VA) Settings to configure thresholds for your device volt amperage sensors.
- Power (Volts) Settings: Use the Power (Volts) Settings to configure thresholds for your device voltage sensors.

- Power (Watts) Settings: Use the Power (Watts) Settings to configure thresholds for your device wattage sensors.
- Temperature Settings (to configure temperature sensors integrated with or connected to your devices)
- Other Numeric Sensors (to configure any other numeric sensors that are connected to your devices, but that cannot be configured using the other sensor configuration tasks)
- Other State Sensors (to configure any other state sensors that are connected to your devices, but that cannot be configured using the other sensor configuration tasks)

Because all of these tasks are very similar from a user interface and interaction perspective, they are covered collectively in the subheading “Configuring Sensors and Thresholds” on page 130.

Alert Actions

Use the Alert Actions task to define Alert Actions for use in the individual Alert Sequences that make up the Alert Profile of your devices. When you create an Alert Action, you select a specific alert notification type (such as sending an e-mail notification, sending an SNMP trap, or posting the alert information to an HTTP server) and provide necessary configuration settings (such as an e-mail recipient’s address, the IP address of your SNMP trap recipient, or the IP address of your HTTP server) that will enable the Alert Action to be successfully carried out.

Available Alert Notification Methods

The Alert Actions interface consists of a series of tabbed panes, each of which corresponds to one of the available alert notification methods that can be configured using the Alert Actions task. An Alert Action consists of a single alert notification method and any specific information that is necessary to deliver the alert notification. NetBotz devices support the following alert notification methods:

- Activate Button Output: Triggers an output relay that has been defined as a Button Relay.
- Call Web Services Alert Receiver: Designed for use with the BotzWare Web Services Interface. The NetBotz BotzWare Web Services interfaces are intended to provide a set of common, programmer-friendly APIs to 3rd party product and solution developers, as well as end customers. For more information, see the BotzWare V2.x Web Services Specification PDF, included on your *BotzWare* CD and available from the NetBotz support web site.
- Play Audio Alert: Plays a description of the alert, in spoken language, through the headphones or powered speakers that are connected to a selected NetBotz Camera Pod 120.
- Play Custom Audio Alert: Plays a user-specified audio clip using the headphones or powered speakers that are connected to a selected Camera Pod 120 or CCTV Adapter Pod. Audio clips are uploaded to the device using the Custom Audio Clip task.
- Send Custom HTTP GET: Delivers alert notifications as custom HTTP GET commands. The URL generated as a result of the alert action is completely user definable, and can include BotzWare macro values.
- Send Custom Text File to FTP Server: Sends a customized text file with user-specified content to an FTP server. This alert action type enables you to use macros supported by BotzWare (including Device, Location, and Alert macros) to define the name of the directory on the server in which custom text files will be stored and the base filename that will be used for the text files.
- Send Data to FTP Server: Sends an alert notification that contains information about the nature of the alert to an FTP server. This alert action type enables you to use macros supported by BotzWare (including Device, Location, and Alert macros) to define the name of the directory on the server in

which data files will be stored and the base filename that will be used for FTP data files. For more information on macros supported by BotzWare, see “BotzWare Macros” on page 285.

- Send E-mail: Sends an alert notification e-mail that contains information about the nature of the alert to one or more e-mail recipients. The alert notification e-mail can optionally include images captured by the device (or by a NetBotz Camera Pod 120 connected to the device) and a graph of the sensor-specific data associated with the alert.
- Send HTTP Post: Sends an HTTP post to a specified HTTP server that contains information about the nature of the alert. The alert notification post can optionally include images captured by the device (or by a NetBotz Camera Pod 120 connected to the device) and a graph of the sensor-specific data associated with the alert.
- Send to InfraStruXure Central: Sends the alert notification information to this InfraStruXure Central server.
- Send Short Message E-mail: Sends a user-configurable alert notification in an e-mail format designed for use with devices that have limited display capabilities, such as cellular telephones and personal data assistants (PDAs). This alert action type enables you to use macros supported by BotzWare (including Device, Location, and Alert macros) to specify the contents of the title and body of the e-mail message. For more information on macros supported by BotzWare, see “BotzWare Macros” on page 285.
- Send Wireless SMS Message: Sends a short (up to 160 characters) alert notification using a wireless SMS connection. Available only if a modem that supports SMS messaging has been installed in or connected to the device.
- Set Switch Output State: Triggers an output relay that has been defined as a Switch Relay.
- Send SNMP v1 Trap: Sends an SNMP trap to a specified SNMP trap recipient that contains information about the nature of the alert.
- Sends an SNMP v3 inform to a specified SNMP recipient that contains information about the nature of the alert.

When an alert notification-specific tab is selected, any selected devices (or devices included in a selected device group) that have a defined Alert Action that corresponds to the selected notification method are listed.

Note

Only devices that have a currently defined Alert Action that corresponds to the selected alert notification method tab are displayed.

Creating Alert Actions

To create a new alert action:

1. Launch the Alert Actions task.
2. Select the alert notification-specific tab that corresponds to the type of alert action you want to create. Any selected devices that have previously been configured with an alert action that uses the selected alert notification method are displayed in the pane.
3. Click Add, then select one or more devices from the device selection list and click Next.
4. Specify notification information for this alert action. The information that must be provided for an alert action depends on which alert notification method you have selected. For detailed notification

method-specific instructions, see “Creating Alert Actions” on page 225.

5. Click OK to save this new Alert Action for use with all selected devices.

Once you have saved the Alert Action it will appear in the list of defined Alert Actions for the selected devices and will be available for use in the Alert Profiles task.

Editing Previously Defined Alert Actions

To edit a previously defined alert action:

1. Launch the Alert Actions task.
2. Select the alert notification-specific tab that corresponds to the type of alert action you want to create. Any selected devices that have previously been configured with an alert action that uses the selected alert notification method are displayed in the pane.
3. Select one or more devices and then click Edit.
4. Specify the new notification information for this Alert Action. The information that must be provided for an Alert Action depends on which alert notification method you have selected. For detailed notification method-specific instructions, see “Creating Alert Actions” on page 225.
5. Click OK to save this updated Alert Action for use with all selected devices.

Alert Profile

Use the Alert Profile task to customize alert notification policy used by your devices. You can customize your device’s default alert notification policy, or create additional alert notification policies to simplify alert management. You can also use the Alert Profile task to temporarily disable all alert notifications globally associated with an Alert Profile.

The alert policy defines the notification actions that are taken by the device in response to alert conditions. The alert profile consists of one or more alert sequences. An alert sequence specifies:

- The period of time that must pass before an alert condition results in notification.
- The number of times the notification will be repeated if the alert condition goes uncorrected.
- The time interval at which the notification is enacted
- One or more Alert Actions that are taken as part of the Alert Sequence's notification process
- The schedule that determines whether the Alert Sequence is active at the date and time that the alert occurs
- Capture settings that can be used to override specific alert-action attributes, such as including graphs or image captures with alert notifications

For more information about alert sequences, see “Creating an Alert Sequence” on page 118.

The Default Alert Profile

APC NetBotz appliances come pre-configured with a Default Alert Profile. This Default policy features the following 4 pre-configured Alert Sequences, all of which are scheduled to be active 24 hours a day, 7 days a week:

- Alert Level 1: Begins immediately after an alert condition occurs (Start Value of 0), repeats 2 times at a 5 minute interval. Initiates the following pre-defined Alert Actions: Primary E-Mail Notification, HTTP Post, FTP Data Delivery.

- Alert Level 2: Begins 20 minutes after an alert condition occurs, repeats 1 time at a 10 minute interval. Initiates the following pre-defined Alert Actions: Secondary E-Mail Notification, HTTP Post, FTP Data Delivery.
- Alert Level 3: Begins 90 minutes after an alert condition occurs, repeats 2 times at a 60 minute interval. Initiates the following pre-defined Alert Actions: Primary E-Mail Notification, Secondary E-Mail Notification, HTTP Post, FTP Data Delivery.
- Continuous Alert: Begins immediately after an alert condition occurs (Start Value of 0), repeats indefinitely at a 1 minute interval. Initiates the following pre-defined Alert Actions: Send SNMP Trap.

Note

Pre-defined Alert Actions or individual sensor Thresholds may require additional information (such as e-mail addresses, server IP addresses, output devices, etc.) for notifications to be successfully delivered. Be sure to adequately configure Alert Actions and Thresholds that will be used in your Alert Profile.

The Default Alert Profile can be edited, but it cannot be Removed. When sensor thresholds are created, the Default Alert Profile will be used unless you use Advanced Threshold Settings to specify otherwise. In many cases, the Default Alert Profile will adequately meet your alert management needs. However, you can also create additional Alert Profiles if needed.

Note

The Default Alert Profile is always used for alerts generated when pods are unplugged or go offline.

Creating an Alert Sequence

To create a new Alert Sequence (or modify a previously created Alert Sequence):

1. Double-click on the Alert Profile icon.
2. Click Add.... If you are modifying a previously created Alert Sequence, select from the Sequence table the desired Alert Sequence and then click Edit....
3. Type in the Label field a name for the Alert Sequence.
4. Type in the Start field (or use the arrow buttons in the field to select) the number of minutes that must pass before an alert condition results in the notification specified by this Alert Sequence. For example, if you want notifications to begin only if the alert condition has gone uncorrected for 5 minutes or more, specify a Start Time of 5 minutes. If you want notifications to begin immediately, specify a Start Time of 0.
5. Check the Repeat Until Normal check box if you want the Alert Actions specified by this Alert Sequence to be repeated automatically until the alert condition no longer exists. If you want the actions to be repeated only a specific number of times, then leave this check box unchecked and instead use the Repeats value to specify how many times to repeat the actions
6. (Optional) Check the Automatically add new alert actions to this schedule check box if you want any new Alert Actions created after this Alert Schedule is defined to be automatically added to this schedule.
7. Type in the Repeats field (or use the arrow buttons in the field to select) the number of times that the notifications specified by this Alert Sequence will be repeated. This field will not be available if the

Repeat Until Normal check box is checked.

8. Type in the Interval field (or use the arrow buttons in the field to select) the number of seconds that will pass between repeated notifications in this Alert Sequence.
9. Specify Capture Settings for Graphs and Pictures associated with this Alert Sequence. Capture settings can be used to override the Maximum Camera Pictures and Include a Graph with the Alert settings for all Alert Actions that you associate with this Alert Sequence.

   By default, alert sequence Capture Settings are set to Capture if requested, which indicates that this alert sequence will capture graphs and pictures if alert actions are configured to request them (i.e. if the Maximum Camera Pictures setting is greater than 0 or the Include a Graph with the Alert check box is checked). While this setting ensures that pictures and graphs are included with alert notifications, in some circumstances you may wish to receive images or graphs only from some alert sequences (such as the initial alert notification), or you might want to preserve graphs and images on the appliance even if they are not included with alert notifications.

   Rather than creating multiple copies of the same Alert Action, some which enable the inclusion of camera pictures and graphs and some that do not, you can just create one Alert Action (for example, e-mail) and use the capture controls to override the Alert Action settings as follows:

   – Set the Graph or Picture Capture Settings to Never capture. When Capture Settings are set to Never capture, images or graphs are not included with any alert actions that are associated with the alert sequence, regardless of the Maximum Camera Pictures and Include a Graph with the Alert settings for the alert actions.

   – Set the Graph or Picture Capture Settings to Always capture. When Capture Settings are set to Always capture, images or graphs are always captured by the appliance, even if the Maximum Camera Pictures and Include a Graph with the Alert settings for the individual alert actions are not set to capture this data. While this data will not be included with the alert notifications associated with your alert actions, the images and graphs associated with the alerts will be available for use via the Alerts View.

Note

Don't forget that images will only be captured and included in an alert notification, regardless of Capture Settings, if you have checked at least one Cameras to Trigger check box when defining a threshold.

1. Specify the Alert Actions that will be carried out as part of this Alert Sequence. Click Add Actions..., and then select one or more Alert Actions from the Add Action window. Click OK to add the selected actions to your Alert Sequence.
2. Click OK to save the Alert Sequence to your Alert Profile.

Creating an Alert Profile

To create a new Alert Profile (or modify a previously created Alert Profile):

1. Double-click on the Alert Profile icon.
2. Click Add.... If you are modifying a previously created Alert Profile, select from the Profile table the desired Alert Profile and then click Edit....
3. Type in the Label field a name for the new Alert Profile.
4. Create one (or more) Alert Sequences for use with this Alert Profile.
5. Click OK to save the Alert Profile.

Suppressing Alert Notifications

You can also use the Alert Profile task to temporarily suppress all alert notifications associated with an Alert Profile. This temporarily prevents your appliance from generating any alert notifications associated with the selected Alert Profile until a time and date you specify. Once enabled, alert notifications will not be generated -- even if an enabled threshold is violated. Once the specified time and date arrives alert notifications will resume normally.

Note

- Disabling alert notifications prevents your appliance from automatically notifying you of conditions that may be hazardous to your critical assets and spaces. This task is designed for use only when scheduled maintenance or downtime would result in your appliance generating alert notifications in response to environmental conditions that you are aware of and are expecting to occur for brief periods of time.
- When alert notifications are disabled, enabled sensors in the Sensor Readings pane will continue to turn red to provide a visual indication that a threshold has been crossed.

To globally disable alert notifications:

1. Select the Alert Profile for which you wish to globally disable alert notifications from the Alert Profile window and then click Edit....
2. Select the Advanced tab.
3. Check the Suppress alert notifications until check box.
4. Use the calendar control to specify the date and time of day at which alert notification functionality will resume.
5. Click OK to suppress all alert notifications from the appliance.

Periodic Reports

Use the Periodic Reports task to configure your devices to generate sensor reading reports and deliver them to e-mail recipients, HTTP servers, or FTP servers on a user-specified schedule. These reports contain the current readings for all sensors built into or connected to your devices.

The Periodic Reports interface consists of a series of view, selected using the Periodic Reports drop box, each of which corresponds to one of the available report generation methods that can be configured using the Periodic Reports task. NetBotz devices support the following alert notification methods:

- Periodic Report to InfraStruXure Central: Reports current sensor readings to this InfraStruXure Central server.
- HTTP Periodic Report: Posts the current sensor readings to an HTTP server.
- FTP Periodic Report: Send a report containing a complete list of the of the current sensor readings to a specified FTP server.
- E-mail Periodic Report: Generates and sends a complete report of the current sensor settings using e-mail.

When you select a report generation method from the Periodic Reports drop box any selected devices (or devices included in a selected device group) that have a defined Periodic Report that corresponds to the selected report generation method are listed.

Note

Only devices that have a currently defined Periodic Report entry that corresponds the selected report generation method tab are displayed.

Configuring a Periodic Report Entry

To create a new Periodic Report entry:

1. Select a device group or container from the navigation pane, or select one or more devices from the device list pane.
2. Double-click on the Periodic Report icon.
3. Select from the Periodic Reports drop box the report generation method that corresponds to the type of periodic report entry that you want to create. Any selected devices that have previously been configured with a Periodic Report entry uses the selected report generation method are displayed.
4. Click Add, then select one or more NetBotz devices from the device selection list and click Next.
5. Specify periodic report generation and delivery information for this Periodic Report entry. The information that must be provided for each specific Periodic Report entry depends on which report generation method you have selected. For detailed notification method-specific instructions, see the method-specific instructions which follow.
6. Click OK to save this new Periodic Report entry for all selected devices.

Configuring a Periodic Report to InfraStruXure Central Entry

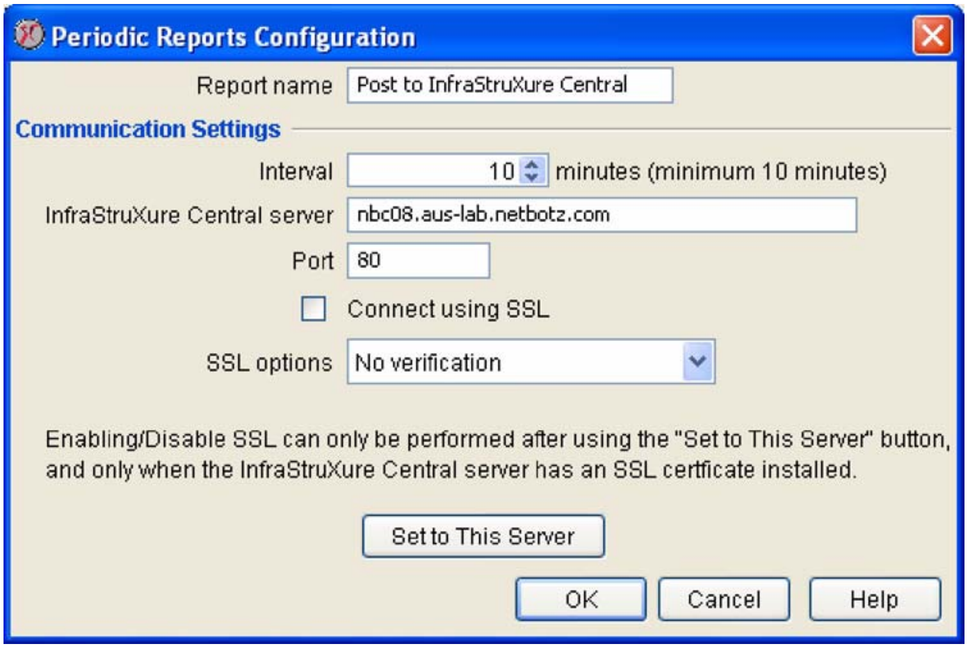
To configure devices to periodically generate and send sensor reports to this InfraStruXure Central server:

1. Select a device group from the navigation pane, or select one or more devices from the device list pane.
2. Double-click on the Periodic Reports icon.
3. Select Periodic Report to InfraStruXure Central from the Periodic Reports drop box. Any selected devices with previously created report generation entries of this type are displayed.
4. Click Add, then select one or more devices from the selection list and click Next.
5. A Periodic Report configuration interface window opens. This window contains the following

fields:

Field	Description
Report Name	A name for this report. Used to identify the report in the Periodic Reports task window.
Interval	The frequency with which reports will be generated.
InfraStruXure Central server	The IP address or hostname of the InfraStruXure Central server to which this report will be sent.
Port	The IP port on which the InfraStruXure Central server is configured to communicate.
Connect using SSL check box	Check this check box to use SSL when communicating with this server.
SSL options	Select from this drop-box the SSL options that will be used for this report.
Set to This Server button	Click Set to This Server to automatically send the report to the InfraStruXure Central server to with which you are currently communicating.

6. Type the appropriate values in the fields.



Periodic Reports Configuration

Report name: Post to InfraStruXure Central

Communication Settings

Interval: 10 minutes (minimum 10 minutes)

InfraStruXure Central server: nbc08.aus-lab.netbotz.com

Port: 80

□ Connect using SSL

SSL options: No verification

Enabling/Disable SSL can only be performed after using the "Set to This Server" button, and only when the InfraStruXure Central server has an SSL certficate installed.

7. When you are finished, click OK to save any changes to the device. Click Cancel to close this window without saving any changes.

Configuring an HTTP Periodic Report

To configure your devices to periodically generate and post sensor reports to a specified HTTP server:

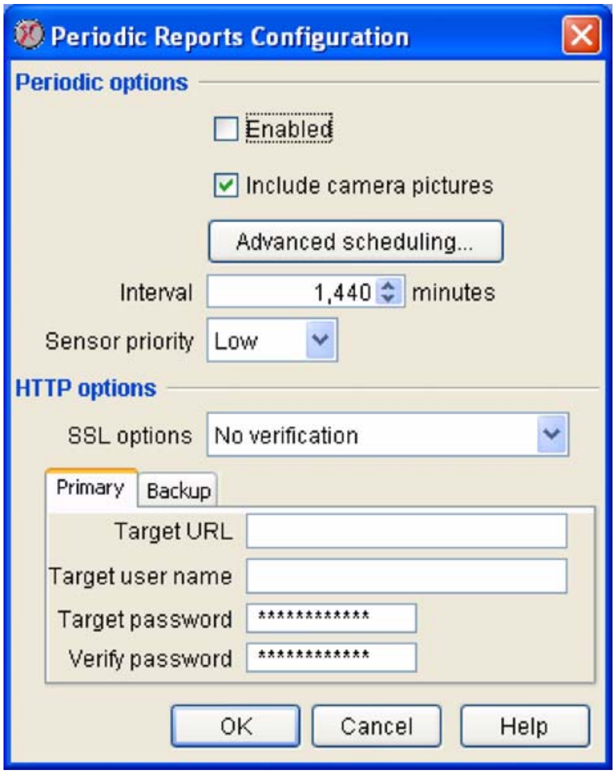
1. Select a device group from the navigation pane, or select one or more devices from the device list

pane.

2. Double-click on the Periodic Reports icon.
3. Select HTTP Periodic Report the Periodic Reports drop box. Any selected devices with previously created report generation entries of this type are displayed.
4. Click Add, then select one or more NetBotz devices from the device selection list and click Next.
5. A Periodic Report configuration interface window opens. This window contains the following fields:

Field	Description
Enabled	Check this check box to enable periodic HTTP reporting.
Include camera pictures	Check this check box to include current image captures by cameras connected to or integrated with your devices in the HTTP post. Image captures that are included with periodic reports are 640x480 resolution, regardless of appliance Camera settings.
Interval	The frequency with which HTTP reports will be generated.
Sensor priority	Acts as a filter that can be used to limit the amount of sensor data that is included with the periodic report. You can select High, Medium, or Low priority settings: • High: Only sensor data associated with physical sensors that are integrated with or connected to the appliance are included in the report. Sensor data associated with remote devices, such as MIB II data gathered from remote targets using Basic Device Crawlers and Advanced Data that is gathered using add-on applications such as Advanced Device Crawlers, is not included in the report. • Medium: Sensor data associated with physical sensors and with Advanced Data sensor sets from remote devices (such as that which is gathered using Advanced Device Crawlers) is included in the report. Data associated with remote devices that is not grouped in an Advanced Data sensor set, such as MIB II data gathered from remote targets using Basic Device Crawlers, is not included in the report. • Low: Sensor data from all sensors is included in the report.
SSL options	Select from this drop-box the SSL options that will be used for this post.
Target URL	The URL of the web server to which the report will be posted.
Target user name	The user name that will be used, along with the Target password, to gain access to the specified web server.
Target password	The password that will be used, along with the Target user name, to gain access to the specified web server.
Verify password	Type the Target password here again to confirm the password.

This window features Primary and Backup tabs, each of which has the same fields available. The settings specified on the Primary tab are used by default for any periodic HTTP reports. The settings on the Backup pane are used if communication with the Primary server fails.



☐ Enabled

☑ Include camera pictures

Interval 1,440 minutes

Sensor priority Low

SSL options No verification

Target URL

Target user name

Target password ************

Verify password ************

6. Type the appropriate values in the fields.
7. Specify Advanced Scheduling for the Periodic Report (optional). By default, all Periodic Reports will be generated according to the Interval value you specify. However, you can specify that a Periodic Report will be active only occur during specific time ranges. To configure Advanced Scheduling:
   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.
   b. By default, all time periods in the schedule are set to Enabled. To disable the Periodic Report for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Periodic Report for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.
   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Periodic Report task.
8. When you are finished, click OK to save this entry to selected devices. Click Cancel to close this window without saving any changes.

Configuring an FTP Periodic Report

To configure your devices to periodically generate and deliver sensor reports to a specified FTP server:

1. Select a device group from the navigation pane, or select one or more devices from the device list pane.
2. Double-click on the Periodic Reports icon.
3. Select FTP Periodic Report the Periodic Reports drop box. Any selected devices with previously

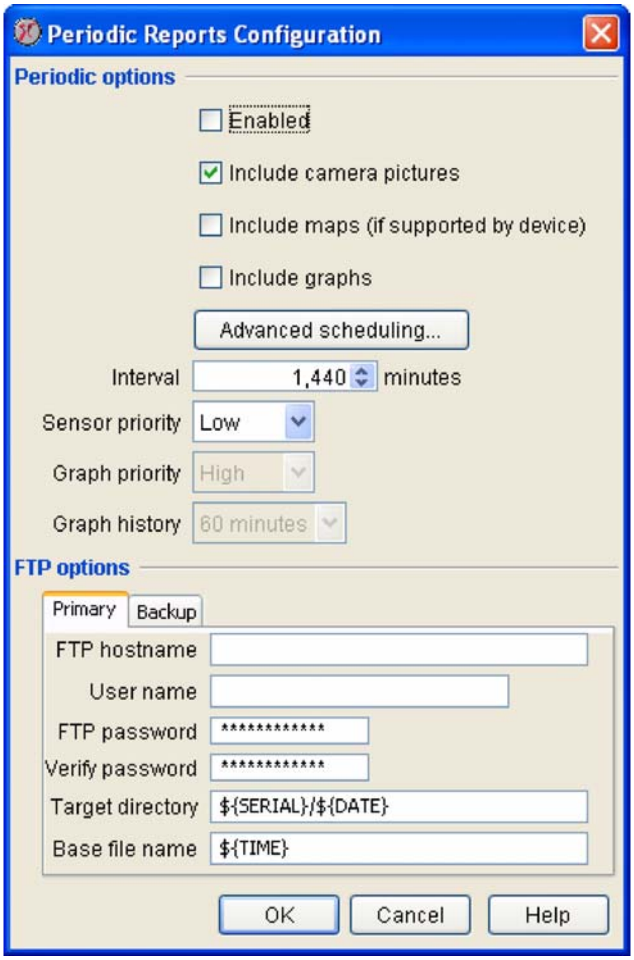
created report generation entries of this type are displayed.

4. Click Add, then select one or more NetBotz devices from the device selection list and click Next.
5. A Periodic Report configuration interface window opens. This window contains the following fields:

Field	Description
Enabled	Check this check box to enable periodic FTP reporting.
Include camera pictures	Check this check box to include current image captures by cameras connected to or integrated with your devices in the FTP post. Image captures that are included with periodic reports are 640x480 resolution, regardless of appliance Camera settings.
Include maps	Check this check box to include any maps that are stored on the appliance in the FTP post.
Include graphs	Check this check box to include graphs of the sensor readings for all sensors that are associated with the appliance in the FTP post.
Interval	The frequency with which FTP reports will be generated.
Sensor priority	Acts as a filter that can be used to limit the amount of sensor data that is included with the periodic report. You can select High, Medium, or Low priority settings: • High: Only sensor data associated with physical sensors that are integrated with or connected to the appliance are included in the report. Sensor data associated with remote devices, such as MIB II data gathered from remote targets using Basic Device Crawlers and Advanced Data that is gathered using add-on applications such as Advanced Device Crawlers, is not included in the report. • Medium: Sensor data associated with physical sensors and with Advanced Data sensor sets from remote devices (such as that which is gathered using Advanced Device Crawlers) is included in the report. Data associated with remote devices that is not grouped in an Advanced Data sensor set, such as MIB II data gathered from remote targets using Basic Device Crawlers, is not included in the report. • Low: Sensor data from all sensors is included in the report.

Field	Description
Graph priority	Acts as a filter that can be used to limit the amount of sensor data that is graphed and included in the periodic report. You can select High, Medium, or Low priority settings: • High: Only sensor data associated with physical sensors that are integrated with or connected to the appliance will be graphed and included in the report. Sensor data associated with remote devices, such as MIB II data gathered from remote targets using Basic Device Crawlers and Advanced Data that is gathered using add-on applications such as Advanced Device Crawlers, is not included in the graph. • Medium: Sensor data associated with physical sensors and with Advanced Data sensor sets from remote devices (such as that which is gathered using Advanced Device Crawlers) will be graphed and included in the report. Data associated with remote devices that is not grouped in an Advanced Data sensor set, such as MIB II data gathered from remote targets using Basic Device Crawlers, is not included in the graph. • Low: Sensor data from all sensors will be graphed and included in the report.
Graph history	Specifies the maximum time period for which data will be graphed.
FTP Hostname	The hostname or IP address of the FTP server to which the report will be delivered.
User name	The user name that will be used, along with the FTP password, to gain access to the specified FTP server.
FTP password	The password that will be used, along with the User name, to gain access to the specified FTP server.
Verify password	Type the FTP password here again to confirm the password.
Target Directory	The relative directory path to be used for storing the data on the FTP server. This should always be a path relative to the default directory associated with the user ID used to log on to the FTP server. If the directories on the path do not exist they will be created automatically. The Target Directory field accepts macros. The Target directory field accepts macros. For more information on macros supported by BotzWare, see “BotzWare Macros” on page 285.
Base Filename	The base filename to be used for storing the data on the FTP server. The alert data will be stored in a file with this name, followed by the “.nbalert” file extension. Pictures from alerts will be stored in files with this name, followed by the “.n.jpg” file extension, where n is the picture number (1, 2, 3, etc.). The Base Filename field accepts macros. For more information on macros supported by BotzWare, see “BotzWare Macros” on page 285.

This window features Primary and Backup tabs, each of which has the same fields available. The settings specified on the Primary tab are used by default for any periodic FTP reports. The settings on the Backup pane are used if communication with the Primary server fails.



Periodic Reports Configuration

Periodic options

□ Enabled

☑ Include camera pictures

□ Include maps (if supported by device)

□ Include graphs

Interval 1,440 minutes

Sensor priority Low

Graph priority High

Graph history 60 minutes

FTP options

FTP hostname

User name

FTP password ************

Verify password ************

Target directory ${SERIAL}/${DATE}

Base file name ${TIME}

6. Type the appropriate values in the fields.
7. Specify Advanced Scheduling for the Periodic Report (optional). By default, all Periodic Reports will be generated according to the Interval value you specify. However, you can specify that a Periodic Report will be active only occur during specific time ranges. To configure Advanced Scheduling:
   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.
   b. By default, all time periods in the schedule are set to Enabled. To disable the Periodic Report for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Periodic Report for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.
   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Periodic Report task.
8. When you are finished, click OK to save this entry to selected devices. Click Cancel to close this window without saving any changes.

Configuring an E-mail Periodic Report

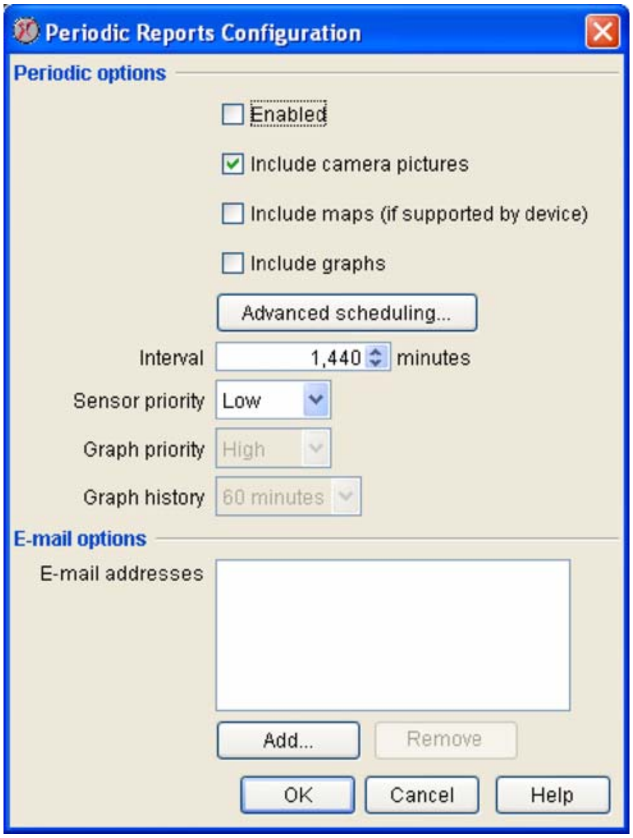
To configure devices to periodically generate and e-mail sensor reports to specified recipients:

1. Select a device group or container from the navigation pane, or select one or more devices from the device list pane.
2. Double-click on the Periodic Reports icon.
3. Select the E-Mail Periodic Report from the Periodic Reports drop box. Any selected devices with previously created report generation entries of this type are displayed.
4. Click Add, then select one or more NetBotz devices from the device selection list and click Next.
5. A Periodic Report configuration interface window opens. This window contains the following fields:

Field	Description
Enabled	Check this check box to enable periodic e-mail reporting.
Include camera pictures	Check this check box to include current image captures by Camera Pod 120s connected to the NetBotz device in the e-mailed report. Image captures that are included with periodic reports are 640x480 resolution, regardless of appliance Camera settings.
Include maps	Check this check box to include any maps that are stored on the appliance in the e-mailed report.
Include graphs	Check this check box to include graphs of the sensor readings for all sensors that are associated with the appliance in the e-mailed report.
Interval	The frequency with which e-mail reports will be generated.
Sensor priority	Acts as a filter that can be used to limit the amount of sensor data that is included with the periodic report. You can select High, Medium, or Low priority settings: • High: Only sensor data associated with physical sensors that are integrated with or connected to the appliance are included in the report. Sensor data associated with remote devices, such as MIB II data gathered from remote targets using Basic Device Crawlers and Advanced Data that is gathered using add-on applications such as Advanced Device Crawlers, is not included in the report. • Medium: Sensor data associated with physical sensors and with Advanced Data sensor sets from remote devices (such as that which is gathered using Advanced Device Crawlers) is included in the report. Data associated with remote devices that is not grouped in an Advanced Data sensor set, such as MIB II data gathered from remote targets using Basic Device Crawlers, is not included in the report. • Low: Sensor data from all sensors is included in the report.

Field	Description
Graph priority	Acts as a filter that can be used to limit the amount of sensor data that is graphed and included in the periodic report. You can select High, Medium, or Low priority settings: • High: Only sensor data associated with physical sensors that are integrated with or connected to the appliance will be graphed and included in the report. Sensor data associated with remote devices, such as MIB II data gathered from remote targets using Basic Device Crawlers and Advanced Data that is gathered using add-on applications such as Advanced Device Crawlers, is not included in the graph. • Medium: Sensor data associated with physical sensors and with Advanced Data sensor sets from remote devices (such as that which is gathered using Advanced Device Crawlers) will be graphed and included in the report. Data associated with remote devices that is not grouped in an Advanced Data sensor set, such as MIB II data gathered from remote targets using Basic Device Crawlers, is not included in the graph. • Low: Sensor data from all sensors will be graphed and included in the report.
Graph history	Specifies the maximum time period for which data will be graphed.
E-mail addresses	The addresses to which periodic e-mail reports will be delivered.

6. Type the appropriate values in the fields.



Periodic Reports Configuration

Periodic options

☐ Enabled

☑ Include camera pictures

☐ Include maps (if supported by device)

☐ Include graphs

Advanced scheduling...

Interval 1,440 minutes

Sensor priority Low

Graph priority High

Graph history 60 minutes

E-mail options

E-mail addresses

7. Specify Advanced Scheduling for the Periodic Report (optional). By default, all Periodic Reports will be generated according to the Interval value you specify. However, you can specify that a Periodic Report will be active only occur during specific time ranges. To configure Advanced Scheduling:
   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.
   b. By default, all time periods in the schedule are set to Enabled. To disable the Periodic Report for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Periodic Report for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.
   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Periodic Report task.

When you are finished, click OK to save this entry to selected devices. Click Cancel to close this window without saving any changes.

Configuring Sensors and Thresholds

The majority of tasks that are available from the Sensor & Alert Settings pane enable you to configure the sensors that are built into or connected to your NetBotz devices. Each sensor threshold configuration task is named for the type of sensor with which the sensor will be used (temperature, air flow, humidity, and so forth).

Each sensor threshold configuration task is named either a) for the type of sensor with which the sensor will be used (temperature, air flow, humidity, and so forth) or b) with a general name that describes the sort of sensor that is configured using the task. The sensor configuration tasks are:

- Air Flow Settings (to configure air flow sensors integrated with your devices)
- Amp Detector Settings (to configure amp detector sensors connected your devices)
- Audio Settings (to configure audio sensors integrated with your devices)
- Dew Point Settings (to configure dew point sensors integrated with your devices)
- Door Settings (to configure door switch sensors connected to your devices)
- Dry Contact Settings (to configure dry contact sensors connected to your devices)
- Humidity Settings (to configure humidity sensors integrated with or connected to your devices)
- Motion Sensor Settings (to configure the camera motion sensors integrated with your devices)
- Power (VA) Settings (to configure your device volt amperage sensors)
- Power (Volts) Settings (to configure your device voltage sensors)
- Power (Watts) Settings (to configure your device wattage sensors)
- Temperature Settings (to configure temperature sensors integrated with or connected to your devices)
- Other Numeric Sensors (to configure any other numeric sensors that are connected to your devices, but that cannot be configured using the other sensor configuration tasks)
- Other State Sensors (to configure any other state sensors that are connected to your devices, but that cannot be configured using the other sensor configuration tasks)

Numeric and State Sensors: Definitions

The sensors used by your devices fall into two categories: Numeric sensors and state sensors. Numeric sensors report sensor readings as a current value within a broad range of potential values defined by a minimum and maximum value, such as temperature or humidity readings. State sensors, on the other hand, report sensor readings as one of two mutually exclusive states, such as a door being “open” or “closed” or motion being “detected” or “not detected.” Due to the differences in the kind of data reported by these two sensor types, the thresholds that can be applied to each sensor type differ greatly.

The interface for each sensor-specific threshold configuration task consists of a series of panes, each of which corresponds to a different threshold type that is available for use with that sensor and device. When you select a threshold-specific tab, any thresholds of that type that have been configured on any selected devices are displayed in the task pane.

Specifying Sensor Labels and History Settings

Use the Sensor Configuration window to specify a unique identification label for a sensor or to specify the total amount of data from the selected sensor that will be preserved on your NetBotz devices. To specify a label for a sensor, or to specify the total amount of time that data reported by a selected sensor should be stored on the device:

1. Select a device group from the navigation pane, or select one or more devices from the device list pane.
2. Right-click on the Sensor Settings icon that corresponds to the type of sensor that for which you will

edit the label or history settings and then select Label/History Settings from the context menu.

3. Select one or more NetBotz devices from the device selection list and then click Edit.
4. Type in the Label field a label to identify this sensor. This label can be up to 64 characters in length, and will be used to identify the sensor in alert notifications.
5. Select from the Sensor Value History drop box the total amount of time that data reported by this sensor should be stored on the device. The total amount of data available on the device affects the maximum amount of data that can be graphed.
6. Click OK to save the new Sensor values. Click Cancel to close this window without saving any changes.

Numeric Sensors and Thresholds

The following Sensor & Alert Settings tasks enable you to configure thresholds on numeric-based sensors:

- Air Flow Settings
- Amp Detector Settings
- Audio Setting
- Dew Point Settings
- Humidity Settings
- Power (VA) Settings
- Power (Volts) Settings
- Power (Watts) Settings
- Temperature Settings
- Other Numeric Settings

The following threshold types can be assigned to any numeric sensor:

- Maximum Value Threshold: An alert condition occurs if the current sensor value exceeds a specified acceptable value.
- Minimum Value Threshold: An alert condition occurs if the current sensor value falls below a specified acceptable value.
- Range Threshold: An alert condition occurs if the current sensor value is not within a specified range of acceptable values.
- Above Value for Time Threshold: An alert condition occurs when the current sensor value exceeds a specified value for a specified amount of time.
- Below Value for Time Threshold: An alert condition occurs when the current sensor value falls below a specified value for a specified amount of time.
- Rate of Decrease Threshold: An alert condition occurs if the value reported by the sensor decreases more than a specified amount within a specified amount of time.
- Rate of Increase Threshold: An alert condition occurs if the value reported by the sensor rises more than a specified amount within a specified amount of time.

State Sensors and Thresholds

The following Sensor & Alert Settings tasks enable you to configure thresholds on state-based sensors:

- Door Settings
- Dry Contact Settings
- Motion Sensor Setting
- Other State Settings

The following threshold types can be assigned to any state sensor:

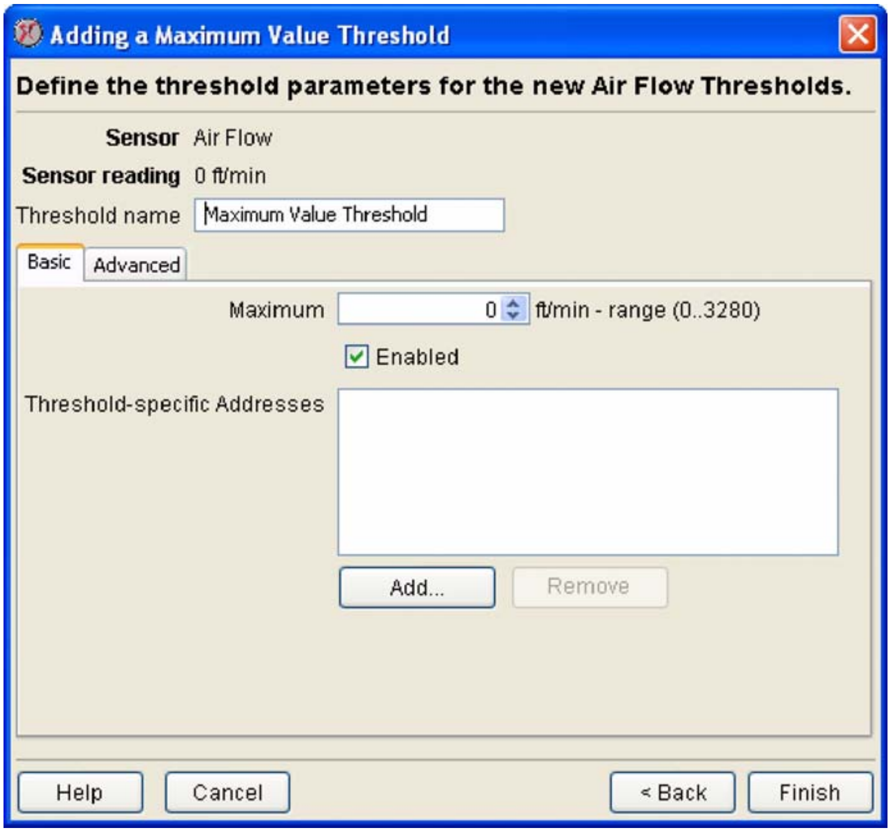
- Alert State Threshold: An alert condition occurs if a specified state is reported by the sensor.
- Alert State for Time Threshold: An alert condition occurs if a specified state is reported by the sensor for more than a specified time.
- State Mismatch Threshold: An alert condition occurs if any state other than the “normal” state is reported by the sensor.
- State Mismatch for Time Threshold: An alert condition occurs if any state other than the “normal” state is reported by the sensor for more than the specified time.

Defining Numeric Thresholds

Detailed instructions on how to define each of the available numeric threshold types follow.

Maximum Value Threshold

A maximum value threshold is defined by specifying a maximum acceptable value for selected sensors. If the value reported by the sensor exceeds the specified value an alert condition is reported.


Adding a Maximum Value Threshold

Define the threshold parameters for the new Air Flow Thresholds.

Sensor: Air Flow
Sensor reading: 0 ft/min
Threshold name: Maximum Value Threshold

Maximum: 0 ft/min - range (0..3280)
☑ Enabled
Threshold-specific Addresses

To define a maximum value threshold:

1. Launch the Sensor & Alert Settings task that corresponds to the numeric-based sensor for which you will define a threshold.
2. Select Maximum Value Threshold from the Threshold drop box. Any selected devices that have previously defined maximum value thresholds will be listed in the Management Devices list.
3. Select the desired threshold operation and targets:
   – If you are editing one or more previously defined maximum value thresholds, select the devices on which the threshold has been configured from the Management Devices list and then click Edit.

   – If you are defining a new maximum threshold click Add. Then, select one or more devices for which this threshold will be configured, and click Next. Finally, select the sensors on the selected devices for which this threshold will be configured and then click Next.
4. Type in the Threshold Name field a name for this threshold.
5. Specify Basic threshold settings. From the Basic tab in the Thresholds pane:
   a. Type in the Maximum field (or use the arrows in the field to specify) the highest acceptable value for the selected sensors. This is the value that, if exceeded, will result in an alert condition.
   b. Check the Enabled check box to enable the threshold. If this check box is not checked, the alert threshold will be saved but will not be active.

   Add to the Threshold-Specific Addresses list the e-mail addresses of any personnel to whom e-mail alert notifications should be sent if this threshold triggers an alert condition. Click Add..., type in the e-mail address to which the alert notification will be sent, and then click OK.

   If you’ve installed an SMS-capable modem you can deliver alert notification to SMS-enabled devices by entering threshold-specific addresses for them in the following format:

   sms:sms_device_address

   where *sms_device_address* is the telephone number or e-mail address associated with the SMS-enabled device (for example, “sms:5123334444” or “sms:user@mycorp.com”).

   Note: These threshold-specific notifications are sent only if your device has one or more Alert Actions defined that use the Send E-Mail Message alert notification method and that have the Include Addresses from Thresholds check box checked. For more information, see “Alert Actions” on page 115 and “Creating Alert Actions” on page 225.

6. If desired, specify Advanced Threshold settings. All Advanced threshold settings are optional. From the Advanced tab in the Thresholds pane:
   – Specify a Return To Normal Delay value. Use the controls to specify the number of seconds that must pass after this threshold has returned to normal before the threshold state is considered returned to normal. Default value is 0 (state returns to normal immediately after the measured value is no longer violating the threshold).

   – Set an Advanced Schedule for this threshold (optional). By default, all thresholds are assumed to be enabled 24 hours a day, 7 days a week. However, you can specify that a threshold will be enabled only during specific time ranges. To set an Advanced Schedule:

   a. Click Advanced Schedule.... The Schedule Threshold window opens.

b. By default, all time periods in the schedule are set to Enabled. To disable the threshold for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the threshold for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

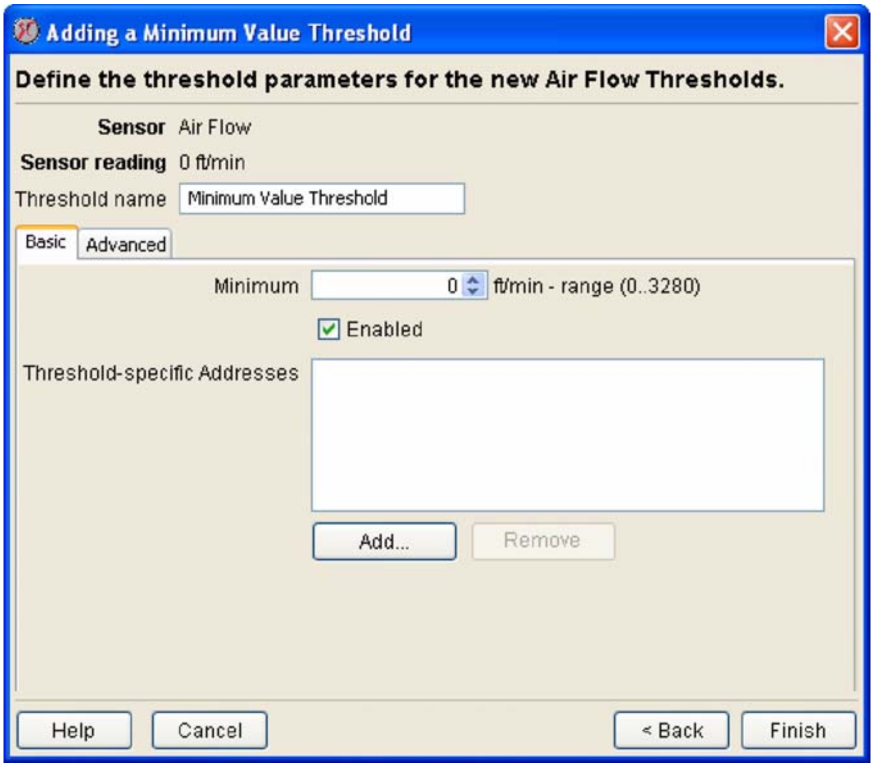
c. When you have finished creating your Advanced Threshold, click OK to save the schedule and return to the Thresholds task.

- Select an Alert Severity value for this threshold. Available Alert Severities are, in order of escalating severity: Information, Warning, Error, Critical, or Failure. By default, the Alert Severity generated by this threshold will be “Error.”
- Select Cameras to Trigger in response to the alert. To include images from one or more connected NetBotz Camera Pod 120s, check the check boxes that correspond to the desired pods.
- Specify a User-specified URL and User-specified Description. You can use these fields to include additional user-specific information with any alert notifications that are generated using this threshold.
- Check the Return-To-Normal Requires User Input check box. When checked, if this threshold is exceeded the sensor will not report a Return-To-Normal state until a user with Administrator or Application (with Alert Update) privileges opens the resulting alert entry in the Alerts View and clicks the Mark Alert Resolved button.

7. Click Finish to save this threshold.

Minimum Value Threshold

A minimum value threshold is defined by specifying a minimum acceptable value for selected sensors. If the value reported by the sensor falls below the specified value an alert condition is reported.



Adding a Minimum Value Threshold

Define the threshold parameters for the new Air Flow Thresholds.

Sensor Air Flow

Sensor reading 0 ft/min

Threshold name Minimum Value Threshold

Minimum 0 ft/min - range (0..3280)

☑ Enabled

Threshold-specific Addresses

To define a minimum value threshold:

1. Launch the Sensor & Alert Settings task that corresponds to the numeric-based sensor for which you will define a threshold.
2. Select Minimum Value Threshold from the Threshold drop box. Any selected devices that have previously defined minimum value thresholds will be listed in the Management Devices list.
3. Select the desired threshold operation and targets:

   – If you are editing one or more previously defined minimum value thresholds, select the devices on which the threshold has been configured from the Management Devices list and then click Edit.

   – If you are defining a new minimum threshold click Add. Then, select one or more devices for which this threshold will be configured, and click Next. Finally, select the sensors on the selected devices for which this threshold will be configured and then click Next.
4. Type in the Threshold Name field a name for this threshold.
5. Specify Basic threshold settings. From the Basic tab in the Thresholds pane:

   a. Type in the Minimum field (or use the arrows in the field to specify) the lowest acceptable value for the selected sensors. This is the value that, if fallen below, will result in an alert condition.

   b. Check the Enabled check box to enable the threshold. If this check box is not checked, the alert threshold will be saved but will not be active.

   Add to the Threshold-Specific Addresses list the e-mail addresses of any personnel to whom e-mail alert notifications should be sent if this threshold triggers an alert condition. Click Add..., type in the e-mail address to which the alert notification will be sent, and then click OK.

   If you’ve installed an SMS-capable modem you can deliver alert notification to SMS-enabled devices by entering threshold-specific addresses for them in the following format:

   sms:sms_device_address

   where *sms_device_address* is the telephone number or e-mail address associated with the SMS-enabled device (for example, “sms:5123334444” or “sms:user@mycorp.com”).

Note

These threshold-specific notifications are sent only if your device has one or more Alert Actions defined that use the Send E-Mail Message alert notification method and that have the Include Addresses from Thresholds check box checked. For more information, see “Alert Actions” on page 115 and “Creating Alert Actions” on page 225.

6. If desired, specify Advanced Threshold settings. All Advanced threshold settings are optional. From the Advanced tab in the Thresholds pane:

   – Specify a Return To Normal Delay value. Use the controls to specify the number of seconds that must pass after this threshold has returned to normal before the threshold state is considered returned to normal. Default value is 0 (state returns to normal immediately after the measured value is no longer violating the threshold).

   – Set an Advanced Schedule for this threshold (optional). By default, all thresholds are assumed to be enabled 24 hours a day, 7 days a week. However, you can specify that a threshold will be enabled only during specific time ranges. To set an Advanced Schedule:

   a. Click Advanced Schedule.... The Schedule Threshold window opens.

b. By default, all time periods in the schedule are set to Enabled. To disable the threshold for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the threshold for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

c. When you have finished creating your Advanced Threshold, click OK to save the schedule and return to the Thresholds task.

– Select an Alert Severity value for this threshold. Available Alert Severities are, in order of escalating severity: Information, Warning, Error, Critical, or Failure. By default, the Alert Severity generated by this threshold will be “Error.”

– Select Cameras to Trigger in response to the alert. To include images from one or more connected NetBotz Camera Pod 120s, check the check boxes that correspond to the desired pods.

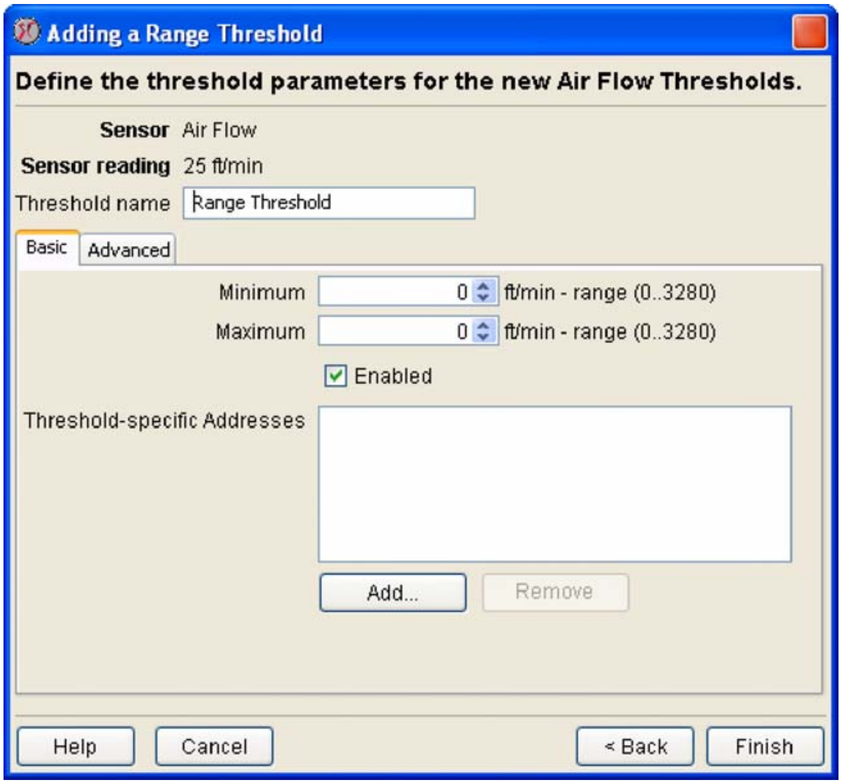
– Specify a User-specified URL and User-specified Description. You can use these fields to include additional user-specific information with any alert notifications that are generated using this threshold.

– Check the Return-To-Normal Requires User Input check box. When checked, if this threshold is exceeded the sensor will not report a Return-To-Normal state until a user with Administrator or Application (with Alert Update) privileges opens the resulting alert entry in the Alerts View and clicks the Mark Alert Resolved button.

7. Click Finish to save this threshold.

Range Threshold

A range threshold is defined by defining an acceptable range of values for selected sensors by specifying a minimum and maximum value. If the value reported by the sensor falls outside of the limits defined by the range an alert condition is reported.


Adding a Range Threshold

Define the threshold parameters for the new Air Flow Thresholds.

Sensor Air Flow
Sensor reading 25 ft/min
Threshold name Range Threshold

Minimum 0 ft/min - range (0..3280)
Maximum 0 ft/min - range (0..3280)
☑ Enabled
Threshold-specific Addresses

To define a range threshold:

1. Launch the Sensor & Alert Settings task that corresponds to the numeric-based sensor for which you will define a threshold.
2. Select Range Threshold from the Threshold drop box. Any selected devices that have previously defined range thresholds will be listed in the Management Devices list.
3. Select the desired threshold operation and targets:
   - – If you are editing one or more previously defined range thresholds, select the devices on which the threshold has been configured from the Management Devices list and then click Edit.
   - – If you are defining a new range threshold click Add. Then, select one or more devices for which this threshold will be configured, and click Next. Finally, select the sensors on the selected devices for which this threshold will be configured and then click Next.
4. Type in the Threshold Name field a name for this threshold.
5. Specify Basic threshold settings. From the Basic tab in the Thresholds pane:
   a. Type in the Maximum field (or use the arrows in the field to specify) the highest acceptable value for the selected sensors. This is the value that defines the upper limit of the acceptable range for this sensor. If the sensor reading exceeds this value an alert condition results.
   b. Type in the Minimum field (or use the arrows in the field to specify) the lowest acceptable value for the selected sensors. This is the value that defines the lower limit of the acceptable range for this sensor. If the sensor reading falls below this value an alert condition results.
   c. Check the Enabled check box to enable the threshold. If this check box is not checked, the alert threshold will be saved but will not be active.

   Add to the Threshold-Specific Addresses list the e-mail addresses of any personnel to whom e-mail alert notifications should be sent if this threshold triggers an alert condition. Click Add..., type in the e-mail address to which the alert notification will be sent, and then click OK.

   If you’ve installed an SMS-capable modem you can deliver alert notification to SMS-enabled devices by entering threshold-specific addresses for them in the following format:

   sms:sms_device_address

   where *sms_device_address* is the telephone number or e-mail address associated with the SMS-enabled device (for example, “sms:5123334444” or “sms:user@mycorp.com”).

   Note: These threshold-specific notifications are sent only if your device has one or more Alert Actions defined that use the Send E-Mail Message alert notification method and that have the Include Addresses from Thresholds check box checked. For more information, see “Alert Actions” on page 115 and “Creating Alert Actions” on page 225.

6. If desired, specify Advanced Threshold settings. All Advanced threshold settings are optional. From the Advanced tab in the Thresholds pane:
   - – Specify a Return To Normal Delay value. Use the controls to specify the number of seconds that must pass after this threshold has returned to normal before the threshold state is considered returned to normal. Default value is 0 (state returns to normal immediately after the measured value is no longer violating the threshold).
   - – Set an Advanced Schedule for this threshold (optional). By default, all thresholds are assumed to be enabled 24 hours a day, 7 days a week. However, you can specify that a threshold will be enabled only during specific time ranges. To set an Advanced Schedule:

a. Click Advanced Schedule.... The Schedule Threshold window opens.

b. By default, all time periods in the schedule are set to Enabled. To disable the threshold for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the threshold for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

c. When you have finished creating your Advanced Threshold, click OK to save the schedule and return to the Thresholds task.

– Select an Alert Severity value for this threshold. Available Alert Severities are, in order of escalating severity: Information, Warning, Error, Critical, or Failure. By default, the Alert Severity generated by this threshold will be “Error.”

– Select Cameras to Trigger in response to the alert. To include images from one or more connected NetBotz Camera Pod 120s, check the check boxes that correspond to the desired pods.

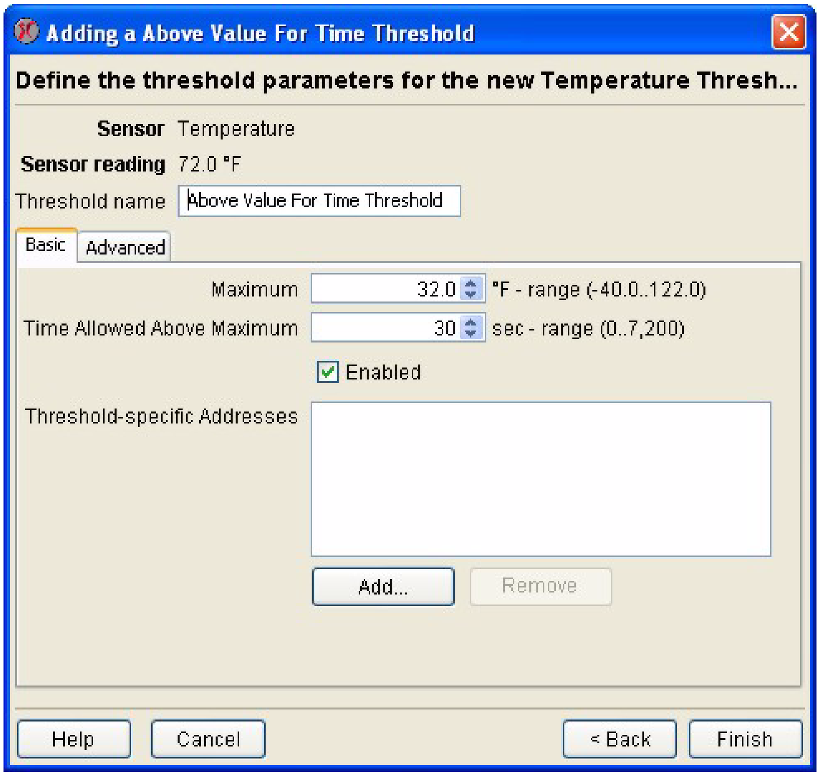
– Specify a User-specified URL and User-specified Description. You can use these fields to include additional user-specific information with any alert notifications that are generated using this threshold.

– Check the Return-To-Normal Requires User Input check box. When checked, if this threshold is exceeded the sensor will not report a Return-To-Normal state until a user with Administrator or Application (with Alert Update) privileges opens the resulting alert entry in the Alerts View and clicks the Mark Alert Resolved button.

7. Click OK to save this threshold.

Above Value for Time Threshold

An above value for time threshold is defined by specifying a maximum acceptable value for selected sensors and a maximum period of time value. If the value reported by the sensor exceeds the specified value for more than the specified period of time an alert condition is reported.



Adding a Above Value For Time Threshold

Define the threshold parameters for the new Temperature Thresh...

Sensor Temperature

Sensor reading 72.0 °F

Threshold name Above Value For Time Threshold

Maximum 32.0 °F - range (-40.0..122.0)

Time Allowed Above Maximum 30 sec - range (0..7,200)

☑ Enabled

Threshold-specific Addresses

To define an above value for time threshold:

1. Launch the Sensor & Alert Settings task that corresponds to the numeric-based sensor for which you will define a threshold.
2. Select Above Value for Time Threshold from the Threshold drop box. Any selected devices that have previously defined above value for time thresholds will be listed in the Management Devices list.
3. Select the desired threshold operation and targets:
   - If you are editing one or more previously defined above value for time thresholds, select the devices on which the threshold has been configured from the Management Devices list and then click Edit.
   - If you are defining a new above value for time threshold click Add. Then, select one or more devices for which this threshold will be configured, and click Next. Finally, select the sensors on the selected devices for which this threshold will be configured and then click Next.
4. Type in the Threshold Name field a name for this threshold.
5. Specify Basic threshold settings. From the Basic tab in the Thresholds pane:
   a. Type in the Maximum field (or use the arrows in the field to specify) the highest acceptable value for the selected sensors. This is the value that, if exceeded for greater than the number of seconds specified in the Time Allowed Above Maximum field, will result in an alert condition.

b. Type in the Time Allowed Above Maximum field (or use the arrows in the field to specify) the number of seconds that the reported value can exceed the value specified in the Maximum field before an alert condition is generated.

c. Check the Enabled check box to enable the threshold. If this check box is not checked, the alert threshold will be saved but will not be active.

Add to the Threshold-Specific Addresses list the e-mail addresses of any personnel to whom e-mail alert notifications should be sent if this threshold triggers an alert condition. Click Add..., type in the e-mail address to which the alert notification will be sent, and then click OK.

If you’ve installed an SMS-capable modem you can deliver alert notification to SMS-enabled devices by entering threshold-specific addresses for them in the following format:

sms:sms_device_address

where *sms_device_address* is the telephone number or e-mail address associated with the SMS-enabled device (for example, “sms:5123334444” or “sms:user@mycorp.com”).

Note

These threshold-specific notifications are sent only if your device has one or more Alert Actions defined that use the Send E-Mail Message alert notification method and that have the Include Addresses from Thresholds check box checked. For more information, see “Alert Actions” on page 115 and “Creating Alert Actions” on page 225.

6. If desired, specify Advanced Threshold settings. All Advanced threshold settings are optional. From the Advanced tab in the Thresholds pane:

– Specify a Return To Normal Delay value. Use the controls to specify the number of seconds that must pass after this threshold has returned to normal before the threshold state is considered returned to normal. Default value is 0 (state returns to normal immediately after the measured value is no longer violating the threshold).

– Set an Advanced Schedule for this threshold (optional). By default, all thresholds are assumed to be enabled 24 hours a day, 7 days a week. However, you can specify that a threshold will be enabled only during specific time ranges. To set an Advanced Schedule:

a. Click Advanced Schedule....The Schedule Threshold window opens.

b. By default, all time periods in the schedule are set to Enabled. To disable the threshold for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the threshold for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

c. When you have finished creating your Advanced Threshold, click OK to save the schedule and return to the Thresholds task.

– Select an Alert Severity value for this threshold. Available Alert Severities are, in order of escalating severity: Information, Warning, Error, Critical, or Failure. By default, the Alert Severity generated by this threshold will be "Error."

– Select Cameras to Trigger in response to the alert. To include images from one or more connected NetBotz Camera Pod 120s, check the check boxes that correspond to the desired pods.

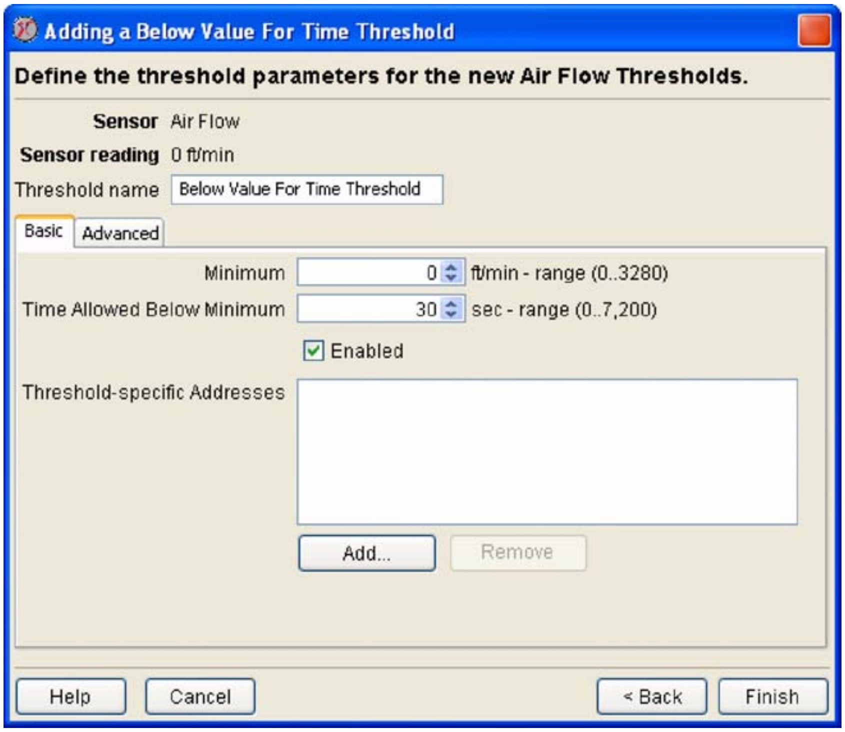
– Specify a User-specified URL and User-specified Description. You can use these fields to include additional user-specific information with any alert notifications that are generated using this threshold.

– Check the Return-To-Normal Requires User Input check box. When checked, if this threshold is exceeded the sensor will not report a Return-To-Normal state until a user with Administrator or Application (with Alert Update) privileges opens the resulting alert entry in the Alerts View and clicks the Mark Alert Resolved button.

7. Click OK to save this threshold.

Below Value for Time Threshold

A below value for time threshold is defined by specifying a minimum acceptable value for selected sensors and a maximum period of time value. If the value reported by the sensor falls below the specified value for more than the specified period of time an alert condition is reported.



Adding a Below Value For Time Threshold

Define the threshold parameters for the new Air Flow Thresholds.

Sensor Air Flow

Sensor reading 0 ft/min

Threshold name Below Value For Time Threshold

Minimum 0 ft/min - range (0..3280)

Time Allowed Below Minimum 30 sec - range (0..7,200)

☑ Enabled

Threshold-specific Addresses

To define a below value for time threshold:

1. Launch the Sensor & Alert Settings task that corresponds to the numeric-based sensor for which you will define a threshold.

2. Select Below Value for Time Threshold from the Threshold drop box. Any selected devices that have previously defined below value for time thresholds will be listed in the Management Devices

list.

3. Select the desired threshold operation and targets:

   – If you are editing one or more previously defined below value for time thresholds, select the devices on which the threshold has been configured from the Management Devices list and then click Edit.

   – If you are defining a new below value for time threshold click Add. Then, select one or more devices for which this threshold will be configured, and click Next. Finally, select the sensors on the selected devices for which this threshold will be configured and then click Next.

4. Type in the Threshold Name field a name for this threshold.

5. Specify Basic threshold settings. From the Basic tab in the Thresholds pane:

   a. Type in the Minimum field (or use the arrows in the field to specify) the highest acceptable value for the selected sensors. This is the value that, if fallen below for greater than the number of seconds specified in the Time Allowed Below Minimum field, will result in an alert condition.

   b. Type in the Time Allowed Below Minimum field (or use the arrows in the field to specify) the number of seconds that the reported value can fall below the value specified in the Minimum field before an alert condition is generated.

   c. Check the Enabled check box to enable the threshold. If this check box is not checked, the alert threshold will be saved but will not be active.

   Add to the Threshold-Specific Addresses list the e-mail addresses of any personnel to whom e-mail alert notifications should be sent if this threshold triggers an alert condition. Click Add..., type in the e-mail address to which the alert notification will be sent, and then click OK.

   If you've installed an SMS-capable modem you can deliver alert notification to SMS-enabled devices by entering threshold-specific addresses for them in the following format:

   sms:sms_device_address

   where *sms_device_address* is the telephone number or e-mail address associated with the SMS-enabled device (for example, "sms:5123334444" or "sms:user@mycorp.com").

Note

These threshold-specific notifications are sent only if your device has one or more Alert Actions defined that use the Send E-Mail Message alert notification method and that have the Include Addresses from Thresholds check box checked. For more information, see "Alert Actions" on page 115 and "Creating Alert Actions" on page 225.

6. If desired, specify Advanced Threshold settings. All Advanced threshold settings are optional. From the Advanced tab in the Thresholds pane:

   – Specify a Return To Normal Delay value. Use the controls to specify the number of seconds that must pass after this threshold has returned to normal before the threshold state is considered returned to normal. Default value is 0 (state returns to normal immediately after the measured value is no longer violating the threshold).

   – Set an Advanced Schedule for this threshold (optional). By default, all thresholds are assumed to be enabled 24 hours a day, 7 days a week. However, you can specify that a threshold will be enabled only during specific time ranges. To set an Advanced Schedule:

   a. Click Advanced Schedule.... The Schedule Threshold window opens.

   b. By default, all time periods in the schedule are set to Enabled. To disable the threshold for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the threshold for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

c. When you have finished creating your Advanced Threshold, click OK to save the schedule and return to the Thresholds task.

– Select an Alert Severity value for this threshold. Available Alert Severities are, in order of escalating severity: Information, Warning, Error, Critical, or Failure. By default, the Alert Severity generated by this threshold will be "Error."

– Select Cameras to Trigger in response to the alert. To include images from one or more connected NetBotz Camera Pod 120s, check the check boxes that correspond to the desired pods.

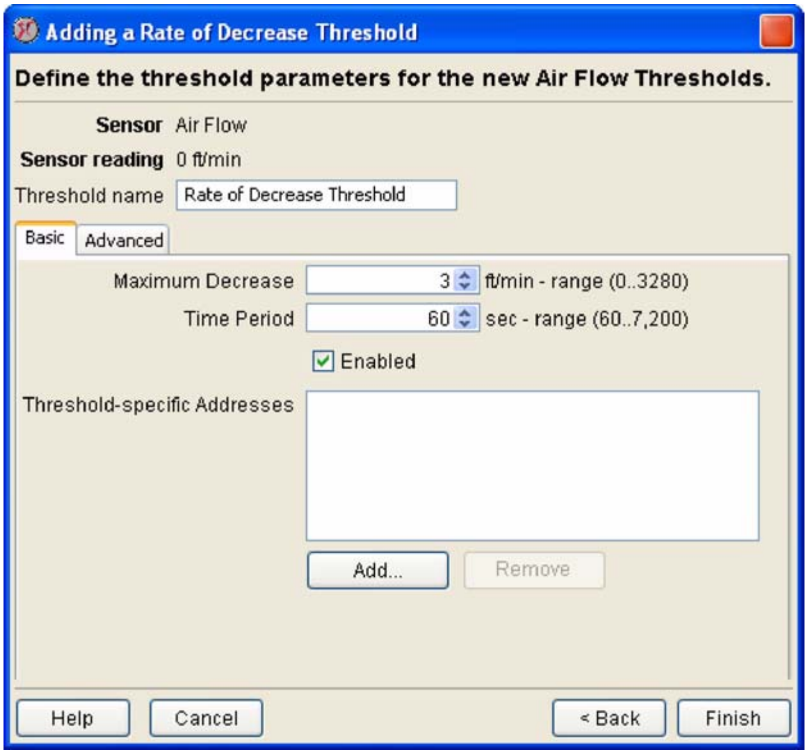
– Specify a User-specified URL and User-specified Description. You can use these fields to include additional user-specific information with any alert notifications that are generated using this threshold.

– Check the Return-To-Normal Requires User Input check box. When checked, if this threshold is exceeded the sensor will not report a Return-To-Normal state until a user with Administrator or Application (with Alert Update) privileges opens the resulting alert entry in the Alerts View and clicks the Mark Alert Resolved button.

7. Click OK to save this threshold.

Rate of Decrease Threshold

A rate of decrease threshold is defined by specifying a maximum acceptable decrease in value for selected sensors and a period of time value. If the value reported by the sensor falls by more than the specified maximum acceptable decrease in less than the specified period of time an alert condition is reported.



Adding a Rate of Decrease Threshold

Define the threshold parameters for the new Air Flow Thresholds.

Sensor Air Flow

Sensor reading 0 ft/min

Threshold name Rate of Decrease Threshold

Maximum Decrease 3 ft/min - range (0..3280)

Time Period 60 sec - range (60..7,200)

☑ Enabled

Threshold-specific Addresses

To define a rate of decrease threshold:

1. Launch the Sensor & Alert Settings task that corresponds to the numeric-based sensor for which you will define a threshold.
2. Select Rate of Decrease Threshold from the Threshold drop box. Any selected devices that have previously defined rate of decrease thresholds will be listed in the Management Devices list.
3. Select the desired threshold operation and targets:
   - If you are editing one or more previously defined rate of decrease thresholds, select the devices on which the threshold has been configured from the Management Devices list and then click Edit.
   - If you are defining a new rate of decrease threshold click Add. Then, select one or more devices for which this threshold will be configured, and click Next. Finally, select the sensors on the selected devices for which this threshold will be configured and then click Next.
4. Type in the Threshold Name field a name for this threshold.
5. Specify Basic threshold settings. From the Basic tab in the Thresholds pane:
   a. Type in the Maximum Decrease field (or use the arrows in the field to specify) the highest acceptable change value for the selected sensors. If the value reported by the sensor decreases by more than the Maximum Decrease value in a period of time that is equal to or less than the number of seconds specified in the Time Period field, an alert condition results.
   b. Type in the Time Period field (or use the arrows in the field to specify) the number of seconds that defines the unacceptable change period. If the value reported by the sensor decreases by more than the Maximum Decrease value in a period of time that is equal to or less than the Time Period value an alert condition is generated.
   c. Check the Enabled check box to enable the threshold. If this check box is not checked, the alert threshold will be saved but will not be active.

   Add to the Threshold-Specific Addresses list the e-mail addresses of any personnel to whom e-mail alert notifications should be sent if this threshold triggers an alert condition. Click Add..., type in the e-mail address to which the alert notification will be sent, and then click OK.

   If you’ve installed an SMS-capable modem you can deliver alert notification to SMS-enabled devices by entering threshold-specific addresses for them in the following format:

   sms:sms_device_address

   where *sms_device_address* is the telephone number or e-mail address associated with the SMS-enabled device (for example, “sms:5123334444” or “sms:user@mycorp.com”).

Note

These threshold-specific notifications are sent only if your device has one or more Alert Actions defined that use the Send E-Mail Message alert notification method and that have the Include Addresses from Thresholds check box checked. For more information, see “Alert Actions” on page 115 and “Creating Alert Actions” on page 225.

6. If desired, specify Advanced Threshold settings. All Advanced threshold settings are optional. From the Advanced tab in the Thresholds pane:
   - Specify a Return To Normal Delay value. Use the controls to specify the number of seconds that must pass after this threshold has returned to normal before the threshold state is considered

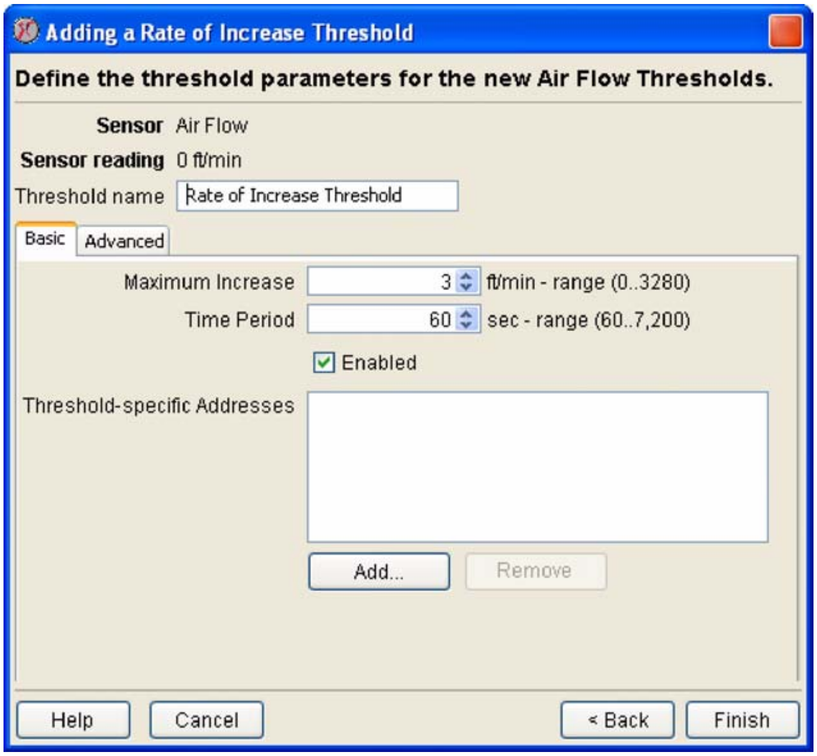
returned to normal. Default value is 0 (state returns to normal immediately after the measured value is no longer violating the threshold).

- Set an Advanced Schedule for this threshold (optional). By default, all thresholds are assumed to be enabled 24 hours a day, 7 days a week. However, you can specify that a threshold will be enabled only during specific time ranges. To set an Advanced Schedule:
  a. Click Advanced Schedule.... The Schedule Threshold window opens.
  b. By default, all time periods in the schedule are set to Enabled. To disable the threshold for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the threshold for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.
  c. When you have finished creating your Advanced Threshold, click OK to save the schedule and return to the Thresholds task.
- Select an Alert Severity value for this threshold. Available Alert Severities are, in order of escalating severity: Information, Warning, Error, Critical, or Failure. By default, the Alert Severity generated by this threshold will be “Error.”
- Select Cameras to Trigger in response to the alert. To include images from one or more connected NetBotz Camera Pod 120s, check the check boxes that correspond to the desired pods.
- Specify a User-specified URL and User-specified Description. You can use these fields to include additional user-specific information with any alert notifications that are generated using this threshold.
- Check the Return-To-Normal Requires User Input check box. When checked, if this threshold is exceeded the sensor will not report a Return-To-Normal state until a user with Administrator or Application (with Alert Update) privileges opens the resulting alert entry in the Alerts View and clicks the Mark Alert Resolved button.

7. Click OK to save this threshold.

Rate of Increase Threshold

A rate of increase threshold is defined by specifying a maximum acceptable increase in value for selected sensors and a period of time value. If the value reported by the sensor rises by more than the specified maximum acceptable increase in less than the specified period of time an alert condition is reported.



Define the threshold parameters for the new Air Flow Thresholds.

Sensor Air Flow

Sensor reading 0 ft/min

Threshold name Rate of Increase Threshold

Maximum Increase 3 ft/min - range (0..3280)

Time Period 60 sec - range (60..7,200)

☑ Enabled

Threshold-specific Addresses

To define a rate of increase threshold:

1. Launch the Sensor & Alert Settings task that corresponds to the numeric-based sensor for which you will define a threshold.
2. Select Rate of Increase Threshold from the Threshold drop box. Any selected devices that have previously defined rate of increase thresholds will be listed in the Management Devices list.
3. Select the desired threshold operation and targets:
   – If you are editing one or more previously defined rate of increase thresholds, select the devices on which the threshold has been configured from the Management Devices list and then click Edit.

   – If you are defining a new rate of increase threshold click Add. Then, select one or more devices for which this threshold will be configured, and click Next. Finally, select the sensors on the selected devices for which this threshold will be configured and then click Next.
4. Type in the Threshold Name field a name for this threshold.
5. Specify Basic threshold settings. From the Basic tab in the Thresholds pane:
   a. Type in the Maximum Increase field (or use the arrows in the field to specify) the highest acceptable change value for the selected sensors. If the value reported by the sensor increases by more than the Maximum Increase value in a period of time that is equal to or less than the number of seconds specified in the Time Period field, an alert condition results.
   b. Type in the Time Period field (or use the arrows in the field to specify) the number of seconds that defines the unacceptable change period. If the value reported by the sensor increases by more

than the Maximum Increase value in a period of time that is equal to or less than the Time Period value an alert condition is generated.

c. Check the Enabled check box to enable the threshold. If this check box is not checked, the alert threshold will be saved but will not be active.

Add to the Threshold-Specific Addresses list the e-mail addresses of any personnel to whom e-mail alert notifications should be sent if this threshold triggers an alert condition. Click Add..., type in the e-mail address to which the alert notification will be sent, and then click OK.

If you've installed an SMS-capable modem you can deliver alert notification to SMS-enabled devices by entering threshold-specific addresses for them in the following format:

sms:sms_device_address

where *sms_device_address* is the telephone number or e-mail address associated with the SMS-enabled device (for example, "sms:5123334444" or "sms:user@mycorp.com").

Note

These threshold-specific notifications are sent only if your device has one or more Alert Actions defined that use the Send E-Mail Message alert notification method and that have the Include Addresses from Thresholds check box checked. For more information, see "Alert Actions" on page 115 and "Creating Alert Actions" on page 225.

6. If desired, specify Advanced Threshold settings. All Advanced threshold settings are optional. From the Advanced tab in the Thresholds pane:

– Specify a Return To Normal Delay value. Use the controls to specify the number of seconds that must pass after this threshold has returned to normal before the threshold state is considered returned to normal. Default value is 0 (state returns to normal immediately after the measured value is no longer violating the threshold).

– Set an Advanced Schedule for this threshold (optional). By default, all thresholds are assumed to be enabled 24 hours a day, 7 days a week. However, you can specify that a threshold will be enabled only during specific time ranges. To set an Advanced Schedule:

a. Click Advanced Schedule.... The Schedule Threshold window opens.

b. By default, all time periods in the schedule are set to Enabled. To disable the threshold for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the threshold for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

c. When you have finished creating your Advanced Threshold, click OK to save the schedule and return to the Thresholds task.

– Select an Alert Severity value for this threshold. Available Alert Severities are, in order of escalating severity: Information, Warning, Error, Critical, or Failure. By default, the Alert Severity generated by this threshold will be "Error."

– Select Cameras to Trigger in response to the alert. To include images from one or more connected NetBotz Camera Pod 120s, check the check boxes that correspond to the desired pods.

– Specify a User-specified URL and User-specified Description. You can use these fields to include additional user-specific information with any alert notifications that are generated using this threshold.

– Check the Return-To-Normal Requires User Input check box. When checked, if this threshold is exceeded the sensor will not report a Return-To-Normal state until a user with Administrator or

Application (with Alert Update) privileges opens the resulting alert entry in the Alerts View and clicks the Mark Alert Resolved button.

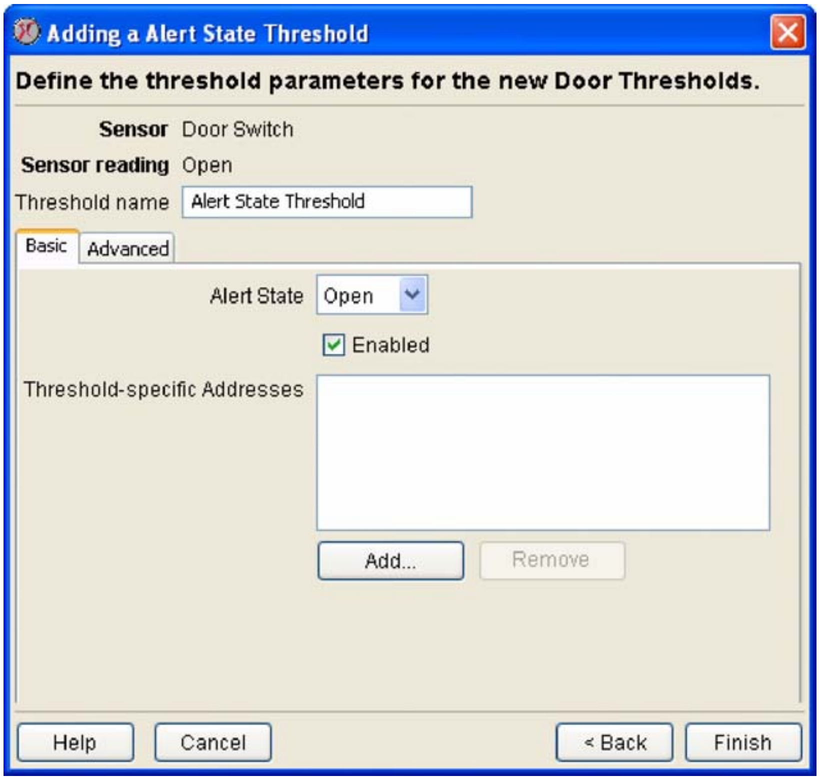
7. Click OK to save this threshold.

Defining State Thresholds

Detailed instructions on how to define each of the available state threshold types follow.

Alert State Threshold

An alert state threshold is defined by specifying the state which, if reported by selected sensors, will cause an alert condition to be reported. If the state reported by the sensor is the specified state for any length of time an alert condition is reported.



Adding a Alert State Threshold

Define the threshold parameters for the new Door Thresholds.

Sensor Door Switch

Sensor reading Open

Threshold name: Alert State Threshold

Alert State: Open

☑ Enabled

Threshold-specific Addresses

To define an alert state threshold:

1. Launch the Sensor & Alert Settings task that corresponds to the state-based sensor for which you will define a threshold.

2. Select Alert State Threshold from the Threshold drop box. Any selected devices that have previously defined alert state thresholds will be listed in the Management Devices list.

3. Select the desired threshold operation and targets:

   – If you are editing one or more previously defined alert state thresholds, select the devices on which the threshold has been configured from the Management Devices list and then click Edit.

   – If you are defining a new alert state threshold click Add. Then, select one or more devices for which this threshold will be configured, and click Next. Finally, select the sensors on the selected devices for which this threshold will be configured and then click Next.

4. Type in the Threshold name field a name for this threshold.

5. Specify Basic threshold settings. From the Basic tab in the Thresholds pane:

a. Select from the Alert State drop box the state that, if reported by the sensors, will result in an alert condition.

b. Check the Enabled check box to enable the threshold. If this check box is not checked, the alert threshold will be saved but will not be active.

Add to the Threshold-Specific Addresses list the e-mail addresses of any personnel to whom e-mail alert notifications should be sent if this threshold triggers an alert condition. Click Add..., type in the e-mail address to which the alert notification will be sent, and then click OK.

If you've installed an SMS-capable modem you can deliver alert notification to SMS-enabled devices by entering threshold-specific addresses for them in the following format:

sms:sms_device_address

where *sms_device_address* is the telephone number or e-mail address associated with the SMS-enabled device (for example, "sms:5123334444" or "sms:user@mycorp.com").

Note

These threshold-specific notifications are sent only if your device has one or more Alert Actions defined that use the Send E-Mail Message alert notification method and that have the Include Addresses from Thresholds check box checked. For more information, see "Alert Actions" on page 115 and "Creating Alert Actions" on page 225.

6. If desired, specify Advanced Threshold settings. All Advanced threshold settings are optional. From the Advanced tab in the Thresholds pane:

– Specify a Return To Normal Delay value. Use the controls to specify the number of seconds that must pass after this threshold has returned to normal before the threshold state is considered returned to normal. Default value is 0 (state returns to normal immediately after the measured value is no longer violating the threshold).

– Set an Advanced Schedule for this threshold (optional). By default, all thresholds are assumed to be enabled 24 hours a day, 7 days a week. However, you can specify that a threshold will be enabled only during specific time ranges. To set an Advanced Schedule:

a. Click Advanced Schedule.... The Schedule Threshold window opens.

b. By default, all time periods in the schedule are set to Enabled. To disable the threshold for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the threshold for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

c. When you have finished creating your Advanced Threshold, click OK to save the schedule and return to the Thresholds task.

– Select an Alert Severity value for this threshold. Available Alert Severities are, in order of escalating severity: Information, Warning, Error, Critical, or Failure. By default, the Alert Severity generated by this threshold will be "Error."

– Select Cameras to Trigger in response to the alert. To include images from one or more connected NetBotz Camera Pod 120s, check the check boxes that correspond to the desired pods.

– Specify a User-specified URL and User-specified description. You can use these fields to include additional user-specific information with any alert notifications that are generated using this threshold.

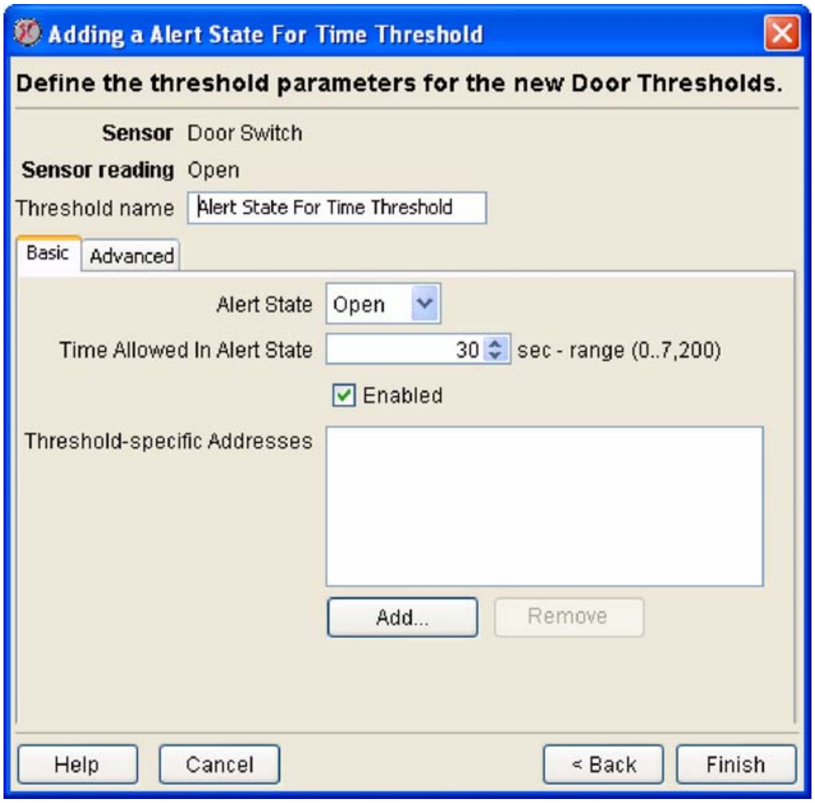
– Check the Return-To-Normal Requires User Input check box. When checked, if this threshold is exceeded the sensor will not report a Return-To-Normal state until a user with Administrator or

Application (with Alert Update) privileges opens the resulting alert entry in the Alerts View and clicks the Mark Alert Resolved button.

7. Click OK to save this threshold.

Alert State for Time Threshold

An alert state for time threshold is defined by specifying both a maximum time permitted value and the state which, if reported by selected sensors, will cause an alert condition to be reported. If the state reported by the sensor is the specified state and the state remains unchanged for more than the specified maximum time permitted value an alert condition is reported.



Adding a Alert State For Time Threshold

Define the threshold parameters for the new Door Thresholds.

Sensor Door Switch

Sensor reading Open

Threshold name Alert State For Time Threshold

Alert State Open

Time Allowed In Alert State 30 sec - range (0..7,200)

☑ Enabled

Threshold-specific Addresses

To define an alert state for time threshold:

1. Launch the Sensor & Alert Settings task that corresponds to the state-based sensor for which you will define a threshold.

2. Select Alert State for Time Threshold from the Threshold drop box. Any selected devices that have previously defined alert state for time thresholds will be listed in the Management Devices list.

3. Select the desired threshold operation and targets:

   – If you are editing one or more previously defined alert state for time thresholds, select the devices on which the threshold has been configured from the Management Devices list and then click Edit.

   – If you are defining a new alert state for time threshold click Add. Then, select one or more devices for which this threshold will be configured, and click Next. Finally, select the sensors on the selected devices for which this threshold will be configured and then click Next.

4. Type in the Threshold Name field a name for this threshold.

5. Specify Basic threshold settings. From the Basic tab in the Thresholds pane:

a. Select from the Alert State drop box the state that, if reported by the sensors, will result in an alert condition.

b. Type in the Time Allowed in Alert State field (or use the arrows in the field to specify) the number of seconds that the reported value can be in the selected Alert State before an alert condition is generated.

c. Check the Enabled check box to enable the threshold. If this check box is not checked, the alert threshold will be saved but will not be active.

Add to the Threshold-Specific Addresses list the e-mail addresses of any personnel to whom e-mail alert notifications should be sent if this threshold triggers an alert condition. Click Add..., type in the e-mail address to which the alert notification will be sent, and then click OK.

If you’ve installed an SMS-capable modem you can deliver alert notification to SMS-enabled devices by entering threshold-specific addresses for them in the following format:

sms:sms_device_address

where *sms_device_address* is the telephone number or e-mail address associated with the SMS-enabled device (for example, “sms:5123334444” or “sms:user@mycorp.com”).

Note

These threshold-specific notifications are sent only if your device has one or more Alert Actions defined that use the Send E-Mail Message alert notification method and that have the Include Addresses from Thresholds check box checked. For more information, see “Alert Actions” on page 115 and “Creating Alert Actions” on page 225.

6. If desired, specify Advanced Threshold settings. All Advanced threshold settings are optional. From the Advanced tab in the Thresholds pane:

– Specify a Return To Normal Delay value. Use the controls to specify the number of seconds that must pass after this threshold has returned to normal before the threshold state is considered returned to normal. Default value is 0 (state returns to normal immediately after the measured value is no longer violating the threshold).

– Set an Advanced Schedule for this threshold (optional). By default, all thresholds are assumed to be enabled 24 hours a day, 7 days a week. However, you can specify that a threshold will be enabled only during specific time ranges. To set an Advanced Schedule:

a. Click Advanced Schedule.... The Schedule Threshold window opens.

b. By default, all time periods in the schedule are set to Enabled. To disable the threshold for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the threshold for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

c. When you have finished creating your Advanced Threshold, click OK to save the schedule and return to the Thresholds task.

– Select an Alert Severity value for this threshold. Available Alert Severities are, in order of escalating severity: Information, Warning, Error, Critical, or Failure. By default, the Alert Severity generated by this threshold will be "Error."

– Select Cameras to Trigger in response to the alert. To include images from one or more connected NetBotz Camera Pod 120s, check the check boxes that correspond to the desired pods.

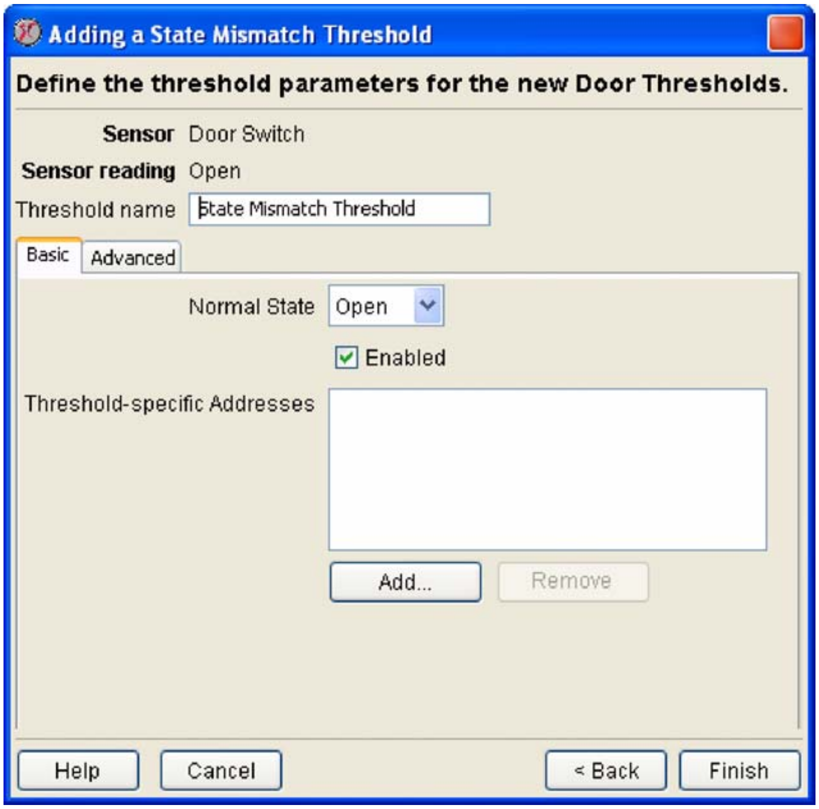
– Specify a User-specified URL and User-specified Description. You can use these fields to include additional user-specific information with any alert notifications that are generated using this threshold.

– Check the Return-To-Normal Requires User Input check box. When checked, if this threshold is exceeded the sensor will not report a Return-To-Normal state until a user with Administrator or Application (with Alert Update) privileges opens the resulting alert entry in the Alerts View and clicks the Mark Alert Resolved button.

7. Click OK to save this threshold.

State Mismatch Threshold

A state mismatch threshold is defined by specifying a "normal" state for the sensor. If any state other than the normal state is reported by the sensor, an alert condition is reported.



Adding a State Mismatch Threshold

Define the threshold parameters for the new Door Thresholds.

Sensor Door Switch

Sensor reading Open

Threshold name State Mismatch Threshold

Normal State Open

☑ Enabled

Threshold-specific Addresses

To define a state mismatch threshold:

1. Launch the Sensor & Alert Settings task that corresponds to the state-based sensor for which you will define a threshold.

2. Select State Mismatch Threshold from the Threshold drop box. Any selected devices that have

previously defined state mismatch thresholds will be listed in the Management Devices list.

3. Select the desired threshold operation and targets:

   – If you are editing one or more previously defined state mismatch thresholds, select the devices on which the threshold has been configured from the Management Devices list and then click Edit.

   – If you are defining a new state mismatch threshold click Add. Then, select one or more devices for which this threshold will be configured, and click Next. Finally, select the sensors on the selected devices for which this threshold will be configured and then click Next.

4. Type in the Threshold Name field a name for this threshold.

5. Specify Basic threshold settings. From the Basic tab in the Thresholds pane:

   a. Select from the Normal State drop box the state that is the normal operational state for the device. If any state other than the selected "normal" state is reported by the sensor an alert condition is generated.

   b. Check the Enabled check box to enable the threshold. If this check box is not checked, the alert threshold will be saved but will not be active.

   c. Add to the Threshold-Specific Addresses list the e-mail addresses of any personnel to whom e-mail alert notifications should be sent if this threshold triggers an alert condition. Click Add..., type in the e-mail address to which the alert notification will be sent, and then click OK.

      If you've installed an SMS-capable modem you can deliver alert notification to SMS-enabled devices by entering threshold-specific addresses for them in the following format:

      sms:sms_device_address

      where *sms_device_address* is the telephone number or e-mail address associated with the SMS-enabled device (for example, "sms:5123334444" or "sms:user@mycorp.com").

Note

These threshold-specific notifications are sent only if your device has one or more Alert Actions defined that use the Send E-Mail Message alert notification method and that have the Include Addresses from Thresholds check box checked. For more information, see "Alert Actions" on page 115 and "Creating Alert Actions" on page 225.

6. If desired, specify Advanced Threshold settings. All Advanced threshold settings are optional. From the Advanced tab in the Thresholds pane:

   – Specify a Return To Normal Delay value. Use the controls to specify the number of seconds that must pass after this threshold has returned to normal before the threshold state is considered returned to normal. Default value is 0 (state returns to normal immediately after the measured value is no longer violating the threshold).

   – Set an Advanced Schedule for this threshold (optional). By default, all thresholds are assumed to be enabled 24 hours a day, 7 days a week. However, you can specify that a threshold will be enabled only during specific time ranges. To set an Advanced Schedule:

     a. Click Advanced Schedule.... The Schedule Threshold window opens.

     b. By default, all time periods in the schedule are set to Enabled. To disable the threshold for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the threshold for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

c. When you have finished creating your threshold Enable Schedule, click OK to save the schedule and return to the Thresholds task.

– Select an Alert Severity value for this threshold. Available Alert Severities are, in order of escalating severity: Information, Warning, Error, Critical, or Failure. By default, the Alert Severity generated by this threshold will be "Error."

– Select Cameras to Trigger in response to the alert. If desired, alert notifications generated in response to this threshold can include image captures from any Camera Pod 120s connected to your device. To include images from one or more connected Camera Pod 120s, check the check boxes that correspond to the desired pods.

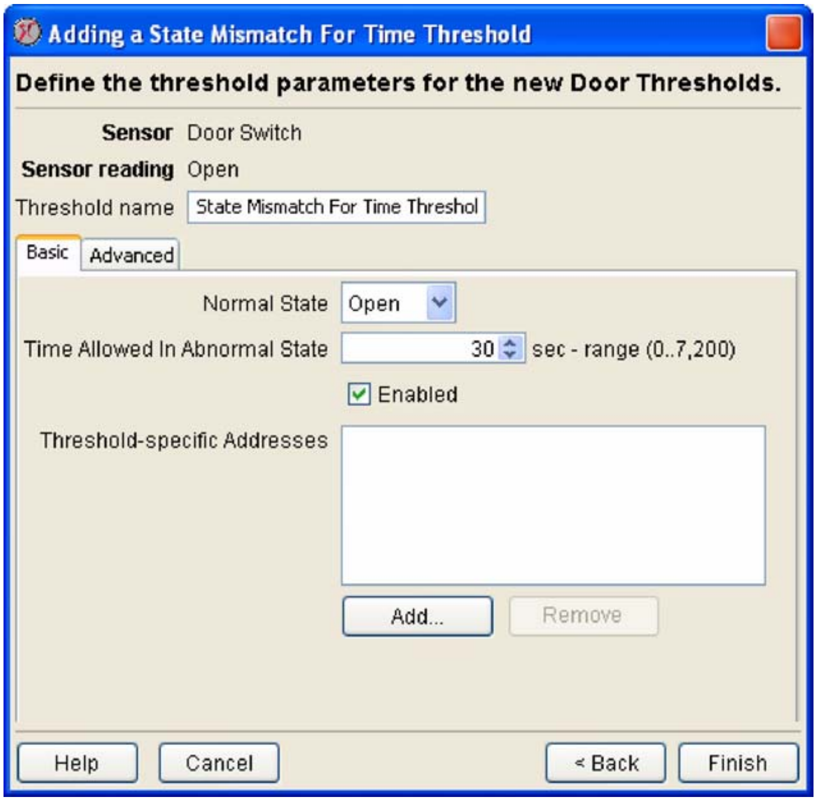
– Specify a User-specified URL and User-specified Description. You can use these fields to include additional user-specific information with any alert notifications that are generated using this threshold.

– Check the Return-To-Normal Requires User Input checkbooks. When checked, if this threshold is exceeded the sensor will not report a Return-To-Normal state until a user with Administrator or Application (with Alert Update) privileges opens the resulting alert entry in the Alerts View and clicks the Mark Alert Resolved button.

7. Click OK to save this threshold.

State Mismatch for Time Threshold

A state mismatch for time threshold is defined by specifying both a "normal" state for the sensor and a maximum time permitted value. If any state other than the normal state is reported by the sensor for more than the maximum amount of time permitted an alert condition is reported.



Adding a State Mismatch For Time Threshold

Define the threshold parameters for the new Door Thresholds.

Sensor Door Switch

Sensor reading Open

Threshold name State Mismatch For Time Threshol

Normal State Open

Time Allowed In Abnormal State 30 sec - range (0..7,200)

☑ Enabled

Threshold-specific Addresses

To define an alert state for time threshold:

1. Launch the Sensor & Alert Settings task that corresponds to the state-based sensor for which you

will define a threshold.

2. Select State Mismatch for Time Threshold from the Threshold drop box. Any selected devices that have previously defined state mismatch for time thresholds will be listed in the Management Devices list.
3. Select the desired threshold operation and targets:
   – If you are editing one or more previously defined state mismatch for time thresholds, select the devices on which the threshold has been configured from the Management Devices list and then click Edit.

   – If you are defining a new state mismatch for time threshold click Add. Then, select one or more devices for which this threshold will be configured, and click Next.
4. Finally, select the sensors on the selected devices for which this threshold will be configured and then click Next.
5. Type in the Threshold Name field a name for this threshold.
6. Specify Basic threshold settings. From the Basic tab in the Thresholds pane:
   a. Select from the Normal State drop box the state that is the normal operational state for the device. If any state other than the selected "normal" state is reported by the sensor an alert condition is generated.
   b. Type in the Time Allowed in Alert State field (or use the arrows in the field to specify) the number of seconds that the reported value can be in a state other than the selected Normal State before an alert condition is generated.
   c. Check the Enabled check box to enable the threshold. If this check box is not checked, the alert threshold will be saved but will not be active.
   d. Add to the Threshold-Specific Addresses list the e-mail addresses of any personnel to whom e-mail alert notifications should be sent if this threshold triggers an alert condition. Click Add..., type in the e-mail address to which the alert notification will be sent, and then click OK.

   If you've installed an SMS-capable modem you can deliver alert notification to SMS-enabled devices by entering threshold-specific addresses for them in the following format:

   sms:sms_device_address

   where *sms_device_address* is the telephone number or e-mail address associated with the SMS-enabled device (for example, "sms:5123334444" or "sms:user@mycorp.com").

Note

These threshold-specific notifications are sent only if your device has one or more Alert Actions defined that use the Send E-Mail Message alert notification method and that have the Include Addresses from Thresholds check box checked. For more information, see "Alert Actions" on page 115 and "Creating Alert Actions" on page 225.

6. If desired, specify Advanced Threshold settings. All Advanced threshold settings are optional. From the Advanced tab in the Thresholds pane:
   – Specify a Return To Normal Delay value. Use the controls to specify the number of seconds that must pass after this threshold has returned to normal before the threshold state is considered

returned to normal. Default value is 0 (state returns to normal immediately after the measured value is no longer violating the threshold).

– Set an Advanced Schedule for this threshold (optional). By default, all thresholds are assumed to be enabled 24 hours a day, 7 days a week. However, you can specify that a threshold will be enabled only during specific time ranges. To set an Advanced Schedule:

a. Click Advanced Schedule.... The Schedule Threshold window opens.

b. By default, all time periods in the schedule are set to Enabled. To disable the threshold for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the threshold for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

c. When you have finished creating your threshold Enable Schedule, click OK to save the schedule and return to the Thresholds task.

– Select an Alert Severity value for this threshold. Available Alert Severities are, in order of escalating severity: Information, Warning, Error, Critical, or Failure. By default, the Alert Severity generated by this threshold will be “Error.”

– Select Cameras to Trigger in response to the alert. If desired, alert notifications generated in response to this threshold can include image captures from any Camera Pod 120s connected to your device. To include images from one or more connected Camera Pod 120s, check the check boxes that correspond to the desired pods.

– Specify a User-specified URL and User-specified Description. You can use these fields to include additional user-specific information with any alert notifications that are generated using this threshold.

– Check the Return-To-Normal Requires User Input check box. When checked, if this threshold is exceeded the sensor will not report a Return-To-Normal state until a user with Administrator or Application (with Alert Update) privileges opens the resulting alert entry in the Alerts View and clicks the Mark Alert Resolved button.

7. Click OK to save this threshold.

Mass Configuration: Device Settings

The selections available from the Mass Configuration view enable you perform mass configuration tasks on the APC NetBotz devices installed on your network. Use Mass Configuration tasks to set APC NetBotz device configuration settings, enable license-key based functionality to your APC NetBotz devices, enable and disable alerts, set threshold values, configure device web interfaces, and to configure the alert actions and policies that will be used when alerts are reported by the sensors that are built into or connected to your APC NetBotz devices. The individual tasks are divided into *Sensor and Alert Settings* and *Device Settings*. This chapter covers only the Device Settings tasks. For information regarding Sensor and Alert Settings tasks see “Mass Configuration: Sensor and Alert Settings” on page 113.

The tasks available from the Device Settings portion of the Mass Configuration panel enable you to configure your APC NetBotz devices. Detailed information about the tasks available from the Device Settings portion of the Configuration panel follows.

Configuring Offline Devices

If a device goes offline, InfraStruXure Central will assume that the offline state is a temporary event. When a device is in an offline state you can still perform Mass Configuration tasks on the device. InfraStruXure Central will store these tasks in the Management Device Job Control queue, and will automatically perform the tasks as soon as the device comes back online.

Whenever you start a Mass Configuration task, the first window that is displayed shows a table of devices on which the selected task can be performed. This table features a Status column, in which the current status of each device is displayed. If a device is currently in an offline state the Status field for the device will read “Offline,” but you will still be able to enact Mass Configuration tasks on the device, just as if the device were online. When a Mass Configuration task is enacted against an offline device, the Status field will show that the task did not complete and is being retired automatically, and a small image of a clock is displayed to indicate that the configuration request against this device is currently in a pending state.

If InfraStruXure Central is unable to carry out a mass configuration task because a device is in an Offline state, it adds the task to the Pending Requests list (“Management Device Job Control” on page 89).

Managing BotzWare Version 1.x Devices

The Pod Sharing task enables you to use NetBotz 500 devices to receive data from legacy NetBotz devices running BotzWare 1.x (including RackBotz and WallBotz 300, 303, 310, 400, and 410 devices). Once a NetBotz 500 is configured to access these legacy models they are treated exactly like other shared pods or devices, providing alert and sensor data exactly as if they were directly connected to the NetBotz 500. For more information on Pod Sharing, see “Pod Sharing” on page 206.

About Information

Use the About Information task to quickly display a variety of product information about any selected device. After you select a group from the Group list or one or more devices from the Devices in... list and start the About Information task the device selection window appears. In addition to the IP address/hostname and status of each selected device, the About Information device selection window also includes one task-specific information column: Current Version, which displays information about the version of firmware version running on each device.

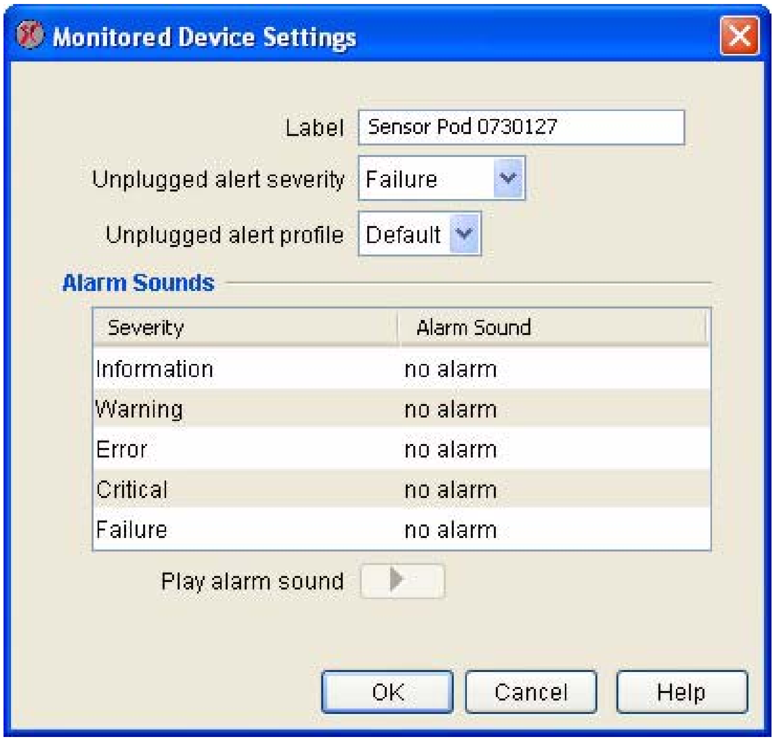
To view detailed information about any of the devices in the device selection list, select a device from the list and then click View. A new window appears that displays additional, highly detailed information about the device, as well as about any pods that are connected to the device (if applicable).

Note

The About Information task can be run only on one device at a time.

Monitored Device Settings

Use the Monitored Device Settings task to specify the label that will be used to uniquely identify each monitored device. In addition, when using Monitored Device Settings you can also configure a number of other device-specific settings.



Label: Sensor Pod 0730127

Unplugged alert severity: Failure

Unplugged alert profile: Default

Alarm Sounds

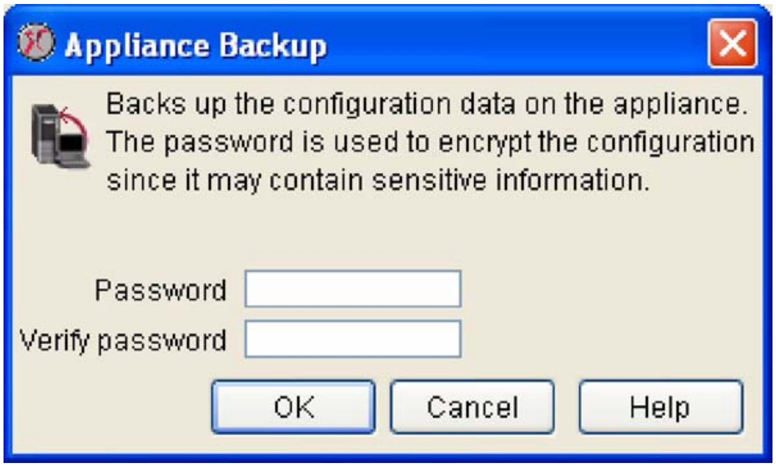
Severity	Alarm Sound
Information	no alarm
Warning	no alarm
Error	no alarm
Critical	no alarm
Failure	no alarm

To use the Monitored Device Settings task:

1. Launch the Monitored Device Settings task.
2. Select one or more monitored devices from the device selection list and then click Edit.
3. The Monitored Device Settings window opens. Type in the available fields the labels that will be used for all selected pods. Additional configuration settings may be available, depending on the type of device you are configuring. For additional information see the documentation that was included with your device.
4. Click OK to save your monitored device settings.

Backup

Use the Backup task to save your device configurations to password-protected, encrypted files. This backup file, which is stored on the InfraStruXure Central device, contains the entire device configuration, including user accounts settings, pod configurations, alert actions and profiles. Once a device configuration is saved, you can use the Restore task (see “Restore” on page 214) to restore the device configuration at a later date.



Backs up the configuration data on the appliance. The password is used to encrypt the configuration since it may contain sensitive information.

To use the Backup task:

1. Launch the Backup task. In addition to the IP address/hostname and status of each selected device, the Backup task's device selection window also includes one task-specific information column: Last Backup, which displays information about the last backup that was performed on each device. To continue, select one or more devices from the device selection window and click Backup.
2. Type in the Password field the password that will be used to protect this backup file. Note that without this password you will not be able to use the Restore task to decrypt and restore the device settings.
3. Type the password again in the Verify password field.
4. Click OK to back up the configuration of any selected devices.

Camera Configuration

Use the Camera Configuration task to configure cameras integrated with supported devices, and Camera Pod 120s or CCTV Adapter Pods that connected to NetBotz 500 or 420 devices. You can use the Camera Configuration task to specify camera image capture settings, including mode, frame rate, total number of images to be captured when alerts are reported, and total number of images saved prior to an alert condition to include in alert notifications.

After you select a group from the Group list or one or more devices from the Devices in... list and start the Camera Configuration task the device selection window appears. In addition to the IP address/hostname and status of each selected device, the Camera Configuration device selection window also includes the following task-specific information columns:

- Monitored Device: The label that is assigned to the device, if any.
- Mode: Each device's current resolution setting. This setting specifies the resolution at which images are captured for use in alert notifications.
- Maximum Rate: Each device's current maximum rate setting. This setting specifies the refresh rate for image captures when a picture alert is triggered.

- Post-alert Capture Time: Each devices current post-alert capture time setting. The post-alert capture time setting specifies the total number of seconds after the alert triggering event for which images will be included in alert notifications.

Select a device from the Camera Configuration device selection window and then click Edit to open the Camera Capture Settings window. Use the Camera Capture Settings window to configure various camera and image capture settings. From this window you can configure the following camera and image capture settings:

Control	Description
Brightness	Specifies the brightness of the image captured by the camera. The brightness value of the image can be set to values from 0 to 255.
Gamma correction	Use the Gamma correction control to adjust the overall brightness of the camera image. Gamma correction enables you to display captured image more accurately on your computer screen. Images which are not properly corrected can look either bleached out, or too dark.
Video format	Used to specify the format in which video is transmitted by the video source. Available selections include: NTSC-M, NTSCJapan, PAL-B, PAL-D, PAL-G, PAL-H, PAL-I, PAL-M, PAL-N Combination, and SECAM. **Note:** This option is available only when configuring Capture settings for CCTV Adapter Pods.
Rotate camera image 180 degrees	Check this check box to rotate the image captured by the camera 180 degrees. This is useful for correctly orienting the image captures included in alert notifications and in the Advanced View when the device has been mounted upside down due to installation location restrictions. **Note**: This option is not available for use when configuring Capture settings for CCTV Adapter Pods.
Flicker filter	Check this check box to minimize image brightness flickering. In some situations, typically outdoors or in locations with large areas of both brightly lit and low light regions, the brightness level of the dark areas in the image can occasionally flicker or pulse. Enabling flicker filter will eliminate this flickering. Notes: • Enabling flicker filter can also have a slight impact on the number of frames per second at which images are captured and displayed. This impact is typically noticeable only at higher image capture rates (more than 5 per second). • This option is not available for use when configuring Capture settings for CCTV Adapter Pods.
Timestamp	Use this control to specify the location of the timestamp within the image capture. Available selections include None (no timestamp will be included in the image), Bottom Right, Bottom Center, Bottom Left, Top Right, Top Center, and Top Left.

Control	Description
Color Balance / Type of Lighting / Red Balance / Blue Balance	Use this control to specify the color balance settings that will be used by the camera. The four pre-configured Color Balance selections are: • Fluorescent: Best color balance settings for locations with fluorescent lighting. • Incandescent: Best color balance settings for locations with incandescent lighting. • Daylight: Best color balance settings for locations with natural lighting. • Auto-detect: Analyzes the current lighting conditions and automatically selects the best. You can also select Custom and specify Red Adjustment and Blue Adjustment values. Use the spin-buttons to adjust the Red and Blue Adjustment values. Values from 0 to 255 are available.
Mode	The resolution at which images are captured for use in alert notifications.
Rate	Specifies the refresh rate for image captures when a picture alert is triggered. Note: This rate value represents the maximum potential rate at which images will be captures. Other factors, such as exposure time and USB traffic load, can limit or reduce the number of images that are actually captured.
Image Quality	Specifies the amount of compression that will be applied to captured images. As compression is increased, file sizes decrease but the quality of the image decreases as well. The available values, from highest image quality/largest file size to lowest image quality/ smallest file size, is High Quality, Normal Quality, Normal Compression and High Compression. Note: Actual frame rate available from image processor depends on the resolution and image quality of generated images. Maximum frame rate of 30 frames per second is available only at Normal Quality or lower and only at resolutions up to 640x480. Maximum frame rate for 800x600, 1024x768, and 1280x1024 (if available) at Normal Quality or lower is 10 frames per second. For example, if you configure a Camera Pod 120 to capture images in High Quality, the Maximum Frame Rate for some resolutions changes: At 640x480 and lower resolution the maximum frame rate drops from 30 frames per second to 20 frames per second. In 800x600 the maximum frame rate is unchanged (stays at 10 frames per second). In 1024x768 and 1280x1024 the maximum frame rate drops from 10 frames per second to 8 frames per second.

Control	Description
Post-alert capture time	Specifies the total number of seconds after the alert triggering event for which images will be included in alert notifications. The number of post-alert images that are captured is equal to the Post-Alert Capture Time multiplied by the Rate value. Note that the individual Alert Actions may specify a Maximum Camera Pictures setting that is less than the total number of images captured in response to an alert. If the total number of pictures captured by the camera (including both post-alert captures and pre-alert captures) is larger than the Maximum Camera Pictures setting for an Alert Action then the most recent images captured are given preference and included in the alert notification.
Pre-alert capture time	Specifies the total number of seconds prior to the alert triggering event for which available images will be included in the alert notification. The number of post-alert images that are captured is equal to the Pre-Alert Capture Time multiplied by the Rate value. **Note:** The individual Alert Actions may specify a Maximum Camera Pictures setting that is less than the total number of images captured in response to an alert. If the total number of pictures captured by the camera (including both post-alert captures and pre-alert captures) is larger than the Maximum Camera Pictures setting for an Alert Action then the most recent images captured are given preference and included in the alert notification.
Delay time before capturing	Specifies the number of seconds between the triggering of the alert and the first picture capture.
Include audio	Specifies whether the device should also use either the integrated microphone or an external microphone (if one has been plugged into the External Microphone jack on the pod) to capture audio and include it with the alert for the duration of time covered by the alert notification. Note: This option is available only when configuring Camera Pod 120s and CCTV Adapter Pods.
Audio volume	Specifies the volume at which audio will be captured.
Capture Data Summary Information	Shows a variety of information about the files that will be generated by the pod using the currently selected Capture settings. The information in this field will update automatically as new settings are specified or selected.

Type the new values in the appropriate fields. When you are finished, click OK and any changes you have made will be saved to the device. Click Cancel to close the Camera Capture Settings window without saving any changes.

Note

The Camera Configuration task can be run only on one device at a time.

Camera Masking

Use the Camera Masking task to specify the conditions that will cause the camera motion sensor of selected devices to generate an alert, to specify a motion sensitivity mask (to ignore motion is user-specified areas of the image) for selected devices, or to specify a block-out mask (to prevent user-specified regions of the image from being seen.

Note

Block-out mask functionality is available only on devices for which the Premium Software Module has been purchased.

After you select a group from the Group list or one or more devices from the Devices in... list and start the Camera Masking task the device selection window appears. In addition to the IP address/hostname and status of each selected device, the Mask Settings device selection window also includes the following task-specific information columns:

- Monitored Device: The label that is assigned to the device, if any.
- Enable Camera Motion: Indicates whether camera motion sensing is enabled on this device.
- Show Outline of Detected Motion: Indicates whether the Show outline of detected motion option is enabled on this device. When this option is enabled, any region of an image captured by the device that is determined to be indicative of motion is surrounded by a dotted-line outline.

Select a device from the Mask Settings device selection window and then click Edit to open the Mask Settings window. The Mask Settings window includes two tabbed panes:

- The Motion Mask pane: Use the settings available from this pane to configure the Camera Motion sensor to ignore movement that is detected in specified regions of the image capture.
- Block Out Mask pane: Use the settings available from this pane to configure the cameras of selected devices so that specified areas of the image cannot be seen. Note that the functionality in this pane is enabled for use only on devices for which the Premium Software Module has been purchased.

The Motion Mask Tab

Use the settings available from this pane to configure the Camera Motion sensor to ignore movement that is detected in specified regions of the image capture. The following controls are available on the Motion Mask tab:

Field	Description
Sensitivity	The Sensitivity setting specifies how much change in a portion of the image capture will be tolerated before the changed image data is considered movement. Lower values indicate less tolerance for change between images and therefore higher sensitivity.
Area of Motion	The Area of Motion setting specifies how large an area of the image capture must change (as determined by the Sensitivity value) before the changed image data is considered movement. Lower Area of Motion values indicate smaller areas and therefore higher sensitivity.
Enable Camera Motion check box	Check this check box to enable the camera motion sensor.

Field	Description
Show outline of detected motion check box	When this option is enabled, any region of an image captured by the device that is determined to be indicative of motion is surrounded by a dotted-line outline. Note that if this option is enabled then the dotted-line outline will appear in the camera image that is displayed in the Sensor Pane as well.
Motion Sensitivity Mask	Use the Motion Sensitivity Mask to specify regions of the image that will be ignored by the Camera Motion sensor.

Use the Motion Sensitivity Mask to configure the Camera Motion sensor to ignore movement that is detected in specified regions of the image capture. To mask a portion of the image, click and drag in the image to draw a box around the region you want to ignore. Then click Mask Selection to mask the selected region. Red X’s will appear in the region of the image in which movement will be ignored.

To unmask a portion of a previously masked region, click and drag in the image to draw a box around the region you want to unmask. Then, click Unmask Selection to remove the mask from the selected region. Any red X’s that were displayed in the selected region will then be removed.

When you are finished, click OK and any changes you have made will be saved to the selected devices. Click Cancel to close the Camera Masking task without saving any changes.

The Block Out Mask Tab

The following controls are available on the Block Out Mask tab:

Field	Description
Enable Block Out Mask check box	Check this check box to enable the Block Out Mask functionality.
Block Out Mask	Use the Block Out Mask to specify regions of the image that will not be visible when the camera image is viewed.

Use the Block Out Mask to configure the cameras of selected devices so that specified areas of the image cannot be seen. For example, you could place a Block Out Mask over the area of the image that shows a monitor image, thereby preventing users from seeing the information that is shown on the monitor. Instead, a gray box will appear in the masked area.

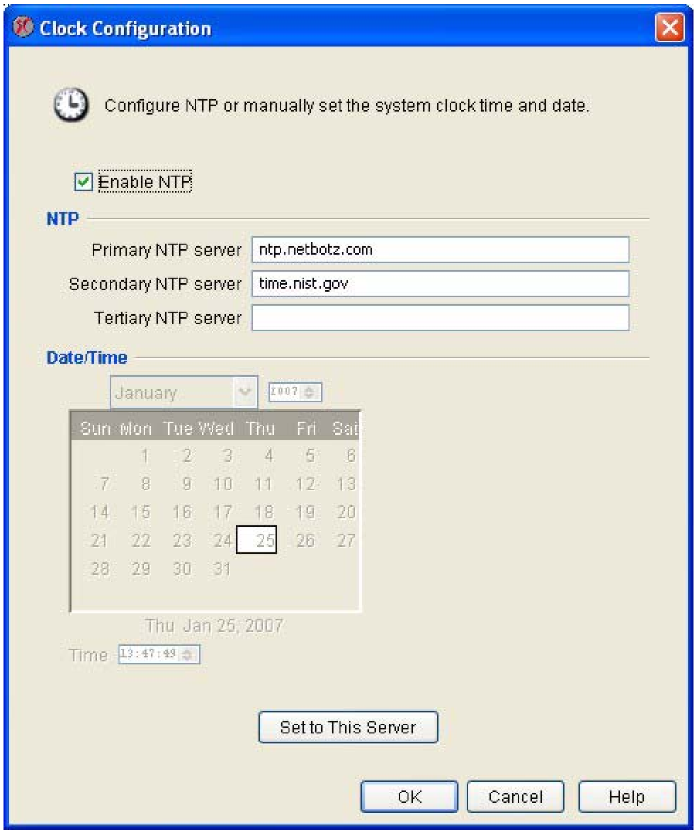
To mask a portion of the image, click and drag in the image to draw a box around the region you want to ignore. Then right-click and select Mask Selection to mask the selected region. A blue block will appear in the region of the image to be blocked.

To unmask a portion of a previously masked region, click and drag in the image to draw a box around the region you want to unmask. Then, click Unmask Selection to remove the mask from the selected region. Any portion of the blue block out mask that you selected will then be removed.

When you are finished, click OK and any changes you have made will be saved to the device. Click Cancel to close the Camera Masking task without saving any changes.

Clock

Use the Clock task to view or change the date and time that are configured on the internal clock of selected devices, or to configure selected devices to obtain and synchronize clock and calendar settings from an NTP server.



Configure NTP or manually set the system clock time and date.

☑ Enable NTP

Primary NTP server: ntp.netbotz.com

Secondary NTP server: time.nist.gov

Tertiary NTP server:

January 2007

Sun	Mon	Tue	Wed	Thu	Fri	Sat
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			

Thu Jan 25, 2007

Time 13:47:49

To use the Clock task:

1. Launch the Clock task. In addition to the IP address/hostname and status of each selected device, the Clock task's device selection window also includes two task-specific information columns:
   - – NTP Enabled: Specifies whether the device's NTP agent has been enabled or not.
   - – Current Date & Time: Displays the date and time that are currently reported by the device.
2. To continue, select one or more devices from the device selection window and click Edit.

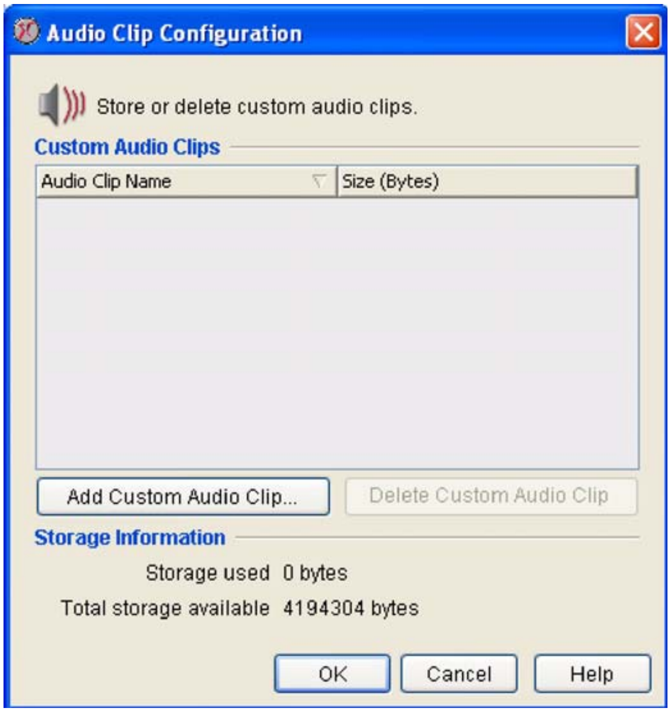
3. The Clock Settings window opens. The following controls are available from the Clock task:

Field	Description
Enable NTP check box	Check this check box to enable the NTP functionality. Un-check this check box to enable the clock and calendar controls on this pane.
Primary, Secondary, and Tertiary NTP servers	IP address of NTP servers for use in automatically setting the device clock.
Date/time controls	Use the arrows in the Time field, the Month drop box, the arrows in the Year field, and the Calendar control to manually configure the day, date, and time used by your device's internal clock.
Set to This Server	Click this button to configure your devices to automatically obtain all clock and calendar settings from this InfraStruXure Central server.

4. Specify the desired values in the appropriate fields. When you are finished, click OK and any changes you have made will be saved to all selected devices.

Custom Audio Clips

Use the Custom Audio Clips task to upload custom audio clips (in WAV or OGG format) to your APC NetBotz 500 device, or to delete previously uploaded clips from the NetBotz 500 device. Once uploaded, audio clips can be used with the Play Custom Audio alert action. This task is available for use only with APC NetBotz 500 devices.



Store or delete custom audio clips.

Storage used 0 bytes

Total storage available 4194304 bytes

Note

There is a limited amount of audio clip storage available on your APC NetBotz 500 device. APC NetBotz 500 devices have a total of 4MB of space available for custom audio clips (shared with any background images that have been stored on the device. For more information, see “Creating and Editing Maps” on page 51). Be sure to take these limitations into consideration when choosing background image files.

To use the Custom Audio Clips task to add or delete custom audio clips from your devices, launch the Custom Audio Clips task. In addition to the IP address/hostname and status of each selected device, the Custom Audio Clips task's device selection window also includes one task-specific information column: Number of Audio Clips, which shows the number of custom audio clips that are currently stored on each device.

To continue, select one or more devices from the device selection window and click Edit.

Adding Custom Audio Clips

To add custom audio clips to the selected devices:

1. Click Add custom audio clip.
2. Use the file selection interface to select a sound file. Files must conform to the following specifications:
   - OGG format: 8khz or 16khz sample rate, mono or stereo.
   - Windows WAV format (PCM only): Any sample rate, mono or stereo. Note that WAV files will be encoded into OGG files on upload, so the actual storage space used will be significantly less than the initial WAV file size.
3. Click OK to upload the file to your device.

Once the file is uploaded, it will be available for use with the Play Custom Audio Alert action.

Deleting Custom Audio Clips

To delete previously uploaded custom audio clips from the selected devices, select the audio clip you wish to delete from the Custom Audio Clips selection list and then click Delete custom audio clip.

Device Crawlers

Use the Device Crawlers task to configure your devices to monitor the general status information of up to 48 remote SNMP targets (such as servers, routers, and switches). If any operational difficulties are noted on a monitored target your devices can generate an alert notification, enabling you to quickly address the problem. Once added, you can set thresholds, monitor alerts, and graph data reported by the Device Crawlers targets, just as with pods and other sensors.

Device Crawlers also enables you to obtain detailed device-specific information on supported devices and to enable OID-specific monitoring and alerting. Device Crawlers enables you to use Device Description Files that make it quick and easy to monitor the environmental and physical data reported by some supported SNMP devices.

Note

- The Device Crawlers task can be run only on one device at a time.
- For more sophisticated monitoring and management of supported SNMP devices, use the Device Scanners task.

Device Crawlers monitors the following MIB II SNMP values on all specified SNMP targets:

- Online: State sensor that reports whether the target is Online or Offline.
- Ping RTT: Analog sensor that reports amount of time it takes SNMP queries or ICMP Ping requests to complete a send and reply from the device.
- SNMP System Contact: Displays the target's system contact data (does not support configuration of thresholds).
- SNMP System Description: Displays the target's system description data (does not support configuration of thresholds).
- SNMP System Location: Displays the target's system location data (does not support configuration of thresholds).
- SNMP System Name: Displays the target's system name data (does not support configuration of thresholds).
- SNMP System Object ID: Displays the target's system object ID data (does not support configuration of thresholds).
- SNMP System Uptime: Analog sensor that reports the uptime value of the target.
- System Model: Displays the target's system model data (does not support configuration of thresholds).
- System Type: Displays the target's system type data (does not support configuration of thresholds).
- System Vendor: Displays the target's system vendor data (does not support configuration of thresholds).

In addition, Device Crawlers will also gather and present the following information about the network interfaces of all configured SNMP targets in individual sensor sets:

- Admin Status: State sensor that reports the admin status of the interface.
- IF Description: Displays the interface's description value (does not support configuration of thresholds).
- IF MAC Address: Displays the interface's MAC address (does not support configuration of thresholds).
- IF Type: State sensor that reports the interface type value.
- Incoming Discards: Analog sensor that reports the number of incoming packets discarded by the interface.
- Incoming Errors: Analog sensor that reports the number of incoming packets containing errors received by the interface.
- Incoming Non-Unicast Packets: Analog sensor that reports the number of incoming non-unicast packets received by the interface.
- Last Change: Analog sensor that reports the last change value for the interface.
- OP Status: Analog sensor that reports the OP status of the interface.
- Outgoing Errors: Analog sensor that reports the number of outgoing packets containing errors sent by the interface.

- Outgoing Non-Unicast Packets: Analog sensor that reports the number of non-unicast packets sent by the interface.
- Outgoing Octets: Analog sensor that reports the number of outgoing octets sent by the interface.
- Outgoing Unicast Packets: Analog sensor that reports the number of outgoing unicast packets sent by the interface.

OID-Specific Monitoring

Device Crawlers provides two methods by which you can monitor individual OIDs on your SNMP targets:

- Selecting OIDs surfaced using Device Definition Files
- Manually adding individual supplemental OIDs

Device Description Files (provided and periodically updated by APC) make it quick and easy to monitor the environmental and physical data reported by some supported SNMP devices. Identifying and monitoring a device’s individual OIDs can be a painstaking process. MIBs can contain thousands of individual OIDs, and most of these are of little or no interest or use for monitoring purposes. Device Description Files make it simple to monitor the environmental and physical data reported on supported devices by automatically surfacing the OIDs that report data that is pertinent to environmental monitoring, making the process of monitoring the condition of these devices far simpler.

If you want to monitor the values reported by OIDs on SNMP targets for which Device Definition Files is not available, Device Crawlers also enables you to manually add supplemental OID data which can then be monitored.

Enhanced Environmental Monitoring

Device Crawlers provides access to the environmental monitoring data that is stored in the MIBs of your SNMP targets. This is accomplished in two ways:

- Using Device Definition Files to quickly and easily surface environmental monitoring-oriented OIDs on supported SNMP targets. Any information surfaced using a DDF will appear as a sensor set named Advanced Details.
- Enabling monitoring of any user-specified and defined supplemental OIDs on an SNMP target

Enhanced Alert Notification

In addition to enhancing your ability to gather SNMP-based data from your SNMP targets, Device Crawlers enables you to generate alert notifications when monitored OID values change. Using both the Device Definition Files and the Supplemental OID functionality, you can extend your environmental monitoring and notification abilities to include environmental conditions in and around all of your SNMP targets as well as those around your devices.

Using the Device Crawlers Task

Instructions for using the Device Crawlers task follow.

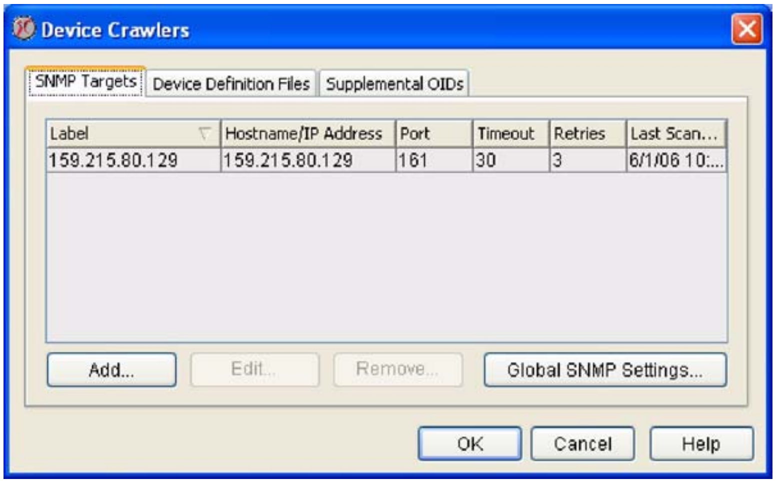
The SNMP Targets View

To define a new SNMP target (or modify a previously defined SNMP target) for use with Device Crawlers:

1. Launch the Device Crawlers task. In addition to the IP address/hostname and status of each selected device, the Device Crawlers task's device selection window also includes one task-specific information column: Target Count, which displays the total number of SNMP targets that have been

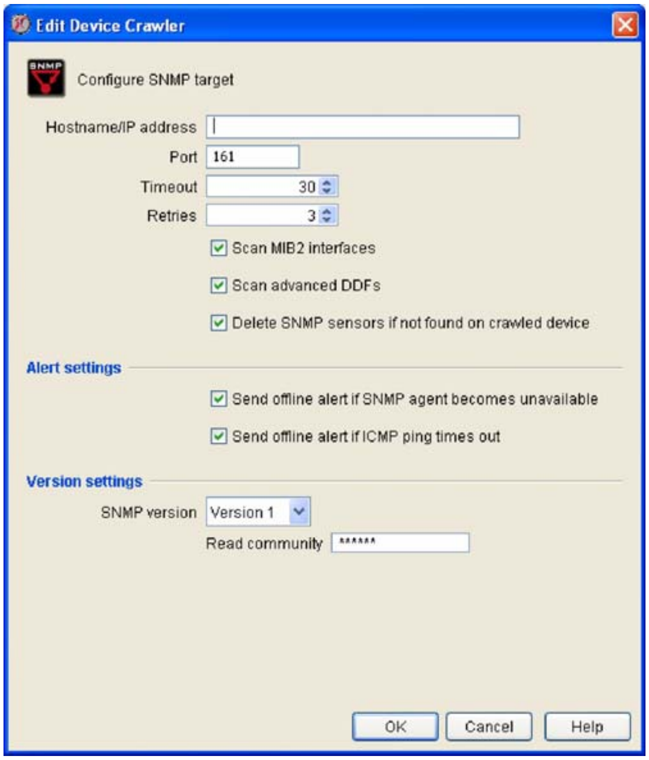
defined for each device.

2. To continue, select one device from the device selection window and click Edit.
3. The Device Crawlers Settings window opens. This window consists of three panes:
   - – The SNMP Targets pane: Enables you to add, edit, or remove SNMP targets for use with Device Crawlers.
   - – The Device Definition Files pane: Displays the names and versions of all Device Definition Files (DDFs) that are currently installed on the selected device, and enables you to download and install new or updated DDFs as they become available.
   - – The Supplemental OIDs pane: Enables you to configure Device Crawlers to monitor the SNMP value of any OID on an SNMP target.



Label	Hostname/IP Address	Port	Timeout	Retries	Last Scan...
159.215.80.129	159.215.80.129	161	30	3	6/1/06 10:...

4. Select the SNMP Targets pane and then click Add. The Add Device Crawler window opens.



Hostname/IP address

Port 161

Timeout 30

Retries 3

☑ Scan MIB2 interfaces

☑ Scan advanced DDFs

☑ Delete SNMP sensors if not found on crawled device

Alert settings

☑ Send offline alert if SNMP agent becomes unavailable

☑ Send offline alert if ICMP ping times out

Version settings

SNMP version Version 1

Read community ******

5. The following SNMP Target Settings are available:

Field	Description
Hostname/IP address	Type in this field the hostname or IP address of the SNMP target.
Port	Type in this field the port number used for SNMP communications on the target. The default value is 161.
Timeoutis seconds	Select the number of seconds that Device Crawlers will wait for a response from a target before Device Crawlers either retries communications or considers the target to be unresponsive. The default value is 30 seconds.
Retries	Select the number of times Device Crawlers will retry communications with an SNMP target that is not responding before considering the target to be unresponsive and moving on to the next target.
Delete SNMP sensors if not found on crawled device	When checked, automatically removes previously defined SNMP-based sensors on a target when, after a successful scan, the sensors are found to no longer be present (no longer defined, unavailable, and so forth). If the sensors are not deleted, they will be displayed with sensor reading values of “N/A” or “null.”
Include network interface status	Check this check box to include the network status of the SNMP target in the list of sensors that are available for use on the target device.
Scan advanced DDFs	To enable Advanced Device Crawler functionality on this SNMP target, check the Scan Advanced DDFs check box. Note: If you have not purchased and applied an Advanced Device Crawler license key, the Advanced Device Crawler functionality can be enabled only on a single SNMP target. If the Advanced Device Crawler functionality is already enabled on an SNMP target, you must first uncheck the Scan Advanced DDFs check box in the enabled target’s settings before you can enable it on another target.
Send offline alert if ICMP ping times out	Check this check box if you want Device Crawlers to generate an alert if ICMP Pings directed at the target device time out. If this time out occurs, the Device Crawlers Online sensor status for this device will report an Online status value of “No,” enabling you to configure thresholds and generate alert notifications in response to this status change.

Field	Description
Send offline alert if SNMP agent becomes unavailable	Check this check box if the monitored device has an SNMP agent and you want Device Crawlers to generate an alert if the device's SNMP agent on this target is unavailable. If the SNMP agent is unavailable, the Device Crawlers Online sensor status for this device will report an Online status value of “No,” enabling you to configure thresholds and generate alert notifications in response to this status change. Note: If the target device does not have an SNMP agent, be sure to leave this check box unchecked. If this check box is checked and the target does not have an SNMP agent the Online sensor status will always report a “No” value, regardless of whether the device is online or not.
SNMP Version	Select the version of SNMP that will be used to communicate with the target. You can select version 1, 2c, or 3.
Read community	Type in this field the read only community string used for SNMP communications on the target. The default value is public.

If you are editing a previously created SNMP target, the following additional SNMP Target Settings are available:

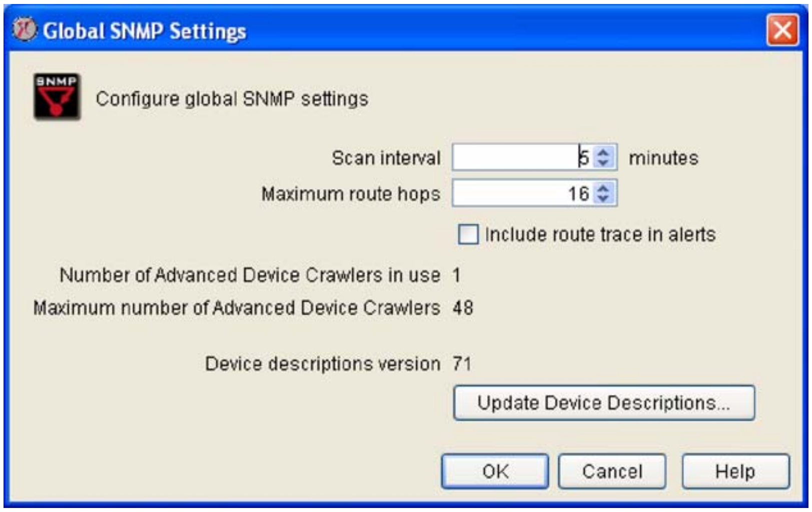
Field	Description
Label	A name that will be used to uniquely identify this SNMP target. By default, the SNMP target label is the IP address or hostname of the target.
Offline alert severity	Select the alert severity value that will be specified in alerts generated if the target goes offline.

6. When you are finished specifying settings for the SNMP target click Apply to save the all defined or modified SNMP target values to your device.

Once you have added an SNMP Target, you can use Advanced Device Crawlers to perform OID-specific monitoring on the target.

Specifying Global SNMP Settings

Click Global SNMP Settings to configure SNMP settings that will be used by Device Crawlers for all SNMP target communications. The Global SNMP Settings window opens.



Configure global SNMP settings

Scan interval 5 minutes

Maximum route hops 16

☐ Include route trace in alerts

Number of Advanced Device Crawlers in use 1

Maximum number of Advanced Device Crawlers 48

Device descriptions version 71

This window contains the following fields:

Field	Description
Scan Interval	Use this control to specify the number of minutes that must pass between Device Crawlers target queries.
Maximum Route Hops	Use this control to specify the maximum number of hops that will be recorded and saved by Device Crawlers route tracing support.
Include Route Trace in Alerts check box	Check this check box to enable Device Crawlers route tracing support. If this check box is not checked, route tracing is disabled and alert notifications will not include route tracing data.
Number of Advanced Device Crawlers in use	Total number of Advanced Device Crawlers being used to monitor remote SNMP targets.
Maximum number of Advanced Device Crawlers	Maximum number of Advanced Device Crawlers that can be configured on this device to monitor remote SNMP targets.
Device descriptions version	The version of the device descriptions data file currently stored on the device.
Update Device Descriptions button	Device Crawlers uses a device descriptions data file to identify the System Model, Type, and Vendor value for SNMP targets. NetBotz periodically updates the contents of the device descriptions file to include new or previously unidentified target types as they become available. Click Update Device Descriptions to contact the NetBotz web site (or browse to a local device descriptions update file) and update the content of the Device Crawlers device description file.

Type the appropriate values in the fields, and then click OK to save the global SNMP settings.

The Device Definition Files Pane

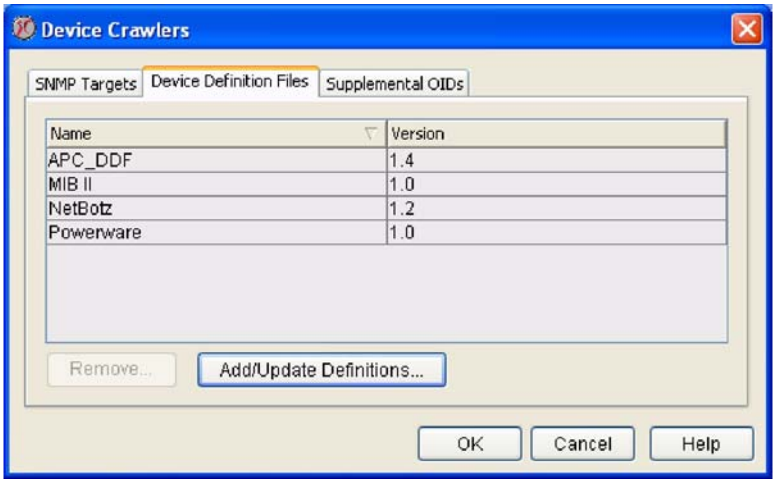
Device Crawlers greatly simplify the process of surfacing and monitoring environmental monitoring-oriented OIDs on supported SNMP device through the use of Device Definition Files, or DDFs. DDFs are specially prepared data files that isolate and surface the OIDs for specified devices that are of use for environmental monitoring purposes. Each DDF file is specifically designed to provide advanced data for a particular product set from a particular manufacturer. DDFs are downloaded and installed using the Device Definition Files pane in the Device Crawlers task.

The Device Definition Files pane includes the following information and controls:

Field	Description
Device Definition Files	Displays the name and version of all Device Definition Files that are currently installed on this device.
Add/Update Definitions	Click this button to download additional DDFs or updated DDFs for use with Advanced Device Crawlers.

To add a new Device Definition File:

1. Click Add/Update Definitions.
2. The Installation Options window appears. Select the location from which you want to download DDFs. Select the Check APC Website radio button to download DDFs from APC, or select the Local file radio button to install DDFs from a drive and directory on your system and then click Browse and navigate to the directory where the DDF file is stored. Select the DDF and click OK to select it.



Name	Version
APC_DDF	1.4
MIB II	1.0
NetBotz	1.2
Powerware	1.0

3. Click Next. A list of available Device Definition Files (including version numbers) appears. Select one or more DDFs that you want to install and use with Advanced Device Crawlers and then click Next.
4. A list of the DDFs you have selected appears. Click Next to download and install the selected DDFs.

After you have installed a Device Definition File any previously added targets that are defined by the contents of the DDF will now have the Advanced Data sensor set available.

The Supplemental OIDs Pane

Even if advanced data is not available for some of your SNMP targets, you can still configure Device Crawlers to monitor individual OIDs on your target. While not as simple as using the surfaced OID data provided by a Device Definition File in an Advanced Data sensor set, you can use the Add Supplemental OID function to manually configure Device Crawlers to monitor any valid OID on your SNMP targets.

The Supplemental OID view displays a list of any currently defined supplemental OIDs, as well as a user-defined description of the OID.

To add a supplemental OID:

1. Click Add. The Add Supplemental OID window opens.
2. Type in the OID field the OID that you want to monitor on the selected SNMP target (for example, “1.3.6.1.4.1.318.1.1.1.2.2.2”).
3. Type in the Description field a description of the OID (for example, “UPS Temperature”).
4. Click OK. Device Crawlers will then query the SNMP target to determine whether the OID you entered is valid and if so to determine what sort of data is returned by the OID, whether the data can be treated as an analog sensor or a state sensor, and so forth. If the OID is valid it will be added to the Advanced Data sensor set.

Once the supplemental OID has been added, it will automatically be detected on any SNMP target to which it applies, and you can easily monitor and receive alert notifications for it just like any other monitored value on a pod or SNMP target. To configure thresholds on values reported by a supplemental OID you must select the device to which the supplemental OID was added and then use either the Other Numeric Sensors or Other State Sensors task (depending on the nature of the data that is provided by the supplemental OID) to define thresholds for the sensor.

Device Scanner

Device Scanner provides highly sophisticated, in-depth monitoring of your supported SNMP physical layer devices. Like the Device Crawlers, Device Scanner enables you to configure your devices to monitor the general status information of SNMP targets. However, the number of SNMP devices that can be monitored using Device Scanners is far higher (up to a maximum of 1025 SNMP devices) and the amount of device-specific sensor and device status data that is surfaced and accessible when using Device Scanner far exceeds that which is available using the Device Crawlers scanning and reporting architecture.

Note

The Device Scanner task can be run only on one device at a time.

Using the Device Scanner Task

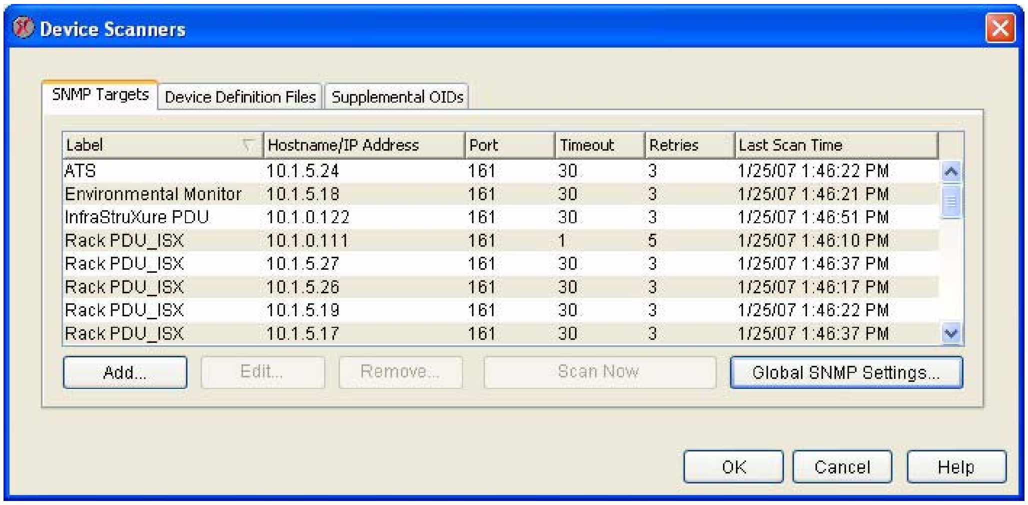
Instructions for using the Device Scanner task follow.

The SNMP Targets View

To define a new SNMP target (or modify a previously defined SNMP target) for use with Device Scanner:

1. Launch the Device Scanner task. In addition to the IP address/hostname and status of each selected device, the Device Scanner task's device selection window also includes one task-specific information column: Target Count, which displays the total number of SNMP targets that have been defined for each device.

2. To continue, select one device from the device selection window and click Edit.
3. The Device Scanner Settings window opens. This window consists of three panes:
   – The SNMP Targets pane: Enables you to add, edit, or remove SNMP targets for use with Device Scanner.
   – The Device Definition Files pane: Displays the names and versions of all Device Definition Files (DDFs) that are currently installed on the selected device, and enables you to download and install new or updated DDFs as they become available.
   – The Supplemental OIDs pane: Enables you to configure Device Scanner to monitor the SNMP value of any OID on an SNMP target.



Label	Hostname/IP Address	Port	Timeout	Retries	Last Scan Time
ATS	10.1.5.24	161	30	3	1/25/07 1:46:22 PM
Environmental Monitor	10.1.5.18	161	30	3	1/25/07 1:46:21 PM
InfraStruXure PDU	10.1.0.122	161	30	3	1/25/07 1:46:51 PM
Rack PDU_ISX	10.1.0.111	161	1	5	1/25/07 1:46:10 PM
Rack PDU_ISX	10.1.5.27	161	30	3	1/25/07 1:46:37 PM
Rack PDU_ISX	10.1.5.26	161	30	3	1/25/07 1:46:17 PM
Rack PDU_ISX	10.1.5.19	161	30	3	1/25/07 1:46:22 PM
Rack PDU_ISX	10.1.5.17	161	30	3	1/25/07 1:46:37 PM

4. Select the SNMP Targets pane, and then click Add (or select a previously defined SNMP target and click Edit). The Add SNMP Target window opens. The following SNMP Target Settings are available:

Field	Description
Hostname/IP address	Type in this field the hostname or IP address of the SNMP target.
Alert profile	Specify the Alert Profile that will be used to determine what alert notification actions will be taken in response to this threshold. By default, the Default Alert Profile is used for all thresholds. However, if you have created additional Alert Profiles you can specify that a threshold use an Alert Profile other than Default. **Note:** The Alert Profile drop box will appear in the Advanced tab only if additional Alert Profiles have been created.
Scan interval	Use this control to specify a device-specific scan interval for this device. The scan interval is the number of minutes that must pass between Device Scanner target queries. The default scan interval for all Device Scanner operations is specified using the Device Scanner Global SNMP Settings. For infomration Device Scanner Global SNMP Settings, see “Specifying Global SNMP Settings” on page 180.

Field	Description
Port	Type in this field the port number used for SNMP communications on the target. The default value is 161.
Timeout in seconds	Select the number of seconds that Device Scanner will wait for a response from a target before Device Scanner either retries communications or considers the target to be unresponsive. The default value is 30 seconds.
Retries	Select the number of times Device Scanner will retry communications with an SNMP target that is not responding before considering the target to be unresponsive and moving on to the next target.
Delete SNMP sensors if not found on crawled device	When checked, automatically removes previously defined SNMP-based sensors on a target when, after a successful scan, the sensors are found to no longer be present (no longer defined, unavailable, and so forth). If the sensors are not deleted, they will be displayed with sensor reading values of “N/A” or “null.”
Include network interface status	Check this check box to include the network status of the SNMP target in the list of sensors that are available for use on the target device.
Include network interface performance	If checked, Device Scanner will include network interface performance data in the list of sensors that are available for use on the target device.
SNMP Version	Select the version of SNMP that will be used to communicate with the target. You can select version 1, 2c, or 3.
Read community	Type in this field the read only community string used for SNMP communications on the target. The default value is public.

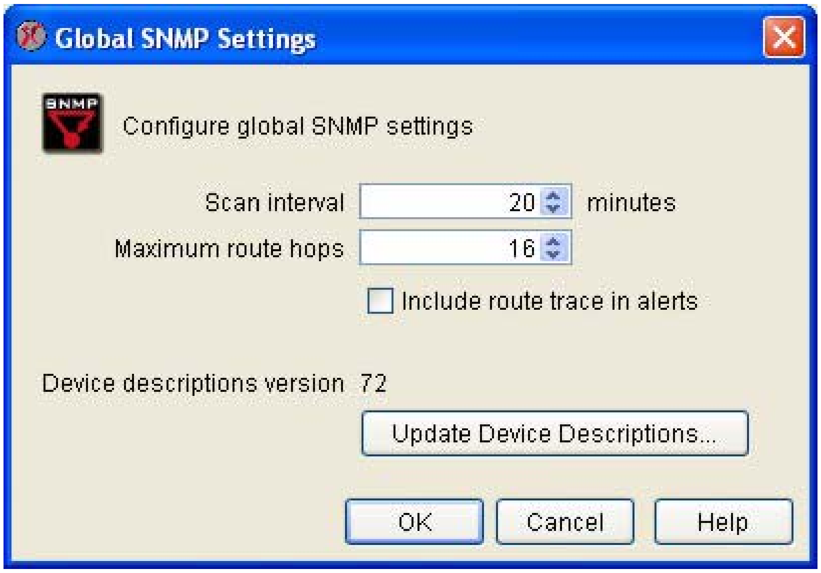
If you are editing a previously created SNMP target, the following additional SNMP Target Settings are available:

Field	Description
Label	A name that will be used to uniquely identify this SNMP target. By default, the SNMP target label is the IP address or hostname of the target.
Offline alert severity	Select the alert severity value that will be specified in alerts generated if the target goes offline.

5. When you are finished specifying settings for the SNMP target click Apply to save the all defined or modified SNMP target values to your device.

Specifying Global SNMP Settings

Click Global SNMP Settings to configure SNMP settings that will be used by Device Scanner for all SNMP target communications. The Global SNMP Settings window opens.



Global SNMP Settings

Configure global SNMP settings

Scan interval 20 minutes

Maximum route hops 16

□ Include route trace in alerts

Device descriptions version 72

This window contains the following fields:

Field	Description
Scan Interval	Use this control to specify the number of minutes that must pass between Device Scanner target queries.
Maximum Route Hops	Use this control to specify the maximum number of hops that will be recorded and saved by Device Scanner route tracing support.
Include Route Trace in Alerts check box	Check this check box to enable Device Scanner route tracing support. If this check box is not checked, route tracing is disabled and alert notifications will not include route tracing data.
Device descriptions version	The version of the device descriptions data file currently stored on the device.
Update Device Descriptions button	Device Scanner uses a device descriptions data file to identify the System Model, Type, and Vendor value for SNMP targets. NetBotz periodically updates the contents of the device descriptions file to include new or previously unidentified target types as they become available. Click Update Device Descriptions to contact the NetBotz web site (or browse to a local device descriptions update file) and update the content of the Device Scanner device description file.

Type the appropriate values in the fields, and then click OK to save the global SNMP settings.

The Device Definition Files Pane

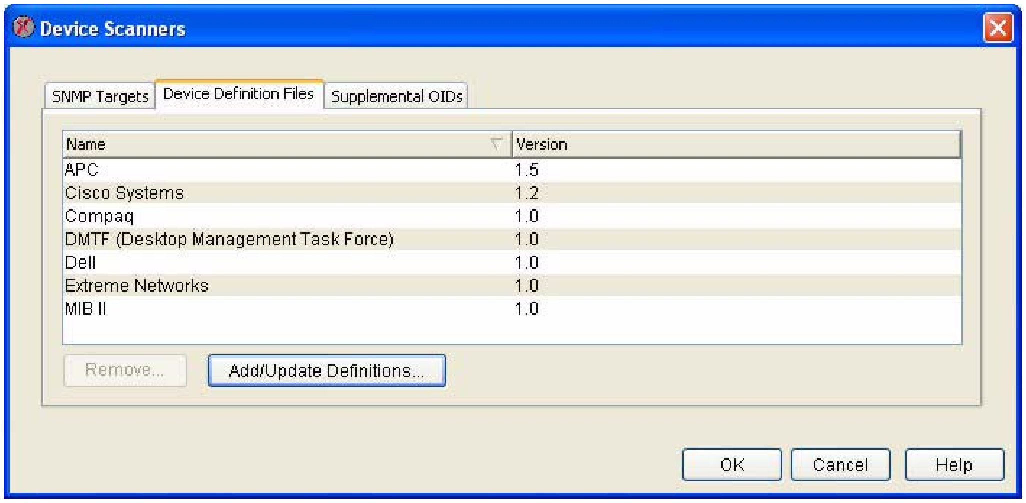
Device Scanner greatly simplifies the process of surfacing and monitoring environmental monitoring-oriented OIDs on supported SNMP device through the use of Device Definition Files, or DDFs. DDFs are specially prepared data files that isolate and surface the OIDs for specified devices that are of use for environmental monitoring purposes. Each DDF file is specifically designed to provide advanced data for a particular product set from a particular manufacturer.

The Device Definition Files pane includes the following information and controls:

Field	Description
Device Definition Files	Displays the name and version of all Device Definition Files that are currently installed on this device.
Add/Update Definitions	Click this button to download additional DDFs or updated DDFs for use with Device Scanner.

To add a new Device Definition File:

1. Click Add/Update Definitions.
2. The Installation Options window appears. Select the location from which you want to download DDFs. Select the Check APC Website radio button to download DDFs from APC, or select the Local file radio button to install DDFs from a drive and directory on your system and then click Browse and navigate to the directory where the DDF file is stored. Select the DDF and click OK to select it.



Name	Version
APC	1.5
Cisco Systems	1.2
Compaq	1.0
DMTF (Desktop Management Task Force)	1.0
Dell	1.0
Extreme Networks	1.0
MIB II	1.0

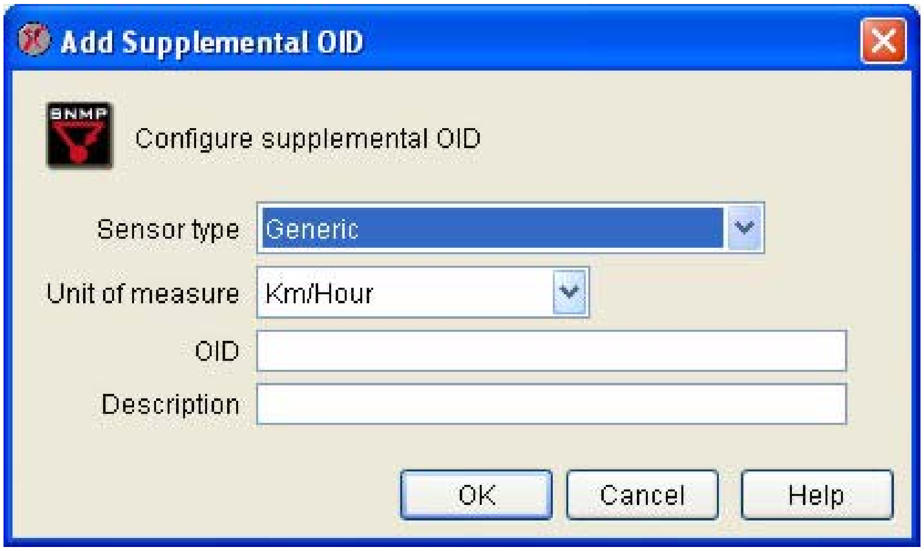
3. Click Next. A list of available Device Definition Files (including version numbers) appears. Select one or more DDFs that you want to install and use with Device Scanner and then click Next.
4. A list of the DDFs you have selected appears. Click Next to download and install the selected DDFs.

After you have installed a Device Definition File any previously added targets that are defined by the contents of the DDF will now have the Advanced Data sensor set available.

The Supplemental OIDs Pane

Even if advanced data is not available for some of your SNMP targets, you can still configure Device Scanner to monitor individual OIDs on your target. While not as simple as using the surfaced OID data provided by a Device Definition File in an Advanced Data sensor set, you can use the Add Supplemental OID function to manually configure Device Scanner to monitor any valid OID on your SNMP targets.

The Supplemental OID view displays a list of any currently defined supplemental OIDs, as well as a user-defined description of the OID.



Add Supplemental OID

Configure supplemental OID

Sensor type: Generic

Unit of measure: Km/Hour

OID:

Description:

To add a supplemental OID:

1. Click Add. The Add Supplemental OID window opens.
2. Select from the Sensor type drop box the type of sensor (temperature, humidity, air flow, and so on) that best matches the data that will be reported by the supplemental OID.
3. Select form the Unit of measure drop box the appropriate unit or measurement (degrees, seconds, volts, and so on) that will be used when reporting sensor data from the supplemental OID.
4. Type in the OID field the OID that you want to monitor on the selected SNMP target (for example, "1.3.6.1.4.1.318.1.1.1.2.2.2").
5. Type in the Description field a description of the OID (for example, "UPS Temperature").
6. Click OK to save the supplemntal OID.

Once the supplemental OID has been added, it will automatically be detected on any SNMP target to which it applies, and you can easily monitor and receive alert notifications for it just like any other monitored value on a pod or SNMP target. To configure thresholds on values reported by a supplemental OID you must select the device to which the supplemental OID was added and then use either the Other Numeric Sensors or Other State Sensors task (depending on the nature of the data that is provided by the supplemental OID) to define thresholds for the sensor.

DNS

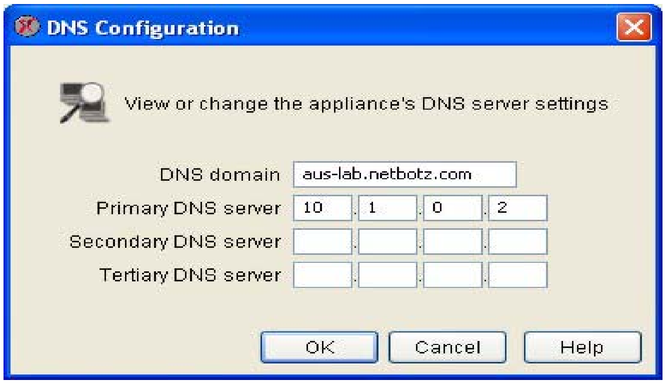
Use the DNS task to view or change the domain name server settings used by selected devices. To use the DNS task:

1. Launch the DNS task. In addition to the IP address/hostname and status of each selected device, the DNS task's device selection window also includes two task-specific information columns:

– DNS Domain: Specifies the DNS domain name to which this device belongs.

– Primary DNS Server: Specifies the IP address of the primary domain name server.

2. To continue, select one or more devices from the device selection window and click Edit.



DNS Configuration

View or change the appliance's DNS server settings

DNS domain: aus-lab.netbotz.com

Primary DNS server: 10 . 1 . 0 . 2

Secondary DNS server: . . .

Tertiary DNS server: . . .

3. The DNS Settings window opens. This window contains the following fields:

Field	Description
DNS domain	The DNS domain name to which this device belongs.
Primary DNS server	The IP address of the primary domain name server.
Secondary DNS server	The IP address of the secondary domain name server.
Tertiary DNS server	The IP address of the tertiary domain name server.

4. Type the new DNS settings in the appropriate fields. When you are finished, click OK to save any these settings to the selected devices. Click Cancel to close this window without saving any changes.

E-mail Server

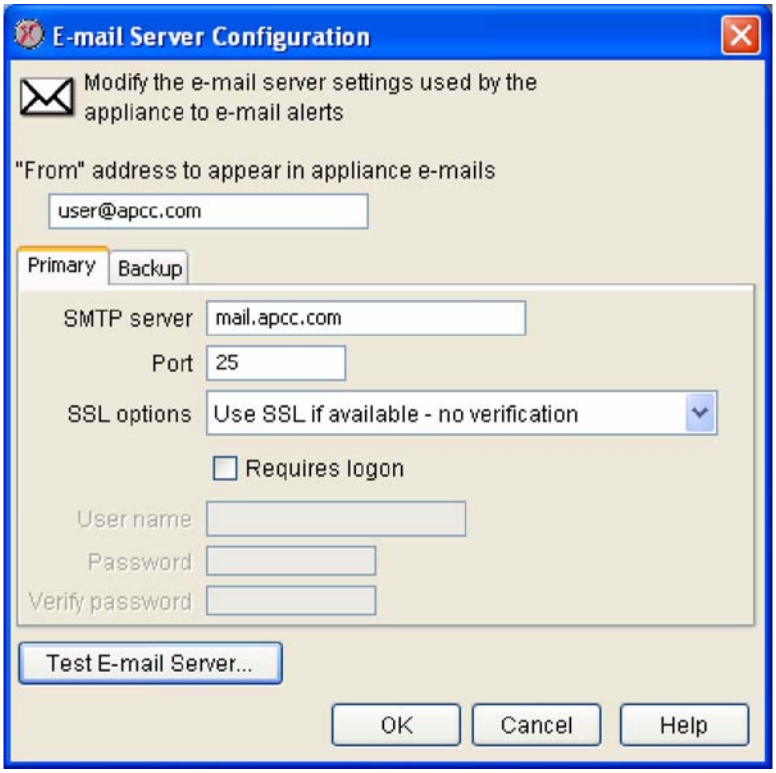
Use the E-mail Server task to specify the e-mail address that will appear in the “From” field of any e-mails generated by the InfraStruXure Central server and to specify primary and backup mail servers that will be used to deliver any e-mail notifications.

To use the E-mail Server task:

1. Launch the E-mail Server task. In addition to the IP address/hostname and status of each selected device, the DNS task's device selection window also includes two task-specific information

columns:

- Primary SMTP Server: Specifies the IP address or hostname of the primary SMTP server used to send e-mail.
- Backup SMTP Server: Specifies the IP address or hostname of the backup SMTP server used to send e-mail.



E-mail Server Configuration

Modify the e-mail server settings used by the appliance to e-mail alerts

"From" address to appear in appliance e-mails: user@apcc.com

Primary | Backup

SMTP server: mail.apcc.com

Port: 25

SSL options: Use SSL if available - no verification

□ Requires logon

User name:

Password:

Verify password:

2. To continue, select one or more devices from the device selection window and click Edit.
3. The E-mail Server Configuration window opens. This window contains two tabbed panes, labeled Primary and Backup. Use the controls on the Primary tab to specify the primary SMTP server settings, and use the controls on the Primary tab to specify the backup SMTP server settings. Each

tab includes the following fields:

Field	Description
From address	The e-mail address that will appear in the “From” field of any e-mail generated by the InfraStruXure Central server.
SMTP server	The IP address of the SMTP server used to send E-mail.
Port	The IP port on the e-mail server used for SMTP communications.
SSL options	Select from this drop box the selection that corresponds to the SSL communication options that you want to apply to communications between the device and the SMTP server. You can choose the following options: • SSL disabled: Do not use SSL for mail delivery, even if supported • Use SSL if available: Attempt to use SSL if the server supports it, but proceed with un-encrypted delivery otherwise. If SSL is used, no certificate verification is required. This is the default. • Require SSL: No verification: Require SSL support on the server (do not deliver without it), but accept any certificate provided by the server (i.e. self signed certificates will be allowed). • Require SSL - verify certificate: Require SSL support on the server (do not deliver without it), and only accept certificates signed by a trusted certificate authority (i.e. self signed certificates will not be allowed, but Verisign and the like certificates will be accepted even if the hostname does not match the host in the certificate). • Require SSL - verify certificate and hostname: Require SSL support on the server (do not deliver without it), and only accept certificates signed by a trusted certificate authority and which contain a hostname matching that used to contact the server (i.e. only certificates issued by trusted sources and which contain the same hostname as used to access the server are allowed).
Requires logon check box	Check this check box if the server requires you to log in to send e-mail.
User name	Provide a user name that will be accepted by the SMTP server when sending e-mail.
Password	Provide a password that will be accepted by the SMTP server when sending e-mail.
Verify password	Type the password again to verify.

4. To change the InfraStruXure Central server E-mail Server settings, type the new values in the appropriate fields. When you are finished, click OK to save any changes to the device. Click Test E-mail Server to test your e-mail server settings. Click Cancel to close this window without saving any changes.

External Ports

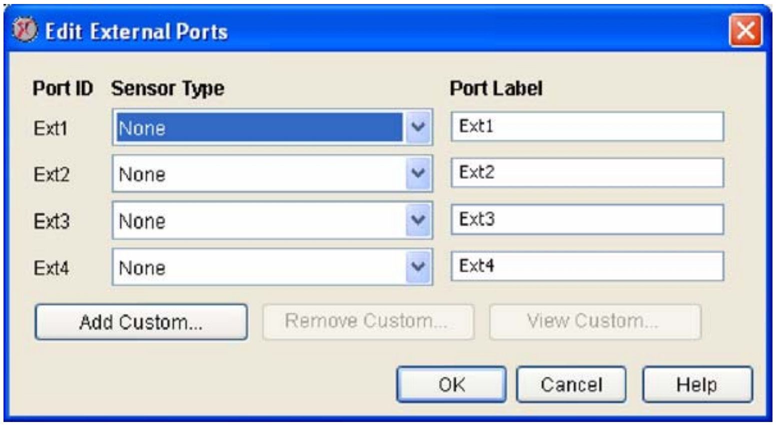
Use the External Ports task to specify the type of external sensors that are attached to each of the external sensor ports that are integrated with your Sensor Pod 120s and NetBotz devices, and to provide a unique identification label for each external sensor. You can use this task to define custom dry contact sensors.

Note

The External Ports task can be run only on one device at a time.

To use the External Ports task:

1. Launch the External Ports task. In addition to the IP address/hostname and status of each selected device, the DNS task's device selection window also includes two task-specific information columns:
   - – Monitored Device: The label that is assigned to the device, if any.
   - – Port count: The number of external sensor ports available on the device.
2. To continue, select a device from the device selection window and click Edit.
3. The Edit External Ports window opens.



Port ID	Sensor Type	Port Label
Ext1	None	Ext1
Ext2	None	Ext2
Ext3	None	Ext3
Ext4	None	Ext4

4. Select from the drop box beside the External Sensor Port ID the specific external sensor that is connected to each port. If desired, type in the Port Label field a label that will be used to uniquely identify the sensor and port to which it is connected.
5. To add a custom dry contact or analog sensor, click Add Custom.

When you have finished, click OK to save your new threshold settings.

Defining Custom Dry Contact and Analog Sensors

If the predefined output dry contact or analog sensor types do not meet your needs, you can create custom sensor definitions. Once defined and saved, the new sensor definition will be available for selection from the Sensor Type Installed drop box when specifying Sensor Pod external port settings, enabling you to use this new sensor definitions for all additional dry contact or analog sensors of the same type.

To add a custom sensor:

1. Click Add custom.... The Select Sensor Type window opens. Next, select the radio button that corresponds to the type of sensor you want to define (Dry Contact, Analog (0-3.3V), Analog (0-

5.0V), or 4-20mA) and click OK.

2. You can create the following custom dry contact or analog sensor types:
   - 0-3.3V analog sensor
   - 0-5.0V analog sensor
   - dry contact sensor
   - 4-20mA sensor

Defining a Custom 0-3.3V or 0-5.0V Analog Sensor

Note

Once a custom analog sensor is added, it cannot be edited. Custom sensors can only be added or removed. You can view the custom sensor settings for selected sensors by clicking View.

After you select Analog (0-3.3V) or Analog (0-5.0V) and click OK, the Add Analog Sensor window opens. This window features the following fields and controls:

Field	Description
Sensor type label	The label represents the name of the custom sensor definition. For example, if you are creating a custom sensor definition for use with temperature sensor Model 42 from MyCo, Inc., you might want to use “MyCo Model 42 Temperature Sensor” as the Sensor Type Label. Once defined, the Sensor Type Label appears only in the Sensor Type Installed drop box when specifying Sensor Pod external port settings.
Default sensor label	This is the text that is used, by default, as a label for any new sensors added using this custom sensor definition. This label is used to identify each individual sensor in the Sensor Readings pane, as well as in all interfaces and alert notifications. Once a sensor has been added to your device, you can use the Monitored Device Settings task to modify the labels for easier sensor-specific identification.
Volts 1 / sensor value and Volts 2 / sensor value	Use the Volts 1 / Sensor Value and Volts 2 / Sensor Value fields to specify 2 reference points (between 0 and 3.3 volts for 0-3.3V analog sensor and between 0 and 5.0 volts for 0-5.0V analog sensors) for the sensor readings. Using these two points, the device will use linear interpolation to determine the full range of sensor values that correspond to the voltage readings reported by the sensor. For example, if you specify Volts 1 /Sensor Value as “1.0” and “10”, and Volts 2/ Sensor Value as “2.0” and “20,” then the device can determine that a voltage reading of 3.1 from the analog sensor represents a sensor value of 31.
Minimum sensor value	The lowest value that will be reported by the sensor.
Maximum sensor value	The highest value that will be reported by the sensor.
Sensor increment	The numeric increments in which the sensor reading rises falls.

Field	Description
Units	The unit of measurement that is used for this sensor.

Type in the appropriate values for the analog sensor hardware. When you have finished, click OK to add this sensor definition to the list of available Sensor Types.

Defining a Custom Dry Contact Sensor

Note

Once a custom dry contact sensor is added, it cannot be edited. Custom dry contact sensors can only be added or removed. You can view the custom sensor settings for selected sensors by clicking View.

After you select Dry Contact and click OK, the Add Dry Contact Sensor window opens. This window features the following fields and controls:

Field	Description
Sensor label	The text used to identify this sensor definition in the Sensor Types selection list and in the External Sensors task.
Attribute label	The text used to identify the data provided by this sensor in the Sensor Readings pane and in alerts generated by this sensor.
Closed value	The text used to describe the sensor value that is reported when the dry contact sensor is in a Closed state. For example, if you are defining a motion detector sensor that is normally closed (NC), the Value Label (Closed) text could read “None” or “No motion” or “OK.”
Open value	The text used to describe the sensor value that is reported when the dry contact sensor is in a Open state. For example, if you are defining a motion detector sensor that is normally closed (NC), the Value Label (Open) text could read “Detected” or “Motion” or “Alert!”
Open-close switch time (ms)	The amount of time that must pass (in milliseconds) when the dry contact sensor goes from Open state to Closed state before the state change is reported.
Close-open switch time (ms)	The amount of time that must pass (in milliseconds) when the dry contact sensor goes from Closed state to Open state before the state change is reported.
Dry contact type	Specifies whether the dry contact sensor is a normally open (NO) or normally closed (NC) dry contact sensor.

To create a new dry contact sensor definition, type in the appropriate values for the dry contact sensor hardware. When you have finished, click OK to add this sensor definition to the list of available Sensor Types.

Defining a Custom 4-20mA Sensor

Note

Once a custom 4-20mA sensor is added, it cannot be edited. Custom 4-20mA sensors can only be added or removed. You can view the custom sensor settings for selected sensors by clicking View.

After you select 4-20mA and click OK, the Add Custom 4-20mA Sensor window opens. This window features the following fields and controls:

Field	Description
Sensor type label	The label represents the name of the custom sensor definition. For example, if you are creating a custom sensor definition for use with temperature sensor Model 42 from MyCo, Inc., you might want to use “MyCo Model 42 Temperature Sensor” as the Sensor Type Label. Once defined, the Sensor Type Label appears only in the Sensor Type Installed drop box when specifying Sensor Pod external port settings.
Default sensor label	This is the text that is used, by default, as a label for any new sensors added using this custom sensor definition. This label is used to identify each individual sensor in the Sensor Readings pane, as well as in all interfaces and alert notifications. Once a sensor has been added to your device, you can use the Monitored Device Settings task to modify the labels for easier sensor-specific identification.
mA 1 / sensor value and mA 2 / sensor value	Use the mA 1 / Sensor Value and mA 2 / Sensor Value fields to specify 2 reference points (between 4 and 20 mA) for the sensor readings. Using these two points, the device will use linear interpolation to determine the full range of sensor values that correspond to the voltage readings reported by the sensor.
Minimum sensor value	The lowest value that will be reported by the sensor.
Maximum sensor value	The highest value that will be reported by the sensor.
Sensor increment	The numeric increments in which the sensor reading rises or falls.
Units	The unit of measurement that is used for this sensor.

Type in the appropriate values for the analog sensor hardware. When you have finished, click OK to add this sensor definition to the list of available Sensor Types.

External Storage

Use the External Storage task to configure your device to store data on the optional Extended Storage System (sold separately, for use only with NetBotz 500 devices) or a network attached storage device (a Windows share or an NFS mount). A maximum of 5000 objects (such as alerts and picture clips) can be stored using External Storage. Sensor readings do not count against the maximum number of object stored.

Note

- The External Storage task can be run only on one device at a time.
- Before you can use this task to configure a device that is using an Extended Storage System, you must activate the External Storage task on the device using the license key you received when you purchased the Extended Storage System. The Extended Storage System is available for use only on NetBotz 500 devices.

You can use this task to:

- Use an Extended Storage System (a USB drive that is connected directly to your NetBotz 500 USB port) for extended storage
- Use network attached storage (NAS) for extended storage. The following NAS implementations are supported:
  - MS Windows 2000 / XP / 2003
  - MS Windows Storage Server
  - Samba V2.2.6 or later (on Linux)
  - NFS V3.x or later
- Remove previously configured extended storage

Note

Not all NAS devices that work with Windows systems necessarily use one of the supported implementations. Also, some devices may use proprietary protocols and standards that require additional drivers in order to communicate with the share. Therefore, some NAS devices may not be mountable or usable.

Configuring Your Device to Use External Storage

To configure your device to use an Extended Storage System or NAS for extended storage:

1. Launch the External Storage task. In addition to the IP address/hostname and status of each selected device, the External Storage task's device selection window also includes one task-specific information column: Status, which displays the current status of any external storage that has been defined for use with the selected devices.
2. To continue, select a device from the device selection window and click Edit.
3. The External Storage window opens. Click Add... to continue.
4. The Select Storage Type pane appears. Three selections are available:
   - USB Drive: Configures the device to use an Extended Storage System for extended storage. Your device cannot be configured to use an Extended Storage System until you have used the License

Keys task to activate the External Storage task, using the license key you received when you purchased the Extended Storage System and the USB drive has been connected to the device.

- Windows Share: Configures the device to use a Windows file system share on a NAS as extended storage.
- NFS Mount: Configures the device to use an NFS Mount on a NAS as extended storage.

5. Select the desired storage type and then refer to the appropriate section that follows for additional instructions.

Using an Extended Storage System

To configure your device to use an Extended Storage System for extended storage:

1. Select USB Drive from the Select Storage Type pane and then click Next.
2. The Select Operation pane appears. Two selections are available:
   - Use Extended Storage: Configure the device to use the Extended Storage System without formatting the file system first. Can be used if the Extended Storage System you have connected to your device has previously been formatted and contains camera and sensor data already.
   - Format and Use Extended Storage: Formats the Extended Storage System’s file system and then configures the device to use the Extended Storage System.
3. Select the operation you wish to perform and then click OK.
   - If you selected Use Extended Storage, a confirmation message appears advising you that the device will need to restart to complete the task. Click Finish to restart the device. When the restart is complete all Extended Storage System functionality will be available for use.
   - If you selected Format and Use Extended Storage, a confirmation message appears, advising you that formatting the extended storage device will destroy any data stored on the device and that formatting can take 10 or more minutes to complete, after which the device must restart to begin using extended storage. Click Finish to complete this task. Once the Extended Storage System is formatted, your device will restart automatically. When the restart is complete all External Storage functionality will be available for use.

Using a Windows Share

Because problems can occur with your NAS devices that would adversely affect device behavior, be sure to use the Backup task to back up the device configuration before using External Storage to configure the device to use a Windows share. This will help ensure that, should you encounter problems with the Windows share, you can easily restore your device to an operational state.

To configure your device you use network attached storage for extended storage purposes:

1. Select Windows Share from the Select Storage Type pane and then click Next.
2. The Windows Share Settings pane appears. This pane features the following fields and controls:

Field	Description
Remote hostname/IP	The hostname or IP address of the Windows share.
Remote share name	The name of the Windows share.
Subdirectory (optional)	The subdirectory in the Windows share that will be used to store data. If no subdirectory is specified, data will be stored in the root directory of the share.
Domain or computer name	The domain to which the Windows share is connected.
User name	The user name required to access the Windows share.
Password / Verify password	The Password that is required to access the Windows share.
Use all available space check box	If checked, the device will not delete data from the share until all available space on the share has been exhausted. If unchecked, use the Limit space to (MB) and Allocation Unit controls to specify how much space on the share will be allocated for use by the device.

3. Once you’ve filled in all of the required information, click Next to continue.
4. The Select Action pane appears. Two selections are available:
   - Use network extended storage: Configure the device to use the specified Windows share without clearing the share of data first.
   - Initialize: Clears all existing data from the Windows share and then configures the device to use the Windows share.
5. Select the operation you wish to perform and then click OK.

Using an NFS Mount

Because problems can occur with your NAS devices that would adversely affect device behavior, be sure to use the Backup task to back up your device configuration before using External Storage to configure the device to use a NFS mount. This will help ensure that, should you encounter problems with the NFS mount, you can easily restore your device to an operational state.

To configure your device you use network attached storage for extended storage purposes:

1. Select NFS Mount from the Select Storage Type pane and then click Next.
2. The NFS Settings pane appears. This pane features the following fields and controls:

Field	Description
Remote hostname/IP	The hostname or IP address of the NAS.
Remote share name	The name of the NFS mount on the NAS.

Field	Description
Subdirectory (optional)	The subdirectory in the NFS mount that will be used to store data. If no subdirectory is specified, data will be stored in the root directory of the mount.
Authenticate using UID check box	Check this check box to authenticate all device access to the mount using UID. If checked, be sure to specify the correct UID value as well.
Use all available space check box	If checked, the device will not delete data from the mount until all available space on the mount has been exhausted. If unchecked, use the Limit space to (MB) and Allocation Unit controls to specify how much space on the mount will be allocated for use by the device.

3. Once you've filled in all of the required information, click Next to continue.
4. The Select Action pane appears. Two selections are available:
   – Use network extended storage: Configure the device to use the specified NFS mount without clearing the share of data first.
   – Initialize: Clears all existing data from the NFS mount and then configures the device to use the NFS mount.
5. Select the operation you wish to perform and then click OK.

Removing External Storage

To remove a previously added and configured NAS or Extended Storage System from your device:

1. Start the External Storage task and then click Stop Using. The following confirmation message appears: "Remove configured drive? This will cause the device to reboot."
2. Click OK to remove the Extended Storage System. Your device will restart automatically.
3. If you are removing an Extended Storage System, power off your device. Then, unplug the Extended Storage System USB cables from the device and power your device on again.

IP Filter

Use the IP Filter task to limit access to your device to users connecting from specified IP addresses or IP address ranges. By default, clients from any IP address can attempt to access your device. While access to the device is granted only when appropriate user account IDs and passwords are provided, IP Filtering provides additional security by preventing connections from IP addresses that do not meet the IP filter criteria you specify.

Note

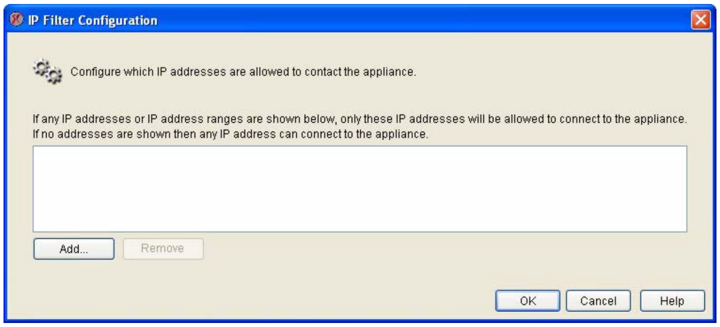
• The IP Filter task can be run only on one device at a time.
• If no IP Filter criteria are specified, then connections from all IP addresses are permitted.

To use the IP Filter task:

1. Launch the IP Filter task. In addition to the IP address/hostname and status of each selected device, the IP Filter task's device selection window also includes one task-specific information column:

Status, which reports whether an IP filter is currently enabled for use on this device.

2. To continue, select a device from the device selection window and click Edit.
3. The IP Filter Configuration window opens.



IP Filter Configuration

Configure which IP addresses are allowed to contact the appliance.

If any IP addresses or IP address ranges are shown below, only these IP addresses will be allowed to connect to the appliance.
If no addresses are shown then any IP address can connect to the appliance.

4. To specify IP Filter criteria, click Add and then specify an IP that will be permitted access. You can also use wildcards to specify a range of addresses. For example, providing an address of 192.168.1.* would permit connections only from clients with an IP address of 192.168.1.0 through 192.168.1.255. Or, if you were to specify 192.168.1.1/24 connections would be permitted only from clients with IP addresses of 192.168.1.1 through 192.168.1.24.
5. After you have types in the IP address, click OK to add the address value to the list of IP Filter criteria. When you have finished specifying IP Filter values, click OK save any changes to the device. Click Cancel to close this window without saving any changes.

IPMI Devices

Use the IPMI Devices task to add network-attached, Intelligent Platform Management Interface-enabled devices to the list of devices that are monitored by your NetBotz device. The Intelligent Platform Management Interface (IPMI) standard defines a hardware and software management interface and implementation that provide different hardware platforms with compatible server management and control functions. The IPMI standard is promoted and supported by over 150 server manufacturers. Once IPMI devices are added, you can set thresholds, monitor alerts, and graph data reported by the IPMI-enabled device's IPMI interface (such as system temperatures, voltages, fans, power supplies, bus errors, system physical security, and so forth), just as with pods and other sensors.

Note

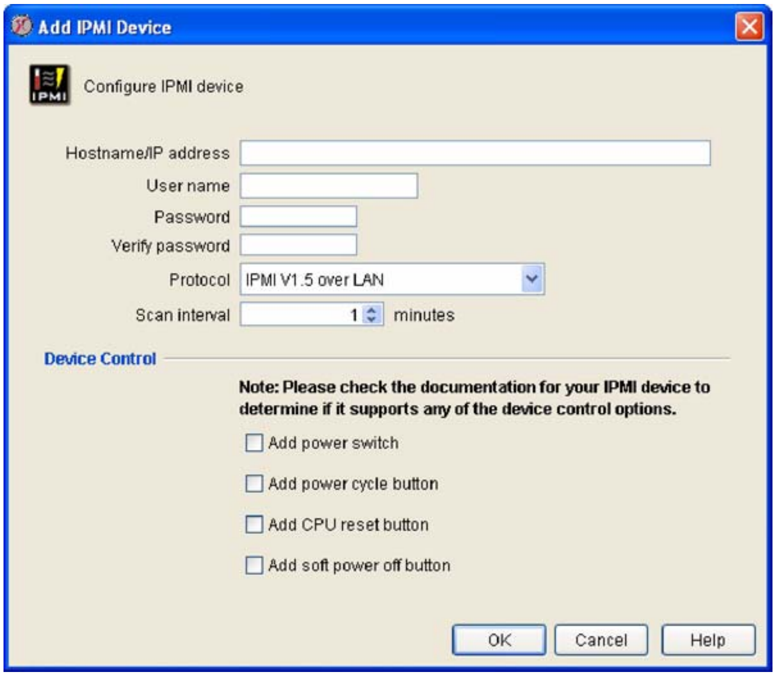
The IPMI Devices task can be run only on one device at a time.

To use the IPMI Devices task:

1. Launch the IPMI Devices task. In addition to the IP address/hostname and status of each selected device, the IPMI Devices task's device selection window also includes one task-specific information column: Target Count, which displays the number of IPMI devices have been defined for use with

the device.

2. To continue, select a device from the device selection window and click Edit.
3. The IPMI Device Configuration window opens.



Add IPMI Device

Configure IPMI device

Hostname/IP address

User name

Password

Verify password

Protocol IPMI V1.5 over LAN

Scan interval 1 minutes

Device Control

Note: Please check the documentation for your IPMI device to determine if it supports any of the device control options.

□ Add power switch

□ Add power cycle button

□ Add CPU reset button

□ Add soft power off button

4. To add a new IPMI device, click Add. To edit a previously created target, select the device from the IPMI Devices selection list and then click Edit.
5. The Add (or Edit) IPMI Devices window opens. This window contains the following fields:

Field	Description
Hostname/IP address	Type in this field the hostname or IP address of the IPMI-enabled device.
User name	Type in this field the user name that, along with the appropriate password, will be used to access the IPMI interface on the IPMI-enabled device.
Password / Verify password	Type in this field the password that, along with the appropriate user name, will be used to access the IPMI interface on the IPMI-enabled device.
Protocol	Select from the drop box that IPMI protocol that will be used to communicate with the IPMI interface on the IPMI-enabled device. You can select any of the following protocols: • IPMI V1.5 over LAN • IPMI V1.5 over LAN for Intel V2 BMCs • IPMI V2.0 over LAN • IPMI V2.0 over LAN for Intel V2 BMCs • SuperMicro IPMI V1.5 over LAN
Scan interval	Specify how frequently the device should query IPMI device for data. Note: You can force the device to do a scan at any time by click Scan Now in the IPMI Device Configuration window.

6. Type the appropriate values in the fields, and then click OK to save the settings for this IPMI-enabled device.

To remove previously created IPMI devices from the IPMI Devices selection list, select one (or more) IPMI-enabled devices from the list and then click Remove.

License Keys

Use the License Keys task to activate or deactivate license key-enabled applications that are available for use on this device.

Note

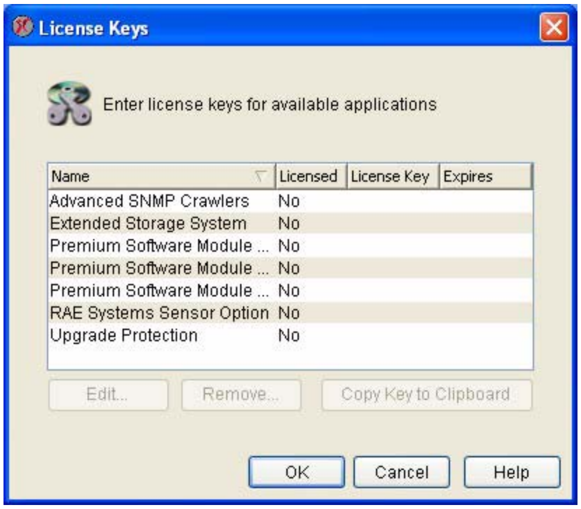
The License Keys task can be run only on one device at a time.

To use the License Keys task:

1. Launch the License Keys task. In addition to the IP address/hostname and status of each selected device, the License Key task's device selection window also includes one task-specific information column: Licensed Functions, which displays the names of any licensed functionality that has been enabled for use on the device.
2. To continue, select a device from the device selection window and click Edit.
3. The License Keys window opens. This window contains a table that includes the following information:

Field	Description
Name	The name of the license key-enabled functionality that is available for use on the selected device.
Licensed	Indicates whether the functionality has been enabled on the selected device.
License Key	If the functionality has been enabled this field displays the alphanumeric license key that was used to enable the functionality.
Expires	If the functionality has been enabled this filed displays the date, if any, on which the license key expires.

To enable functionality using a license key you have purchased or to edit a previously entered license key, select from the License Keys window the name of the license key-enabled functionality, click Edit..., type the license key into the window that appears, and click OK.



Enter license keys for available applications

Name	Licensed	License Key	Expires
Advanced SNMP Crawlers	No		
Extended Storage System	No		
Premium Software Module ...	No		
Premium Software Module ...	No		
Premium Software Module ...	No		
RAE Systems Sensor Option	No		
Upgrade Protection	No		

To remove a previously entered license key, select from the License Keys window the name of the license key-enabled functionality, click Remove..., and then confirm that you want to remove the license key.

To copy a previously entered license key to your system clipboard, select from the License Keys window the name of the license key-enabled functionality and then click Copy Key to Clipboard.

Location

Use the Location task to configure additional sensor-specific location information that will also be included in alert notifications generated by your devices. Location values can be assigned to your NetBotz device as well as any pods, external sensors, or other monitored devices that are connected to the base stations. Location settings for pods and sensors can be inherited from their “parent” (for example, a pod can inherit Location settings from a NetBotz 500, or a sensor can inherit Location setting from the Sensor Pod 120 to which it is connected), or you can specify pod-specific and sensor-specific Location settings as well.

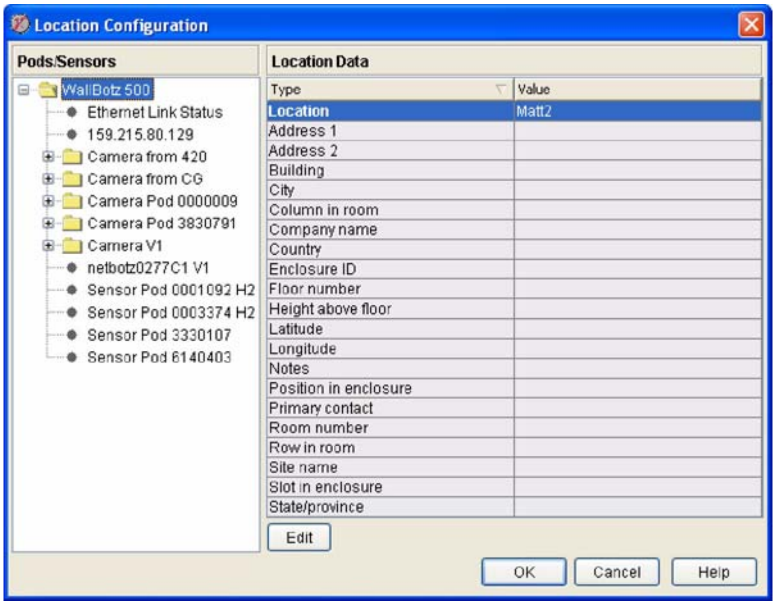
To use the Location task:

1. Launch the Location task. In addition to the IP address/hostname and status of each selected device, the Location task's device selection window also includes one task-specific information column: Appliance Location, which displays the location value that is currently assigned to each device in the list.
2. To continue, select one or more devices from the device selection window and click Edit.
3. The Location Configuration window opens. The following controls are available from the Location

Configuration task:

Field	Description
Pods/Sensors selection tree	Use this tree to select the device for which you wish to specify location settings.
Location Data: Type	A list of location settings that are available for the currently selected device to which you can assign additional information attributes.
Location Data: Value	The currently assigned location value for each of the location settings available for the selected device. If no location value has been specified, the value field beside the location data type is blank. By default, pods and sensors will inherit all location values from their parent object (the device to which they are connected).

4. Select the device for which you wish to specify location values from the Pods/Sensors selection tree.



Location Configuration

Pods/Sensors

- WallBotz 500
  - Ethernet Link Status
  - 159.215.80.129
  - Camera from 420
  - Camera from CG
  - Camera Pod 0000009
  - Camera Pod 3830791
  - Camera V1
  - netbotz0277C1 V1
  - Sensor Pod 0001092 H2
  - Sensor Pod 0003374 H2
  - Sensor Pod 3330107
  - Sensor Pod 6140403

Location Data

Type	Value
Location	Matt2
Address 1	
Address 2	
Building	
City	
Column in room	
Company name	
Country	
Enclosure ID	
Floor number	
Height above floor	
Latitude	
Longitude	
Notes	
Position in enclosure	
Primary contact	
Room number	
Row in room	
Site name	
Slot in enclosure	
State/province	

5. Select the desired location data type and click Edit to open the Edit Location Attribute window.

6. Type in the new location value and click OK to the Edit Location Attribute window. When you have finished specifying Location values, click OK save any changes to the selected devices. Click Cancel to close this window without saving any changes.

Log

Use the Log task to specify the log level for your devices. The log level determines what events will be stored and displayed in the device log. When you select a log level, it instructs the device to save only events that have a log value that is equal to or lower than the selected log level value. Therefore, if you select a lower log level value, fewer events will be recorded in the device log. For example, if you select a log level of 6 - Notice, all events that have a log level of 6 or lower will be recorded in the log, while events that have a log level of 7 or 8 will not be recorded.

The log level values are:

- 1 - Emergency
- 2 - Alert
- 3 - Critical
- 4 - Error
- 5 - Warning
- 6 - Notice
- 7 - Information
- 8 - Trace

We strongly recommend that you use a minimum log level of 6 - Notice. This will ensure that log messages that are associated with alerts are recorded in the log.

Device logging capabilities are also broken out into specific components and/or functions. By default, all components log at the level specified by the Global Level setting. However, you can also specify a unique log level setting for each component. Note that the components that are available for logging are determined by device model and user access privileges. Therefore, some items may not be available on some models or to some user accounts.

You can also configure the device to post log data to a remote syslog server. Syslog is a comprehensive logging system that is used to manage information generated by the kernel and system utilities in your network. Syslog enables you to sort messages based on their source or their importance, and also enables you to route messages to other destinations within your network. When the syslog functionality is enabled, all events that are stored in the Audit Trail will also be forwarded to a remote syslog host for logging to a user-specified syslog facility.

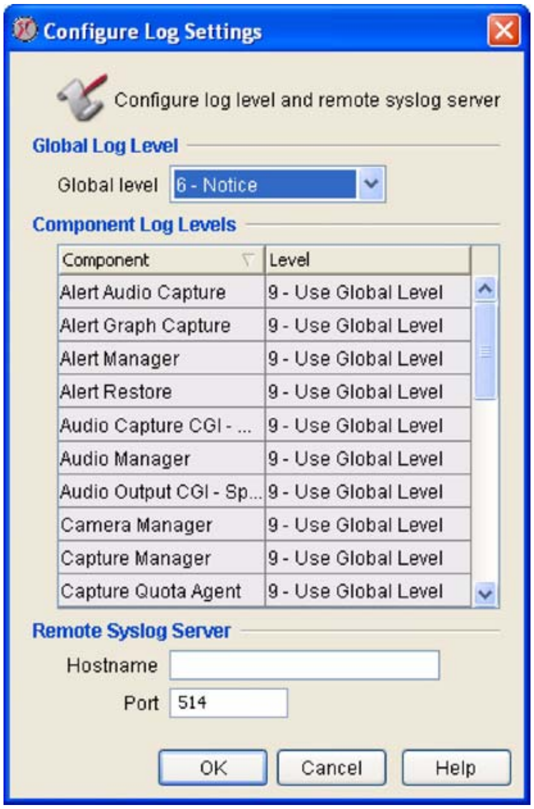
To use the Log task:

1. Launch the Log task. In addition to the IP address/hostname and status of each selected device, the Log task's device selection window also includes two task-specific information columns:
   - Log Level: Displays the currently set log level value for the device.
   - Syslog Host: Displays the IP address/hostname of the syslog server, if any, that the device has been configured to use.
2. To continue, select one or more devices from the device selection window and click Edit.
3. The Configure Log Settings window opens. The following controls are available from this window:

Field	Description
Global Level	The Global Level setting determines the global level of logging that will be displayed on the Audit Page. By default, all components will log at the level specified by the Global Level setting. The lower you set the logging level, the less thorough the logging will be.

Field	Description
Component Log Levels	This selection list contains a list of all available components or functions for which logging is available. By default, each component will log at the level specified by the Global Level setting. To specify a component-specific log setting, select the Level drop box/field beside the desired component and then select the desired log level for the component.
Hostname	Type in this field the IP address or hostname of the remote system that is acting as the syslog host system.
Port	Type in this field the TCP port number used by the remote syslog server for syslog communications. Default is 514.

4. To change the device log settings, select from the Level drop-box the new log level.



Configure Log Settings

Configure log level and remote syslog server

Global Log Level

Global level: 6 - Notice

Component Log Levels

Component	Level
Alert Audio Capture	9 - Use Global Level
Alert Graph Capture	9 - Use Global Level
Alert Manager	9 - Use Global Level
Alert Restore	9 - Use Global Level
Audio Capture CGI - ...	9 - Use Global Level
Audio Manager	9 - Use Global Level
Audio Output CGI - Sp...	9 - Use Global Level
Camera Manager	9 - Use Global Level
Capture Manager	9 - Use Global Level
Capture Quota Agent	9 - Use Global Level

Remote Syslog Server

Hostname:

Port: 514

5. To enable logging of events to a remote syslog host type in the Hostname field the IP address or hostname of the remote syslog server. If the remote syslog server is using a port other that 514 for syslog communications, type in the Port field the appropriate port number.

6. When you are finished, click OK to save any changes to the device. Click Cancel to close this window without saving any changes.

Network Interfaces

Use the Network Interfaces task to view or change the network settings for the network interfaces supported by selected devices. By default, NetBotz devices feature a single network interface: the device’s built-in Ethernet interface. If you have installed additional network interfaces (such as adding a wireless adapter) you can use this task to configure them as well.

Note

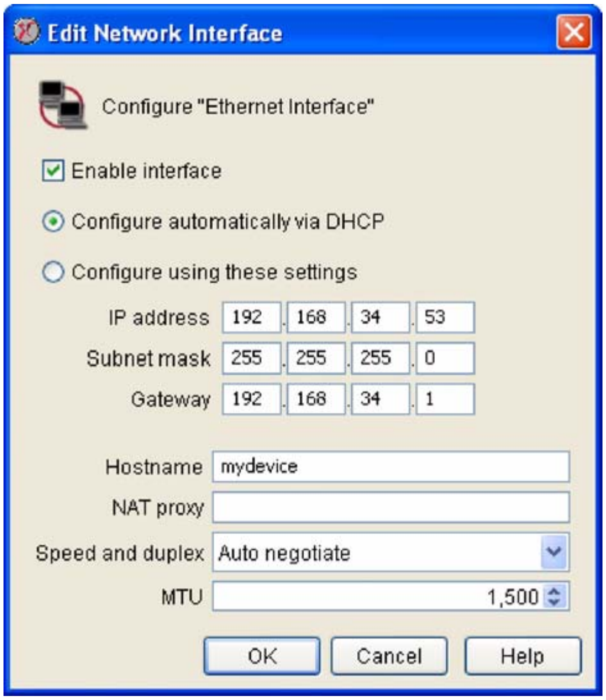
The Network Interfaces task can be run only on one device at a time.

To use the Network Interfaces task:

1. Launch the Network Interfaces task. In addition to the IP address/hostname and status of each selected device, the Network Interfaces task's device selection window also includes two task-specific information columns:
   - DHCP: Indicates whether the interface is configured to obtain network settings using DHCP.
   - Gateway: Displays the IP address/hostname of the network gateway used by the network interface.
2. To continue, select a device from the device selection window and click Edit.
3. The Network Interfaces Configuration window opens. This window contains a table that includes the following information:

Field	Description
Interface	The name of each network interface that is available for use on the selected device.
Hostname	The hostname that is currently being used by each network interface.
IP	The IP address that is assigned to each network interface.
Enabled	Indicates whether each interface is currently enable or not.

4. Select the network interface you want to configure and then click Edit.



Edit Network Interface

Configure "Ethernet Interface"

☑ Enable interface

● Configure automatically via DHCP

○ Configure using these settings

IP address 192 . 168 . 34 . 53

Subnet mask 255 . 255 . 255 . 0

Gateway 192 . 168 . 34 . 1

Hostname mydevice

NAT proxy

Speed and duplex Auto negotiate

MTU 1,500

5. The Edit Network Interfaces window opens, with settings specific to the selected network interface available for editing.

   – If you are editing an Ethernet interface the following controls and fields appear in the Edit Network Interface window:

Field	Description
Enable interface	Check this check box to enable this network interface.
Configure via DHCP radio button	Select this radio button to configure the selected network interface to use a DHCP server on the network to obtain its IP address, subnet mask, and gateway server settings. If you are using DHCP, the time remaining until the device will need to renew its IP address lease is displayed beneath this radio button.
Configure using these settings radio button	Select this radio button if you want to specify the IP address, subnet mask, and gateway address values for the selected network interface.
IP address	The IP address assigned to the selected network interface. This field is available only if you have selected the Configure using these settings radio button.
Subnet mask	The subnet mask for the network that will be used by the selected network interface. This field is available only if you have selected the Configure using these settings radio button.
Gateway	The IP address of the gateway in the network that will be used by the selected network interface. This field is available only if you have selected the Configure using these settings radio button.

Field	Description
Hostname	The host name assigned to the device. If you change the hostname value and are using a DHCP server for IP configuration the device will use the new hostname until the next time it renews its IP address license and will request that the DHCP server use the hostname you entered as the device’s hostname from now on.
NAT proxy name	The name or IP address that is used by a NAT proxy server in your network to enable users to connect to the device from outside the firewall. This address will be included in e-mail alert notifications that are generated by the device instead of the IP address used to identify the device within the firewall. Recipients will then be able to click on the link contained in the e-mail and connect to the device even if they are outside the firewall. Note: A NAT proxy name is needed only if your devices are behind a NAT proxy firewall. If you are not using a NAT proxy, leave this field blank.
Speed and duplex	Use this setting to force the network interface to use specific speed and duplex settings, or to configure the interface to auto negotiate these settings. You can choose Auto Negotiate, 100BaseTx Full Duplex, 100BaseTx Half Duplex, 10BaseT Full Duplex, 10BaseT Half Duplex, or 1000Base Tx Full Duplex (1000Base Tx Full Duplex will be available only if a supported gigabit Ethernet card is installed and properly configured).
MTU	Specifies the maximum transmission unit, the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. Every network has a different MTU, which is set by the network administrator. Ideally, you want the MTU to be the same as the smallest MTU of all the networks between your machine and a message's final destination. Otherwise, if your messages are larger than one of the intervening MTUs, they will get broken up (fragmented), which slows down transmission speeds.

– If you are editing a wireless network interface configuration, the following controls and fields appear in the Edit Network Interface window:

Field	Description
Enable interface	Check this check box to enable this network interface.
Configure via DHCP radio button	Select this radio button to configure the selected network interface to use a DHCP server on the network to obtain its IP address, subnet mask, and gateway server settings. If you are using DHCP, the time remaining until the device will need to renew its IP address lease is displayed beneath this radio button.
Configure using these settings radio button	Select this radio button if you want to specify the IP address, subnet mask, and gateway address values for the selected network interface.
IP address	The IP address assigned to the selected network interface. This field is available only if you have selected the Configure using these settings radio button.
Subnet mask	The subnet mask for the network that will be used by the selected network interface. This field is available only if you have selected the Configure using these settings radio button.
Gateway	The IP address of the gateway in the network that will be used by the selected network interface. This field is available only if you have selected the Configure using these settings radio button.
Hostname	The host name assigned to the device. If you change the hostname value and are using a DHCP server for IP configuration the device will use the new hostname until the next time it renews its IP address license and will request that the DHCP server use the hostname you entered as the device’s hostname from now on.
NAT proxy name	The name or IP address that is used by a NAT proxy server in your network to enable users to connect to the device from outside the firewall. This address will be included in e-mail alert notifications that are generated by the device instead of the IP address used to identify the device within the firewall. Recipients will then be able to click on the link contained in the e-mail and connect to the device even if they are outside the firewall. Note: A NAT proxy name is needed only if your devices are behind a NAT proxy firewall. If you are not using a NAT proxy, leave this field blank.
ESS ID	The extended service set value shared by this device and other members of the wireless network.

Field	Description
Mode	Determines the wireless communication method to use within your wireless network. If your wireless network uses wireless access points (WAPs), select Managed. If your wireless network does not use WAPs, select Ad-Hoc. If you are unsure of whether wireless access points are in use in your network, select Automatic and the adapter will attempt to determine if WAPs are present and self-determine its mode.
Channel	The wireless channel on which the adapter will communicate. Wireless networking clients and WAPs within an ESS must be configured with the same ESS ID and the same channel.
Band	For wireless adapters that support multiple WiFi communication bands, specifies the wireless band that the card will attempt to use for communications. You can select: • Automatic: Searches first for 11a, then 11b, then 11g, and finally for 11a Turbo. The device will use the first band connection/ESSID match it discovers. • 11a: Looks for only 802.11a band connections • 11b: Looks for only 802.11b band connections • 11g: Looks for only 802.11g band connections • 11a Turbo: Looks for only proprietary 802.11a band connection
Encryption	Use this drop box to specify the type of encryption that will be used on the wireless transmissions. You can select WEP, LEAP, or None. • If you select WEP, you must also specify whether an ASCII or Hex WEP Key will be used, as well as the WEP Key value. • If you select LEAP, you must also specify the LEAP Username and Password that will be used. Note: LEAP communications are supported only when used with Cisco 1200 Series AP 12.01T1 wireless access points.
MTU	Specifies the Maximum Transmission Unit, the largest physical packet size, measured in bytes, that a network can transmit. Any messages larger than the MTU are divided into smaller packets before being sent. Every network has a different MTU, which is set by the network administrator. Ideally, you want the MTU to be the same as the smallest MTU of all the networks between your machine and a message's final destination. Otherwise, if your messages are larger than one of the intervening MTUs, they will get broken up (fragmented), which slows down transmission speeds.

6. Make the desired changes tot he network interface settings. When you are finished, click OK to save any changes to the device. Click Cancel to close this window without saving any changes.

Pod Sharing

Use the Pod Sharing task to configure NetBotz 500 devices to host “virtual pods.” Pod Sharing, available for use only with NetBotz 500 devices for which the Premium Software Module has been purchased, enables your NetBotz 500 to connect with and receive data directly from devices integrated with or connected to other NetBotz 320, 420 or 500 devices in your network. Shared pods can be the integrated camera or sensor pod or externally connected pods on a NetBotz 320, 420, or 500. Pod Sharing enables you to use a single NetBotz 500 as a facility “host” to manage alerts from many other NetBotz devices distributed throughout your network. Once a pod has been shared with the NetBotz 500, it functions as though it were connected directly to the device. A single NetBotz 500 can host up to 16 shared pods, total. Up to 4 of the shared pods can be Camera Pod 120s or CCTV Adapter pods. The shared pods can be physically connected to up to 8 target NetBotz devices.

Pod Sharing also enables you to use NetBotz 500 devices to receive data from legacy NetBotz devices running BotzWare 1.x (including RackBotz and WallBotz 300, 303, 310, 400, and 410 devices). Once a NetBotz 500 is configured to access these legacy models they are treated exactly like other shared pods or devices, providing alert and sensor data exactly as if they were directly connected to the NetBotz 500.

Note

- The Pod Sharing task can be run only on one device at a time.
- Only the NetBotz 500 that will host remote pods requires the Premium Software Module. Remote devices to which pods are physically connected and then shared with the NetBotz 500 device do not require the Premium Software Module.
- Pods that are not physically connected to a device do not count against the total number of USB-connected devices allowed for the device model (NetBotz 420s support 1 additional camera pod and up to 4 additional non-camera pods; NetBotz 500s support up to 4 camera pods and up to 17 non-camera pods).
- Framerate from remotely hosted camera pods is limited to 10 frames per second.
- The camera image resolution available from a hosted camera pod is determined by the maximum resolution available to the device to which the pod is physically connected. For example, if you are remotely sharing a Camera Pod 120 that is connected to a NetBotz 500, the maximum resolution available will be 1280x1024. However, if the Camera Pod 120 is shared from a NetBotz 420 the maximum available resolution will 640x480.

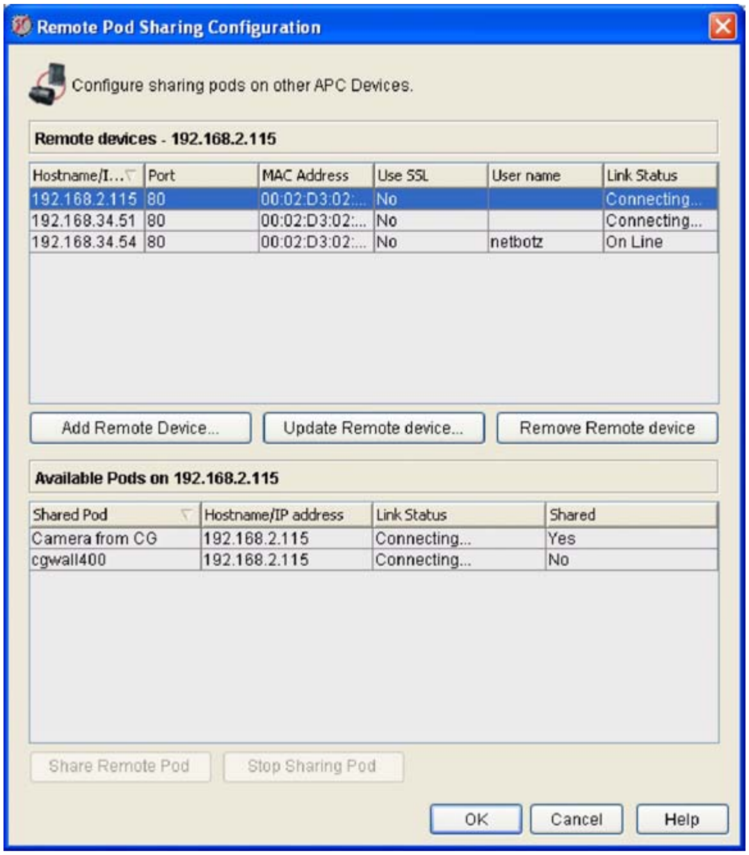
To use the Pod Sharing task:

1. Launch the Pod Sharing task. In addition to the IP address/hostname and status of each selected device, the Pod Sharing task's device selection window also includes one task-specific information column: Shared Pod Count, which displays the number of shared pods that have been defined for each listed device.
2. To continue, select a device from the device selection window and click Edit.
3. The Remote Pod Sharing Configuration window opens. Click on Add Remote Device. The

Configure Remote Device window opens. This window contains the following fields:

Field	Description
Hostname/IP address	The hostname or IP address of the remote device that the pod or other device to be hosted is either integrated with or connected to.
Port	TCP port over which pod sharing communications will occur. Default is 80 for HTTP, and 443 for HTTPS.
SSL options	Select from this drop-box the SSL options that will be used for pod sharing communications.
User name	Type in this field the user name that will be used to access the remote device. Note that some remote pod functionality may be unavailable if a user account that does not have Administrator privileges is used to access the device.
Password/Verify password	Type in these fields the password that will be used to access the remote device.
Timeout (seconds)	Specify the number of seconds that the device will wait for a response from the remote device before it considers the target to be unresponsive.

4. Type in all required values and then click OK to close this window and add the remote device to the Remote Devices list.



Remote Pod Sharing Configuration

Configure sharing pods on other APC Devices.

Remote devices - 192.168.2.115

Hostname/I...	Port	MAC Address	Use SSL	User name	Link Status
192.168.2.115	80	00:02:D3:02:...	No		Connecting...
192.168.34.51	80	00:02:D3:02:...	No		Connecting...
192.168.34.54	80	00:02:D3:02:...	No	netbotz	On Line

Available Pods on 192.168.2.115

Shared Pod	Hostname/IP address	Link Status	Shared
Camera from CG	192.168.2.115	Connecting...	Yes
cgwall400	192.168.2.115	Connecting...	No

5. Next, select from the Remote Devices list the remote device you just added. A list of pods or other

devices that are available for sharing from the remote device appears in the Available Pods selection list.

6. Select a pod or other device from the Available Pods list and then click Share Remote Pod to share the pod with your NetBotz 500.
7. Click OK when you have finished adding shared devices.

PPP/Modem

Use the PPP/Modem task to configure devices to establish a Point-to-Point Protocol (PPP) connection with your TCP/IP network using a supported USB or PC Card modem and a standard analog telephone connection.

Note

- The PPP/Modem task can be run only on one device at a time.
- When configuring devices that will use PPP/Modem connections, you should also configure the camera pod Camera Configuration settings with as low a Picture Count setting as is acceptable for your needs.
- PPP/Modem connection are far slower than LAN connections. Communications with PPP/Modem connected devices will be significantly slower than with those that are connected directly to your LAN, particularly in regard to image collection and display and delivery of alert notifications that include picture data.

To use the PPP/Modem task:

1. Launch the PPP/Modem task. In addition to the IP address/hostname and status of each selected device, the PPP/Modem task's device selection window also includes one task-specific information column: Status, which displays the current status of each device's PPP connection, if any.
2. To continue, select a device from the device selection window and click Edit.
3. The PPP/Modem Configuration window opens. The PPP/Modem Configuration window consists of three panes: Basic, Advanced, and Status. When the Basic tab is selected, the following controls appear in the Basic pane:

Field	Description
Hostname	The hostname that will be associated with the PPP interface.
Phone number	The telephone number that the modem will dial to establish a PPP connection.
User name	The user name that will be provided when establishing a PPP connection.
Password / Verify password	The password that will be provided when establishing a PPP connection.
Country (if supported by modem)	Some modems support country-specific communications parameters to ensure that the modem adheres to communications standards and requirements in use in the country. If your modem supports these strings the Country drop-box will be available. Select from the Country drop box the country in which the device will be dialing out. You can also select None, which will configure the modem to use the default communications parameters.

Field	Description
Schedule: Dial-out enable	Check this check box to create a schedule of times at which your device will establish a PPP connection, regardless of whether alerts have been generated or not. Note: By default no scheduled dial-out events are configured. If you choose to enable scheduled dial-outs, you should then click the Set Schedule button located beside the Enable Dial-Up check box to specify the days and times at which PPP connections will be established.
Schedule: Dial-in enable	Check this check box to enable PPP dial-in support on your device. If dial-in support is enabled, you will be able to use a system and modem to dial into the device and establish a PPP connection. The remote system must provide a Supervisor User ID and Password to establish the PPP connection. Notes: • By default dial-in access is enabled 24 hours a day, 7 days a week, unless you use the dial-in scheduler to enable and disable dial-in access for specified days and times. To configure a dial-in access schedule, click the Set Schedule button located beside the Enable Dial-in check box. • Note that, if the device encounters a situation that requires it to dial-out (due to schedule, alert, or a immediate dial-out request), it will immediately over-ride any current dial-in session without warning.
Alert dial-out settings: Dial-out response to alerts/reports	Select from this drop-box the PPP dial-up action that will be taken by the device when alerts or periodic reports are generated. You can select any of the following: • Disabled — No dial-up action is taken when alerts or reports are generated. • Enabled — Use PPP to connect to the network whenever an alert or report is generated. • Delivery Failure — Use PPP to connect to the network only if network-based alert notification (e-mail, FTP, HTTP posting, etc.) or report delivery fails.
Alert dial-out settings: Remain connected after alerts/reports sent	Use the spin buttons to specify the number of minutes the device will keep the PPP connection active after connecting to the network to deliver alert or report information.

The following controls appear in the Advanced pane:

Field	Description
LCP - Send LCP echo requests to peer	When this check box is checked, your device will send LCP echo requests, allowing PPP to know that the PPP link is active even when there is no network traffic.
Exclusive route - Route all data through PPP when dialed-out	If this check box is checked, all data will be routed via the PPP interface during PPP dial out sessions. When this check box is not checked, the Ethernet interface will be used for communication with hosts that are on the same subnet as the device. However, all communication with hosts not on the same subnet as the device will be carried out using the PPP interface.

Field	Description
Debug - Send debug messages to syslog	When checked, debug messages will be forwarded to the syslog host specified in the Log task.
SIM PIN / Confirm SIM PIN	For modems that use a SIM (subscriber identification module), specify the PIN that is used to unlock the SIM. Note: A SIM may or may not require a PIN in order to function. For modems that do not have a SIM this field must be blank.
Extra initialization commands	If necessary, type additional initialization commands that will be appended to the commands noted in the Initialization commands field here.
Use default modem commands	Check this check box to use the default modem initialization string for your modem.
Initialization commands	If necessary, edit the initialization string used for your modem here.
E-mail addresses for IP address notification	When a PPP connection is established, an e-mail continuing the IP address that has been assigned to the device will be sent to all e-mail addresses listed in this field. To add addresses to this field, click Add, type an address in the E-mail Address field, and then click OK.

The following controls and data appear in the Status pane:

Field	Description
Modem status	Shows the current status reported by the modem to which the device is connected.
Hostname	The hostname being used to identify the PPP interface. Note that this will only show a hostname if you configured one in the Hostname field in the Basic pane.
IP address / Subnet mask	The IP address and subnet mask that has been assigned to the device by the PPP gateway.
Gateway	Shows the IP address of the PPP gateway.
DHCP	Shows whether DHCP is in use for this connection.
Connect speed	Shows the speed of the current PPP connection.
Dial-out due to schedule (yes or no)	If Yes, indicates that the current PPP connection was initiated as a result of a user-specified dial-out schedule.
Dial-out due to alert/report (yes or no)	If Yes, indicates that the current PPP connection was initiates as a result of an alert or report being generated by the device.
Dial-out due to immediate request (yes or no)	If Yes, indicates that the current P connection was initiated as a result of a user-specified immediate dial-out request.
Dial-in due to schedule (yes or no)	If Yes, indicates that the current PPP connection was initiated as a result of a user-specified dial-in schedule.

Field	Description
Request Immediate Dial-up/Cancel Dial-up Request	If the device does not currently have an active PPP connection to a network, you can click Request Immediate Dial-Out to establish a connection. The PPP connection, once initiated, will stay active until you click Cancel Dial-Up Request or the device reboots.

To change the PPP dial-out/dial-in settings, use the controls to specify the desired settings. When you are finished, click OK and any changes you have made will be saved to the device. To end the task without making any changes to your device click Cancel. Click Refresh to update the contents of the task pane with the values that are currently stored on the device.

Using SIM Security

If you will be using the Advanced SIM PIN features, be sure to enter the PIN correctly. If your SIM requires a PIN and you enter the PIN incorrectly the device attempts to use the wrong PIN repeatedly, which could cause the SIM to become “blocked.” If your SIM is blocked, you will require a Pin Unblocking Key (PUK) from your service provider.

Note

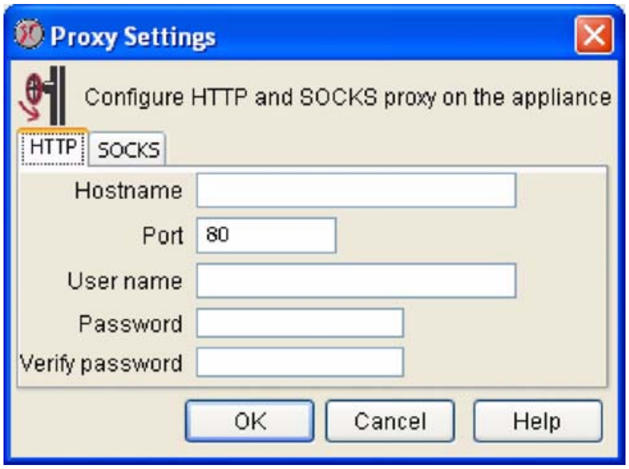
If, after the SIM is disabled, the device continues to attempt to use the SIM while using an incorrect PIN the SIM may become permanently disabled.

Upgrading Devices Over PPP

Depending on connection speed this process can take in excess of one and a half hours (including a device reboot). If the PPP connection fails before the upgrade files are entirely downloaded, then the upgrade will not proceed and upgrade must be re-initiated once the PPP connection is re-established. Make sure you configure the device’s dial-out or dial-in schedule to allow for at least a full hour and a half from the time you starts the upgrade process. If you do not do this, InfraStruXure Central may not be able to reconnect with the device after the device reboots, and will therefore be unable to complete the Upgrade process.

Proxy

Use the Proxy task to provide the necessary settings to enable devices to utilize an HTTP, Socks V4, or V5 Proxy Server. When configured, your devices will use the proxy server for all e-mail and HTTP Post communications, allowing these communications to cross the firewall. These settings do not apply to communications to the device: only communications from the device.


Proxy Settings

Configure HTTP and SOCKS proxy on the appliance

Port: 80

To use the Proxy task:

1. Launch the Proxy task. In addition to the IP address/hostname and status of each selected device, the Clock task's device selection window also includes two task-specific information columns:
   - SOCKS Proxy: Displays the hostname of the SOCKS proxy server that is configured for use with this device, if any.
   - HTTP Proxy: Displays the hostname of the HTTP proxy server that is configured for use with this device, if any.
2. To continue, select one or more devices from the device selection window and click Edit.
3. The Proxy Settings window opens. This window consists of two tabbed panes: the HTTP pane and the SOCKS pane. Each of these panes contains the following fields:

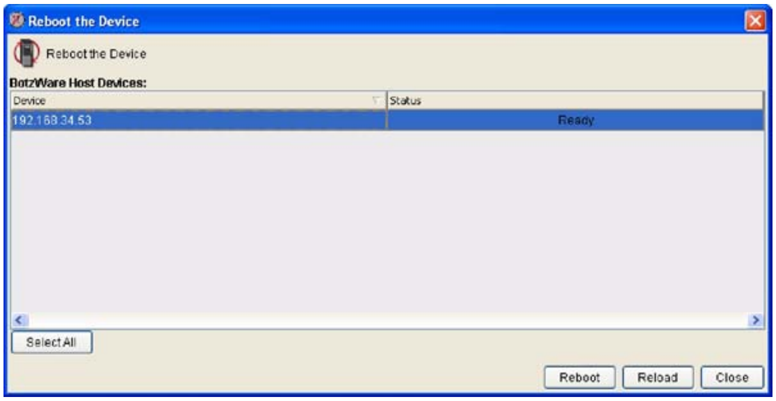
Field	Description
Hostname	The host name or IP address of the proxy server the NetBotz device should use for e-mail, HTTP Posts, and other outbound communications.
Port	The IP port number to connect to on the proxy server.
User name	Some proxy servers can be configured to require a user name and password in order to allow access through the server. Use this field to specify the user name.
Password/Verify password	Some proxy servers can be configured to require a user name and password in order to allow access through the server. Use this field to specify the password.

4. To change the device Proxy settings, type the new values in the appropriate fields. When you are finished, click OK to save any changes to the device. Click Cancel to close this window without saving any changes.

Reboot

Use the Reboot task to reboot all selected devices. To use the Reboot task:

1. Launch the Reboot task.
2. To continue, select one or more devices from the device selection window and click Reboot.



Device	Status
192.168.34.53	Ready

3. Click OK to confirm that you want to reboot all selected devices. To close this task without rebooting your devices, click Close.

Region

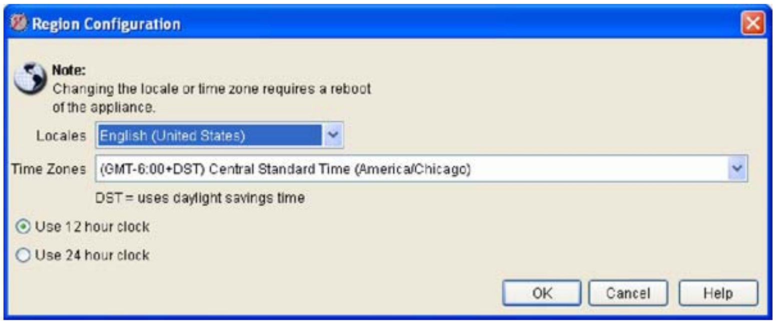
Use the Region task to specify the region in which NetBotz devices are being used and to configure the NetBotz device clock to report time using a 12- or 24-hour clock.

To use the Region task:

1. Launch the Region task. In addition to the IP address/hostname and status of each selected device, the Region task's device selection window also includes two task-specific information columns:
   – 24 Hour Clock: Specifies whether the device is currently configured to use a 24 hour clock display.
   – Current Time Zone: Displays the current time zone setting for the device.
2. To continue, select one or more devices from the device selection window and click Edit.
3. The Region Configuration window opens. This window contains the following fields:

Field	Description
Supported locales	A list of all locales supported by the device.
Time zones	A list of time zones supported by the device.
Use 12 hour clock	Select to configure the device to report time using a 12-hour clock (for example, 2:30PM).
Use 24 hour clock	Select to configure the device to report time using a 24-hour clock (for example, 1430).

To change the Region settings, type the new values in the appropriate fields. When you are finished, click OK to save any changes to the device. Click Cancel to close this window without saving any changes.


Region Configuration

Note:
Changing the locale or time zone requires a reboot of the appliance.

Locales: English (United States)

Time Zones: (GMT-6:00+DST) Central Standard Time (America/Chicago)

DST = uses daylight savings time

● Use 12 hour clock

○ Use 24 hour clock

Note

Changes to the Locale or Time Zone of a device will not take affect until the device is restarted. Use the Reboot task (see “Reboot” on page 213) to restart any devices when you have finished configuring the Region settings if needed.

Restore

Use the Restore task to restore your device configuration using a backup file created previously with the Backup task (see “Monitored Device Settings” on page 160). This task can only be used with devices for which backup files are currently stored on the InfraStruXure Central server.

To use the Restore task:

1. Launch the Restore task. In addition to the IP address/hostname and status of each selected device, the Restore task's device selection window also includes one task-specific information column: Last Backup, which displays information about the last backup that was performed on each device. To continue, select one or more devices from the device selection window and click Restore.
2. Type in the Password field the password that you used to protect the backup file. Note that without this password you will not be able to use the Restore task to restore the device configuration.
3. Click OK to restore your device configuration.

Root Password

Use the Root Password task to change the root password on your devices. NetBotz devices come with a pre-configured root account. The root account is used only for device communications that are performed using the serial port, such as when you use the Serial Configuration Utility to specify network settings. The User ID and Password for this pre-configured account are:

- User name: root
- Password: netbotz

You cannot change the root account user name. However, to ensure security, you can use the Root Password task to change the default root account password. To use the Root Password task:

1. Launch the Reboot task.
2. To continue, select one or more devices from the device selection window and click Edit.
3. Type in the Password field the new root password for all selected devices.
4. Type in the Verify password field the same password as you typed in the Password field.
5. Click OK to save this new root account password to all selected devices. To close this task without saving any changes, click Close.

Serial Devices

Use the Serial Devices task to specify what serial devices are connected to any serial ports that have been added to a device. Serial ports can be added by installing or connecting a serial communications device (such as a modem) to a device, or by connecting a USB-to-Serial-Port adapter to a device or to a USB hub that is connected to a device.

Note

The Serial Devices task can be run only on one device at a time.

To use the Serial Devices task:

1. Launch the Serial Devices task. In addition to the IP address/hostname and status of each selected device, the Serial Devices task's device selection window also includes one task-specific information column: Serial Port Count, which displays the number of serial ports that are available for use on the device.
2. To continue, select a device from the device selection window and click Edit.
3. The Serial Devices Configuration window opens. As serial ports are detected on the device, entries corresponding to each serial port appear automatically in the Serial Devices Configuration window. Use the drop-boxes beside each detected serial port to specify the serial device that is connected to the serial port.
4. If desired, specify a label that will be used to uniquely identify the port to which each device is connected.
5. When you have finished specifying devices using this task, click OK to save your changes. Click Cancel to close this window without saving any changes.

Removing Serial Ports

If a previously detected serial port is not presently detected by the device (for example, if the USB-to-serial port connector has been disconnected from the device), a Remove button will appear beside the port. Click Remove to remove the port configuration.

SMS

Use the SMS task to view or change the SMS (Short Messaging Service) settings on selected devices. These settings must be configured correctly for the Send Wireless SMS Message alert action to function properly.

Note

- The SMS task can be run only on one device at a time.
- This task will be available only if a supported PC Card modem that supports SMS functionality has been installed in the selected device.

To use the SMS task:

1. Launch the SMS task. In addition to the IP address/hostname and status of each selected device, the SMS task's device selection window also includes one task-specific information column: SMS Configuration, which specifies if SMS is available on the device, and whether it is configured or not.
2. To continue, select a device from the device selection window and click Edit.
3. The SMS Configuration window opens. The SMS Configuration window consists of Basic and Advanced panes. The following controls and data appear in the Basic pane:

Field	Description
SIM PIN / Confirm SIM PIN	For modems that use a SIM (subscriber identification module), specify the PIN that is used to unlock the SIM. Note: A SIM may or may not require a PIN in order to function. For modems that do not have a SIM this field must be blank.
Service center (SMSC)	The address of the “Short Message Service Center” used by your SMS service. The SMSC is essentially an SMS “server” that is used to send the messages. The address for the SMSC is typically programmed into the SIM and therefore you can typically leave this field blank. Entering a value in this field will override automatic SMSC selection.
Destination	The destination “address” used to send an SMS to an e-mail destination. The default value for this field is “0000000000,” which is the value that works with AT&T Wireless. When an SMS message needs to be sent to an e-mail destination address, the device puts the e-mail address at the beginning of the message and sends it to the destination address. The SMSC receives the message, pulls out the e-mail address, and sends the remainder of the message to the e-mail address.
Interrupt PPP when an SMS alert occurs check box	If your modem supports both SMS and PPP communications, enabling this setting will allow SMS communications to override PPP communications when necessary. If PPP dial-out is active when the device needs to send an SMS alert, PPP will be interrupted while the SMS message is sent. Once the SMS message has been sent, the PPP connection will be reestablished.

The following controls and data appear in the Advanced pane:

Field	Description
Send debug messages to syslog	When checked, debug messages will be forwarded to the syslog host specified in the Log task (for more information, see “Log” on page 198).
Use default SMS settings	Check this check box to use the default SMS values for your SMS-capable modem. If you need to use custom settings, uncheck this check box and then use the Use protocol descriptor unit check box and the Character set and Initialization commands fields to specify customs settings.
Use protocol descriptor unit (PDU)	Specifies whether the device should use Protocol Descriptor Unit (PDU) mode or “mode” when communicating with the modem to send the SMS message. PDU mode is preferred because it is more versatile than text mode. Some modems do not support both modes.
Character set	Specifies the character set used when communicating with the modem to send the SMS message.
Initialization commands	The initialization string used for the modem that will be used to send SMS messages.

4. Type the new values in the appropriate fields. When you are finished, click OK to save any changes to the device. Click Cancel to close this window without saving any changes.

SNMP

Use the SNMP task to view or change the SNMP settings on selected devices. To use the SNMP task:

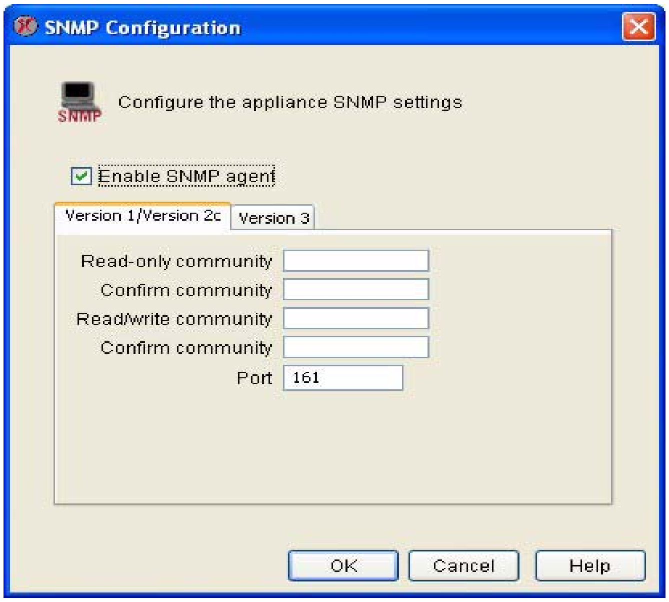
1. Launch the SNMP task. In addition to the IP address/hostname and status of each selected device, the SNMP task's device selection window also includes two task-specific information columns:

   – Agent Enabled: Specifies whether the device's SNMP agent has been enabled or not.

   – Port: Displays the TCP port on which the agent is configured to communicate.

2. To continue, select one or more devices from the device selection window and click Edit.
3. The SNMP Configuration window opens. This window consists of two tabbed panes: The Version 1/Version 2 pane, which includes the basic SNMP configuration controls; and the Version 3 pane,

which includes controls for setting that are specifically for use with SNMP Version 3.



SNMP Configuration

Configure the appliance SNMP settings

☑ Enable SNMP agent

Read-only community

Confirm community

Read/write community

Confirm community

Port 161

- The Version 1/Version 2 pane contains the following fields:

Field	Description
Enable SNMP agent check box	Check this check box to enable the SNMP agent on your device.
Read-only community	Type in this field the read-only community name for SNMP read requests.
Confirm community	When updating or changing the SNMP read-only community name, type the new community name in this field as well.
SNMP read/write community	Type in this field the read/write community name for SNMP read requests.
Confirm community	When updating or changing the SNMP read/write community name, type the new community name in this field as well.
Port	Type in this field the port number to be used for SNMP communications. The default value is 161.

- The Version 3 pane contains the following fields:

Field	Description
Available users/authorized users controls	Use the arrow buttons to authorize or de-authorize specific users.
Authentication protocol	Select the SNMP Version 3 authentication protocol that will be used for SNMP Version 3 communications. You can select MD5 or SHA.
Encryption algorithm	Select the encryption method that will be used for SNMP Version 3 communications. You can choose None, DES, or AES128.

4. Type the new values in the appropriate fields.
5. When you are finished, click OK to save any changes to the device. Click Cancel to close this window without saving any changes.

SSL

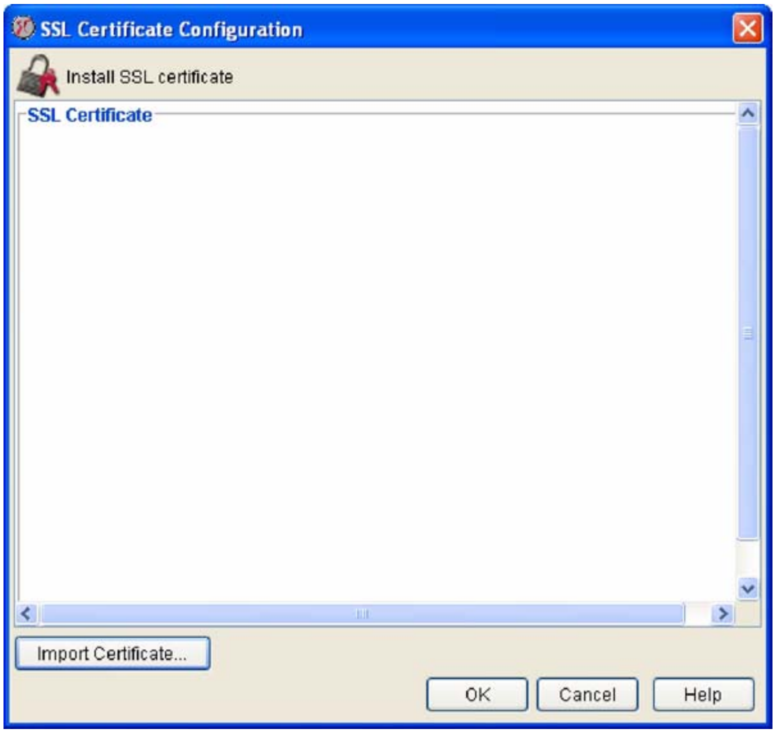
Use the SSL task to install an SSL certificate on selected devices. This will enable SSL-encrypted communication with the device.

Note

The SSL task can be run only on one device at a time.

To use the SSL task:

1. Launch the SSL task. In addition to the IP address/hostname and status of each selected device, the License Key task's device selection window also includes one task-specific information column: Certificate Installed, which specifies if a SSL certificate is currently installed, and if so whether it is a self-signed certificate or a certificate that has been signed by a certification authority.
2. To continue, select a device from the device selection window and click Edit.



3. The SSL Certificate Configuration window opens. Paste your signed certificate data into the Install

SSL Certificate pane and then click OK to install the certificate.

Note

- If you received a Privacy Enhanced Mail (PEM) file from your certification authority, click Import Certificate, select the PEM file, and then click OK to import the contents of the PEM file into the Install SSL Certificate pane. To install the imported file, click OK.
- Depending on your certification authority, you may receive two PEM files instead of one (one containing the public key, and the second containing the private key). If you have received two PEM files, simply use the Import Certificate process to import and install both files.

Upgrade

Use the Upgrade task to check the BotzWare version installed on your devices and to upgrade the BotzWare on any devices that are not up to date. Upgrades are performed using the BotzWare upgrade files stored on the InfraStruXure Central server using the Install/Upgrade Management administrative task. To use the Upgrade task:

1. Launch the Upgrade task. In addition to the IP address/hostname and status of each selected device, the Upgrade task's device selection window also includes two task-specific information columns:
   – Current Version: Specifies the version of BotzWare that is installed on the device.
   – Available Version: Specifies the version of BotzWare that is available to install on the device.
2. To continue, select one or more devices from the device selection window and click Edit.
3. To upgrade one or more devices, select the devices from the list and then click Upgrade. Upgrade files will then be downloaded from the InfraStruXure Central server and applied to the devices. When the upgrade process is complete the device will restart. Once the restart is complete, the status filed beside each device will indicate that the upgrade is complete.

Users

Use the Users task to configure user accounts for personnel that will be permitted access to your device. Each user account has a specific User IDs and Password, as well as an account-specific Privilege Set. Each Privilege Set determines what device features the account can access. The available Privilege Sets are:

Privilege Set	Description
Administrator	Gives user access to all information and configuration tasks available on the device.
Application (with Alert Update)	Gives user access to only the Navigation, Sensor Data and selected portions of the Advanced View Information/Action panes. User accounts configured with the Application Privilege Set can view the Camera, Graphs, Alerts, and About panes. The user can also resolve alert conditions for thresholds that have been configured with the Return-To-Normal Requires User Input setting in their Advanced Settings. However, this Privilege Set does not permit access to the Configuration pane.

Privilege Set	Description
Application	Gives user access to only the Navigation, Sensor Data and selected portions of the Advanced View Information/Action panes. User accounts configured with the Application Privilege Set can view the Camera, Graphs, Alerts, and About panes. However, this Privilege Set does not permit access to the Configuration pane and the user cannot resolve alert conditions for thresholds that have been configured with the Return-To-Normal Requires User Input setting in their Advanced Settings.
Sensor	Gives user access to only the Navigation, Sensor Data and selected portions of the Advanced View Information/Action panes. User accounts configured with the Sensor Privilege Set can view the Camera, Graphs, and About panes. However, this Privilege Set does not permit access to the Alerts or Configuration panes.
Sensor (No Camera)	Gives user access to only the Navigation, Sensor Data and selected portions of the Advanced View Information/Action panes. User accounts configured with the Sensor (No Camera) Privilege Set can view the Graphs and About panes. However, this Privilege Set does not permit access to the Cameras, Alerts, or Configuration panes.
None	Does not permit access to any device features.

By default, your device comes pre-configured with two User accounts:

- Guest: Available to users that do not provide a user name or password at login. By default has access a Privilege Set of None.
- Administrator: Accessed by providing the default user name/password at login. By default has a Privilege Set of Administrator.

Note

- To ensure security, be sure to change the default Administrator account user name and password.
- The Guest and Administrator Accounts are permanent and cannot be removed. However, their settings can be modified as needed.

To use the Users task to create a new user account, or to modify a previously configured user account:

1. Launch the Users task. In addition to the IP address/hostname and status of each selected device, the Users task's device selection window also includes one task-specific information column: User Count, which specifies how many user accounts are configured for use on each device.
2. To continue, select one or more devices from the device selection window and click Edit.
3. The User Configuration window opens. Click Add to create a new user account entry. If editing a

previously created user account, select the account from the Users pane and then click Edit.

4. Type in the Name field a name for this account.
5. Type in the User name field the user name that corresponds to this account.
6. Type in the Password field the password that corresponds to this account.
7. Re-type the password in the Verify password field.
8. Select from the Privilege set drop-box the privilege set that will be assigned to this account.
9. Click OK to save these account settings.

To delete a previously configured account, select the account from the Users pane and then click Remove.

View Device Logs

Use the View Device Logs task to view the contents of the device log of a selected device.

Note

The View Device Logs task can be run only on one device at a time.

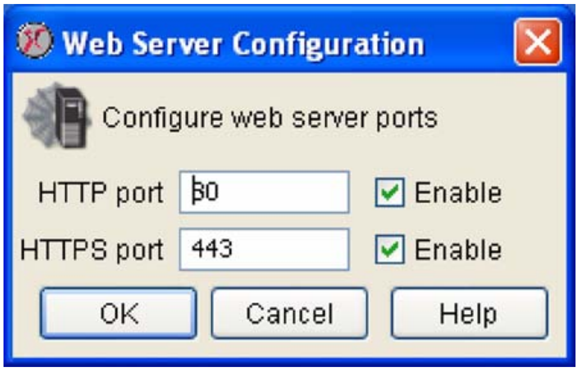
To use the View Device Logs task, launch the View Device Logs task. Then, select a device from the device selection window and click View to view the contents of the selected device's log file.

Web Server

Use the Web Server task to view or change the IP ports through which selected device web servers perform HTTP and HTTPS web server communications.

To use the Web Server task:

1. Launch the Web Server task. In addition to the IP address/hostname and status of each selected device, the SNMP task's device selection window also includes two task-specific information columns:
   – HTTP Port: Displays the TCP port on which HTTP communications are carried out.
   – HTTPS Port: Displays the TCP port on which HTTPS communications are carried out.
2. To continue, select one or more devices from the device selection window and click Edit.



Web Server Configuration

Configure web server ports

HTTP port 80 ☑ Enable

HTTPS port 443 ☑ Enable

3. The Web Server Configuration window opens. This window contains the following fields:

Field	Description
HTTP port	The IP port through which HTTP communications are performed.
HTTPS port	The IP port through which HTTPS communications are performed.
HTTP port/HTTPS port Enable check boxes	Check the check box to enable the corresponding web server port.

Note

IP ports 1 - 65535 are valid, with the exception of ports 20, 21, 22, 23, 25, 123, 161, and 389. These ports are reserved for use by the NetBotz appliance, and using them would create a conflict and would result in operational difficulties.

4. When you are finished, click OK to save any changes to the device. Click Cancel to close this window without saving any changes.

Creating Alert Actions

The information that must be provided for an Alert Action depends on which alert notification method you have selected. The following alert notification methods are available:

- Send to InfraStruXure Central
- Activate Button Output
- Call Web Services Alert Receiver
- Play Audio Alert
- Play Custom Audio Alert
- Send Custom HTTP Get
- Send Custom Text File to FTP Server
- Send Data to FTP Server
- Send E-mail
- Send HTTP Post
- Send Short Message E-mail
- Send SNMP v1 Trap
- Send SNMP v3 Inform
- Send Wireless SMS Message
- Set Switch Output State

Alert notification method-specific instructions for creating Alert Actions follow.

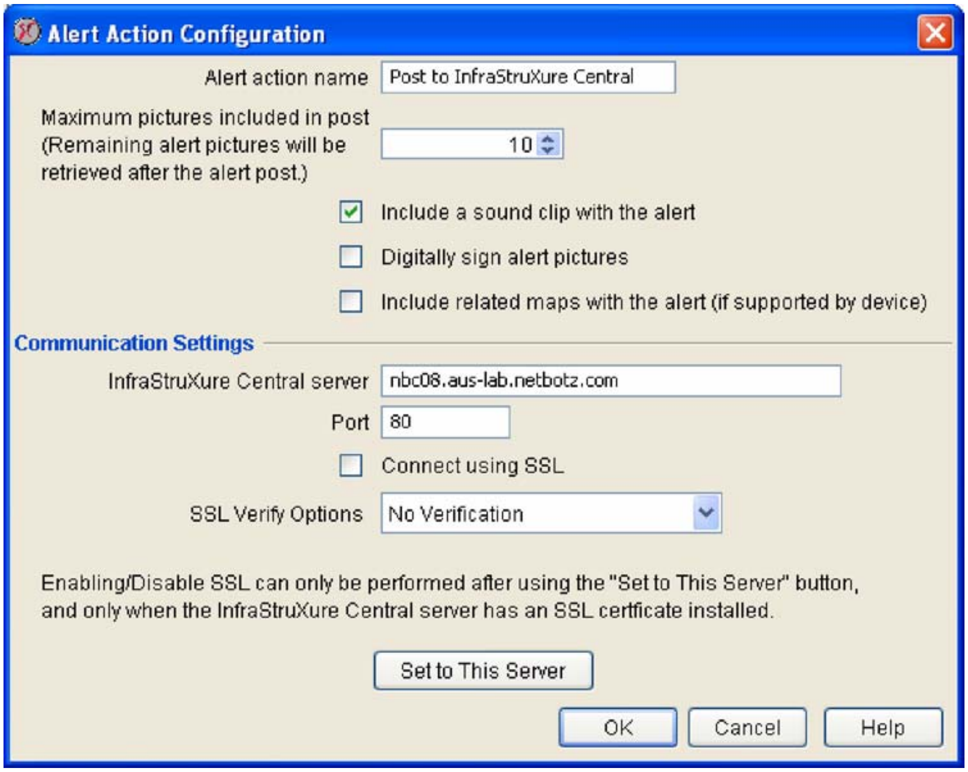
Creating a Send to InfraStruXure Central Alert Action

If you are creating or editing an Alert Action that will use the Send to InfraStruXure Central alert notification method:

1. Launch the Alert Actions task.
2. Select Send to InfraStruXure Central from the Alert Actions drop box. Any selected devices that have previously been configured with an alert action that uses the Send to InfraStruXure

Central alert notification method are displayed in the pane.

- To edit previously created Alert Actions, select the one or more entries from the Send to InfraStruXure Central pane and then click Edit.
- To create a new Send to InfraStruXure Central Alert Action, click Add, select one or more NetBotz devices from the device selection list, and click Next.



Alert Action Configuration

Alert action name: Post to InfraStruXure Central

Maximum pictures included in post (Remaining alert pictures will be retrieved after the alert post.): 10

☑ Include a sound clip with the alert

□ Digitally sign alert pictures

□ Include related maps with the alert (if supported by device)

Communication Settings

InfraStruXure Central server: nbc08.aus-lab.netbotz.com

Port: 80

□ Connect using SSL

SSL Verify Options: No Verification

Enabling/Disable SSL can only be performed after using the "Set to This Server" button, and only when the InfraStruXure Central server has an SSL certficate installed.

3. Type in the Alert Action Name field a name for this Alert Action.
4. The IP address of the InfraStruXure Central server to which the device is currently sending data is displayed in the InfraStruXure Central Server field. If the device is configured to send data to a InfraStruXure Central server other than your own, you can configure the device to send data to the your InfraStruXure Central server by clicking Set to This Server.
5. If the InfraStruXure Central server to which the device is sending data is configured to use SSL, you can configure the device to send data using SSL as well. To configure the device to use SSL when communicating with the InfraStruXure Central server, check the Connect Using SSL check box and then select an SSL Verify Option.
6. Click OK to save this Alert Action.

Creating an Activate Button Output Alert Action

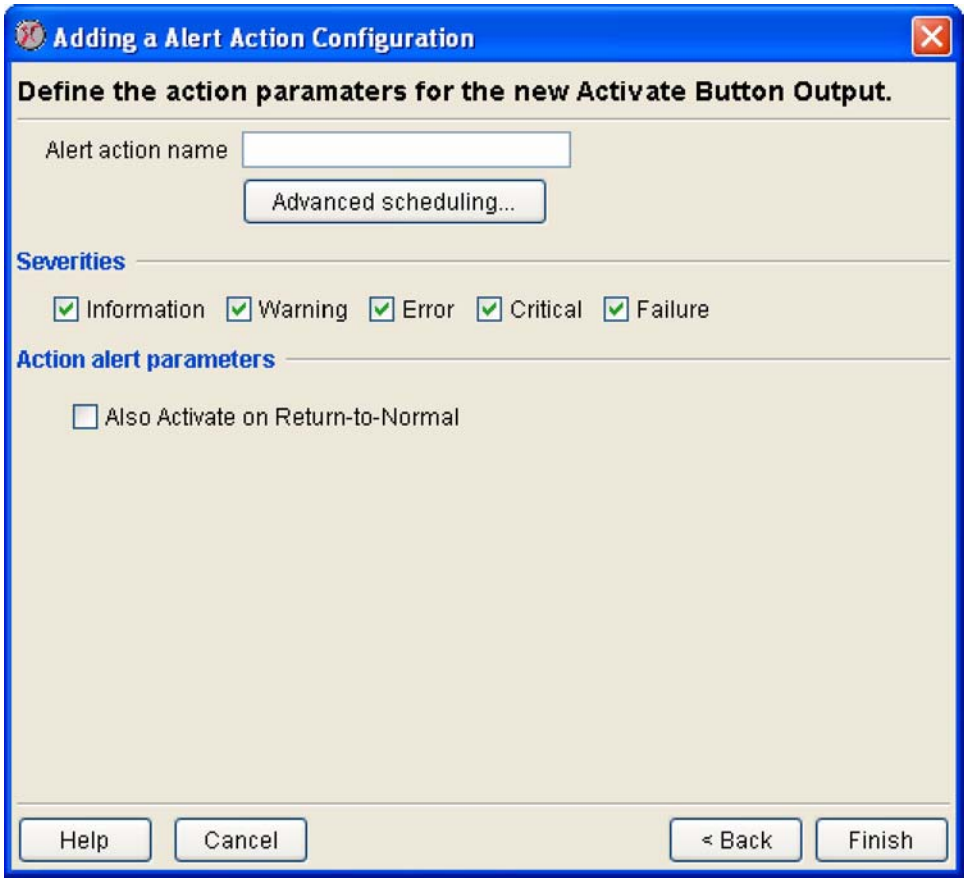
If you are creating an Alert Action that will use the Activate Button Output alert notification method:

1. Launch the Alert Actions task.
2. Select Activate Button Output from the Alert Actions drop box. Any selected devices that have previously been configured with an alert action that uses the Activate Button Output alert

notification method are displayed in the pane.

– To edit previously created Alert Actions, select the one or more entries from the Activate Button Output pane and then click Edit.

– To create a new Activate Button Output Alert Action, click Add, select one or more NetBotz devices from the device selection list, and click Next.



Adding a Alert Action Configuration

Define the action paramaters for the new Activate Button Output.

Alert action name

Severities

☑ Information ☑ Warning ☑ Error ☑ Critical ☑ Failure

Action alert parameters

□ Also Activate on Return-to-Normal

3. Type in the Alert Action Name field a name for this Alert Action.

4. Specify Advanced Scheduling for the Alert Action (optional). By default, all Alert Actions are assumed to be active 24 hours a day, 7 days a week. However, you can specify that an Alert Action will be active only when alert conditions occur during specific time ranges. To configure Advanced Scheduling:
   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.
   b. By default, all time periods in the schedule are set to Enabled. To disable the Alert Action for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Alert Action for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.
   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Alert Action task.

5. Check the check boxes in the Severities check box group that correspond to the alert severities for which buttons will be activated.

6. Select from the Button Output Device drop box the Button Relay device that will be triggered by

this alert action. All Button Relay devices that are defined for use with this device appear in this selection list.

7. If you want this alert action to also be carried out when violated thresholds return to a normal state, check the Also Activate on Return-to-Normal check box.
8. Click OK to save this Alert Action.

Creating a Call Web Services Alert Receiver Alert Action

The Call Web Services Alert Receiver alert action is an advanced functionality alert action that is specifically designed for use with the BotzWare Web Services Interfaces. BotzWare Web Interfaces are intended to provide a set of common, programmer-friendly APIs to 3rd party product and solution developers, as well as end customers. For more information on the BotzWare Web Services Interfaces, please see:

- The *BotzWare V2.x Web Services Specification*, included (in both PDF and DOC formats, enclosed in a single compressed file named WebServicesAPI.zip) in the webservices/doc directory of your *NetBotz Installer* CD-ROM.
- The NetBotz Web Services Toolkit forum, located at:

  http://forums.netbotz.com

Note

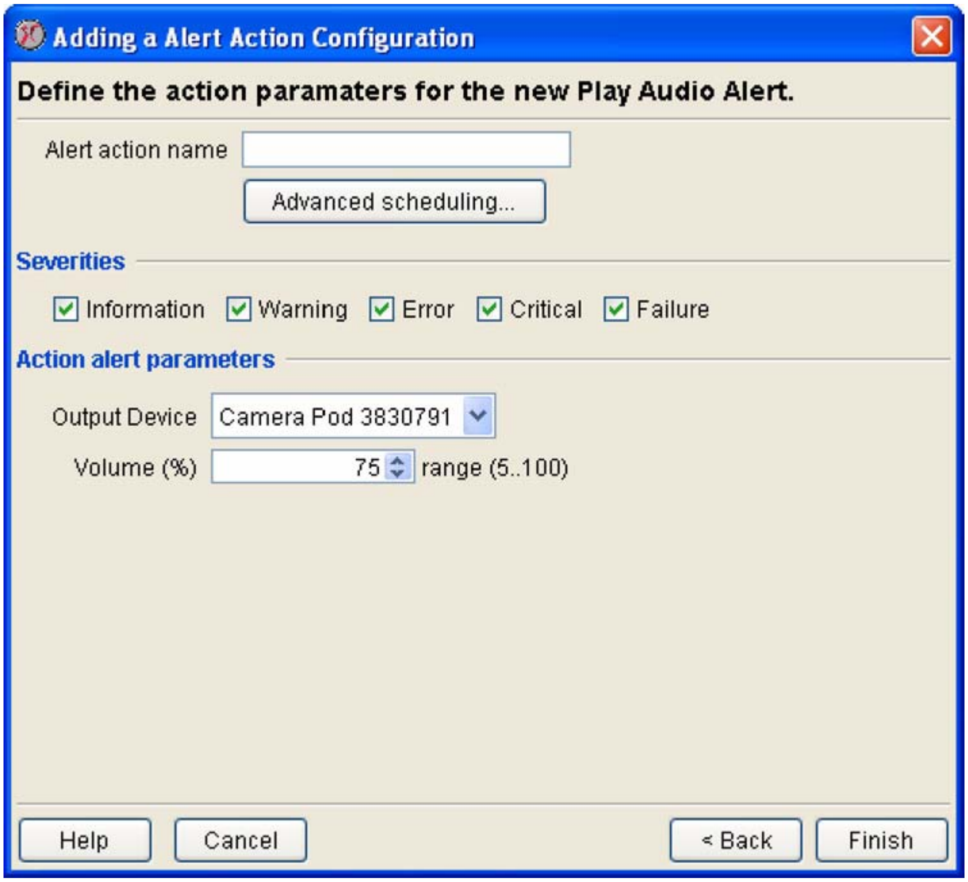
You must be a registered NetBotz forums user to access the Web Services Toolkit forum.

Creating a Play Audio Alert Action

If you are creating an Alert Action that will use the Play Audio alert notification method:

1. Launch the Alert Actions task.
2. Select Play Audio Alert from the Alert Actions drop box. Any selected devices that have previously been configured with an alert action that uses the Play Audio Alert alert notification method are displayed in the pane.
   – To edit previously created Alert Actions, select the one or more entries from the Play Audio alert pane and then click Edit.

– To create a new Play Audio Alert Action, click Add, select one or more NetBotz devices from the device selection list, and click Next.



Define the action paramaters for the new Play Audio Alert.

Alert action name

Severities

☑ Information ☑ Warning ☑ Error ☑ Critical ☑ Failure

Action alert parameters

Output Device: Camera Pod 3830791

Volume (%): 75 range (5..100)

3. Type in the Alert Action Name field a name for this Alert Action.
4. Specify Advanced Scheduling for the Alert Action (optional). By default, all Alert Actions are assumed to be active 24 hours a day, 7 days a week. However, you can specify that an Alert Action will be active only when alert conditions occur during specific time ranges. To configure Advanced Scheduling:
   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.
   b. By default, all time periods in the schedule are set to Enabled. To disable the Alert Action for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Alert Action for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.
   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Alert Action task.
5. Check the check boxes in the Severities check box group that correspond to the alert severities for which audio alerts will be played.
6. Select Output Devices that will play the audio alerts through their headphone/speaker output jacks. Any Camera Pod 120s that are connected to your device will be available for selection.
7. Select an Output Volume for the audio alert. By default, audio alerts are played at 75% of the output

device’s maximum volume.

8. Click OK to save this Alert Action.

Creating a Play Custom Audio Alert Action

If you are creating an Alert Action that will use the Play Custom Audio alert notification method:

1. Launch the Alert Actions task.
2. Select Play Custom Audio from the Alert Actions drop box. Any selected devices that have previously been configured with an alert action that uses the Play Custom Audio alert notification method are displayed in the pane.
   - To edit previously created alert actions, select the one or more entries from the Play Audio pane and then click Edit.
   - To create a new Play Audio alert action, click Add, select one or more devices from the device selection list, and click Next.
3. Type in the Alert Action Name field a name for this Alert Action.
4. Specify Advanced Scheduling for the Alert Action (optional). By default, all Alert Actions are assumed to be active 24 hours a day, 7 days a week. However, you can specify that an Alert Action will be active only when alert conditions occur during specific time ranges. To configure Advanced Scheduling:
   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.
   b. By default, all time periods in the schedule are set to Enabled. To disable the Alert Action for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Alert Action for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.
   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Alert Action task.
5. Check the check boxes in the Severities check box group that correspond to the alert severities for which audio alerts will be played.
6. Select Output Devices that will play the audio alerts through their headphone/speaker output jacks. Any Camera Pod 120s that are connected to your device will be available for selection.
7. Select an Output Volume for the audio alert. By default, audio alerts are played at 75% of the output device’s maximum volume.
8. Click OK to save this Alert Action.

Note

Before an audio clip is available for use in the Play Custom Audio alert action it must first be uploaded to the NetBotz appliance. Audio clips are uploaded to the appliance using the Custom Audio Clips task. For more information see “Custom Audio Clips” on page 168.

Creating a Send Custom HTTP Get Alert Action

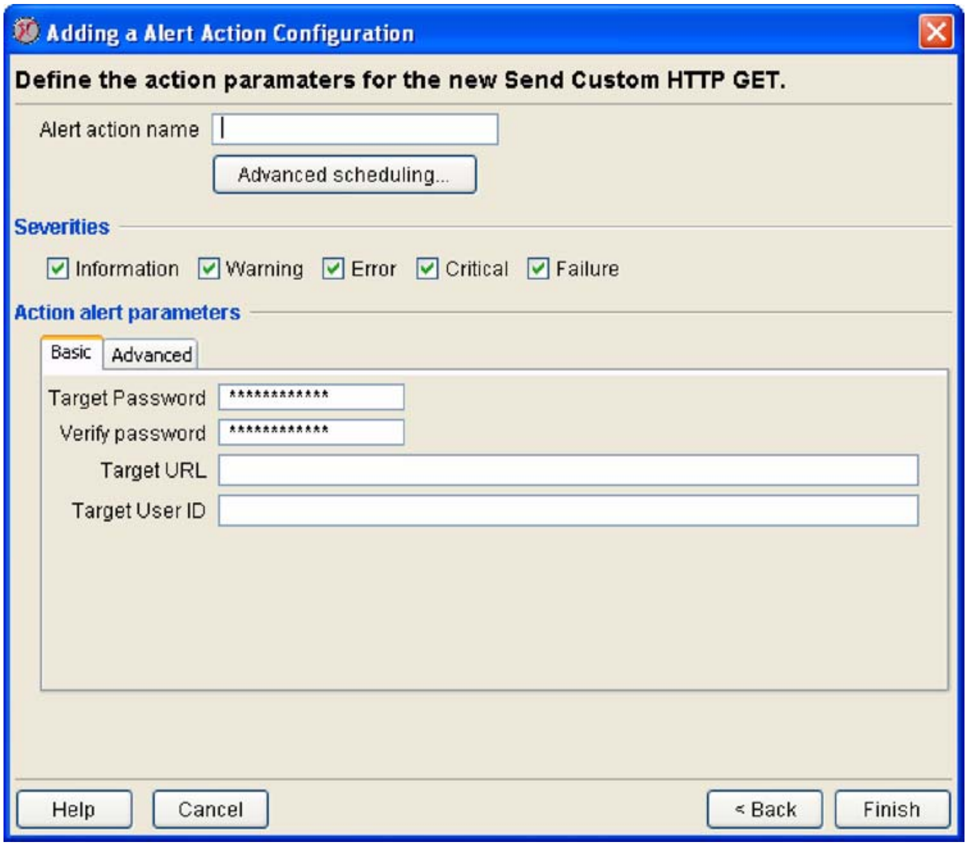
If you are creating an Alert Action that will use the Send Custom HTTP Get alert notification method:

1. Launch the Alert Actions task.
2. Select Send Custom HTTP Get from the Alert Actions drop box. Any selected devices that have

previously been configured with an alert action that uses the Send Custom HTTP Get alert notification method are displayed in the pane.

– To edit previously created Alert Actions, select the one or more entries from the Send Custom HTTP Get alert pane and then click Edit.

– To create a new Send Custom HTTP Get Alert Action, click Add, select one or more NetBotz devices from the device selection list, and click Next.



Adding a Alert Action Configuration

Define the action paramaters for the new Send Custom HTTP GET.

Alert action name

Severities

☑ Information ☑ Warning ☑ Error ☑ Critical ☑ Failure

Action alert parameters

Target Password ************

Verify password ************

Target URL

Target User ID

3. Type in the Alert Action Name field a name for this Alert Action.

4. Specify Advanced Scheduling for the Alert Action (optional). By default, all Alert Actions are assumed to be active 24 hours a day, 7 days a week. However, you can specify that an Alert Action will be active only when alert conditions occur during specific time ranges. To configure Advanced Scheduling:

   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.

   b. By default, all time periods in the schedule are set to Enabled. To disable the Alert Action for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Alert Action for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Alert Action task.

5. Check the check boxes in the Severities check box group that correspond to the alert severities for which audio alerts will be played.

6. The bottom of the pane features a Basic and an Advanced tabbed pane. On the Basic pane, type the

appropriate information in the following fields:

- Type in the Target URL field the custom HTTP GET statement that will be generated by the device.
- Type in the Target User ID and Password fields the User ID and Password needed to execute the custom HTTP GET command at the Target URL.
- Type the Password again in the Confirm Password field.

Note

The Target URL field accepts BotzWare macros.

8. If desired, click the Advanced tab and select optional SSL Verify Options for the custom HTTP GET commands (used for both the primary and backup hosts), or to provide information for use in delivering the custom HTTP GET command to an alternate web host. This backup URL would be used only if attempts to deliver the alert data to the primary Target Host failed. You can also check the following check boxes:
   - Use POST instead of GET: Uses the POST command instead of the GET command.
   - Include XML-encoded Alert Parameter (xmlalert): Appends the parameter “xmlalert=<*xml alert encoding*>” to the provided URL for the action. The encoded XML is the same as is generated by the HTTP POST code, but is URL-encoded to enable those that can't easily handle multi-part/form-data encoded POSTS to get the XML for the alert.
9. Click OK to save this Alert Action.

Example Target URLs

When creating a Send Custom HTTP GET alert action, a data handling application of some sort (CGI script, ASP script, servlet, etc.) must be invoked on the web host invoked in the Target URL, and appropriate data must be passed to the application in a format that is appropriate. Therefore, the content of the Target URL field is entirely dependent on the configuration of the target server which will process the HTTP GET. The following examples demonstrate two possible ways in which this alert action could be configured, and are intended to help you to construct an appropriate Target URL value.

Example #1:

In this first example, the custom HTTP GET command provides user-specified values for a CGI script (pagersend.cgi). This custom HTTP GET would send the *message* “hello there,” with a *subject* of “test message,” *from* “mike” to the specified *pin* (telephone number):

http://www.mymmode.com/messagecenter/pagersend.cgi?pin=512
5551212&from=mike&subject=test+message&message=hello+there

Example #2:

In this example, alert data is sent to a pager using the same CGI script (pagersend.cgi) as we used in Example #1, but this time we use BotzWare macros to dynamically generate the message content:

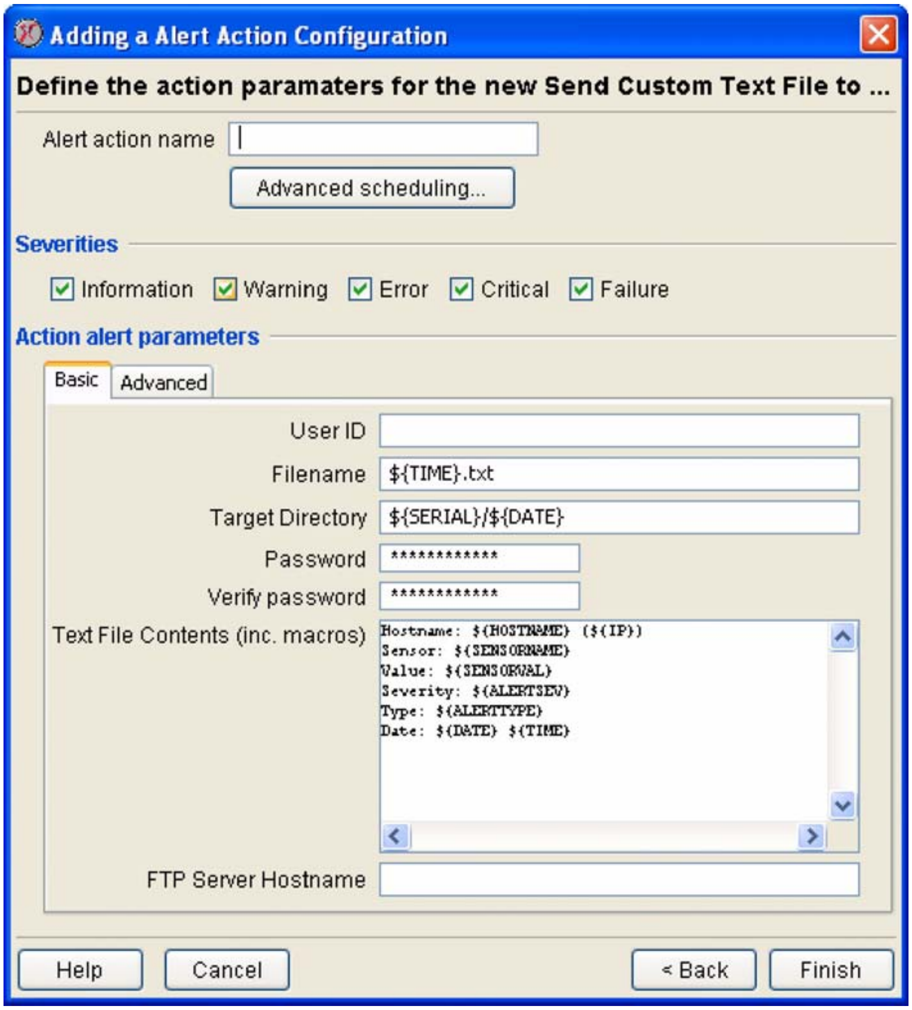
http://www.mymmode.com/messagecenter/pagersend.cgi?pin=512
5551212&from=${HOSTNAME}&subject=test+message&message=${SENSORNAME}+${S
ENSORVAL}+at+${ALERTPOD}

A message generated by this Target URL could read “Humidity 94% at Sensor Pod 0930261” from “mybotz.netbotz.com.”

Creating a Send Custom Text File to FTP Server Alert Action

If you are creating an Alert Action that will use the Send Custom Text File to FTP Server alert notification method:

1. Launch the Alert Actions task.
2. Select Send Custom Text File to FTP Server from the Alert Actions drop box. Any selected devices that have previously been configured with an alert action that uses the Send Custom Text File to FTP Server alert notification method are displayed in the pane.
   - To edit previously created Alert Actions, select the one or more entries from the Send Custom Text File to FTP Server alert pane and then click Edit.
   - To create a new Send Custom Text File to FTP Server Alert Action, click Add, select one or more NetBotz devices from the device selection list, and click Next.



Adding a Alert Action Configuration

Define the action paramaters for the new Send Custom Text File to ...

Alert action name:

Severities: ☑ Information ☑ Warning ☑ Error ☑ Critical ☑ Failure

Action alert parameters

User ID:

Filename: ${TIME}.txt

Target Directory: ${SERIAL}/${DATE}

Password: ************

Verify password: ************

Text File Contents (inc. macros):

```
Hostname: ${HOSTNAME} (${IP})
Sensor: ${SENSORNAME}
Value: ${SENSORVAL}
Severity: ${ALERTSEV}
Type: ${ALERTTYPE}
Date: ${DATE} ${TIME}
```

FTP Server Hostname:

3. Type in the Alert Action Name field a name for this alert action.
4. Specify Advanced Scheduling for the Alert Action (optional). By default, all Alert Actions are assumed to be active 24 hours a day, 7 days a week. However, you can specify that an Alert Action will be active only when alert conditions occur during specific time ranges. To configure Advanced Scheduling:

   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.

b. By default, all time periods in the schedule are set to Enabled. To disable the Alert Action for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Alert Action for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Alert Action task.

5. Check the check boxes in the Severities check box group that correspond to the alert severities for which alert notifications will be sent.
6. The bottom of the pane features a Basic and an Advanced tabbed pane. On the Basic pane, type the appropriate information in the following fields:

– Type in the Text File Contents (inc. macros) field the data that you want to include in the custom text file that will be sent to the specified FTP server.

– Type in the FTP Server Hostname field the TCP/IP hostname or IP address of the FTP server to which the text file will be delivered.

– Type in the User ID and Password fields the User ID and Password needed to deliver the text file to the FTP server at the specified FTP Server Hostname.

– Type the Password again in the Confirm Password field.

– Type in the Target Directory field the relative directory path to be used for storing the text file on the FTP server. This should always be a path relative to the default directory associated with the user ID used to log on to the FTP server. If the directories on the path do not exist they will be created automatically.

– Type in the Base Filename field the base filename to be used for storing the text file on the FTP server.

Note

The Text File Contents (inc. macros), Target Directory, and Base Filename fields accept BotzWare macros.

8. If desired, click the Advanced tab and provide information for use in delivering the data to a backup FTP server. This backup server would be used only if attempts to deliver the alert data to the primary FTP server failed.
9. Click OK to save this Alert Action.

Creating a Send Data to FTP Server Alert Action

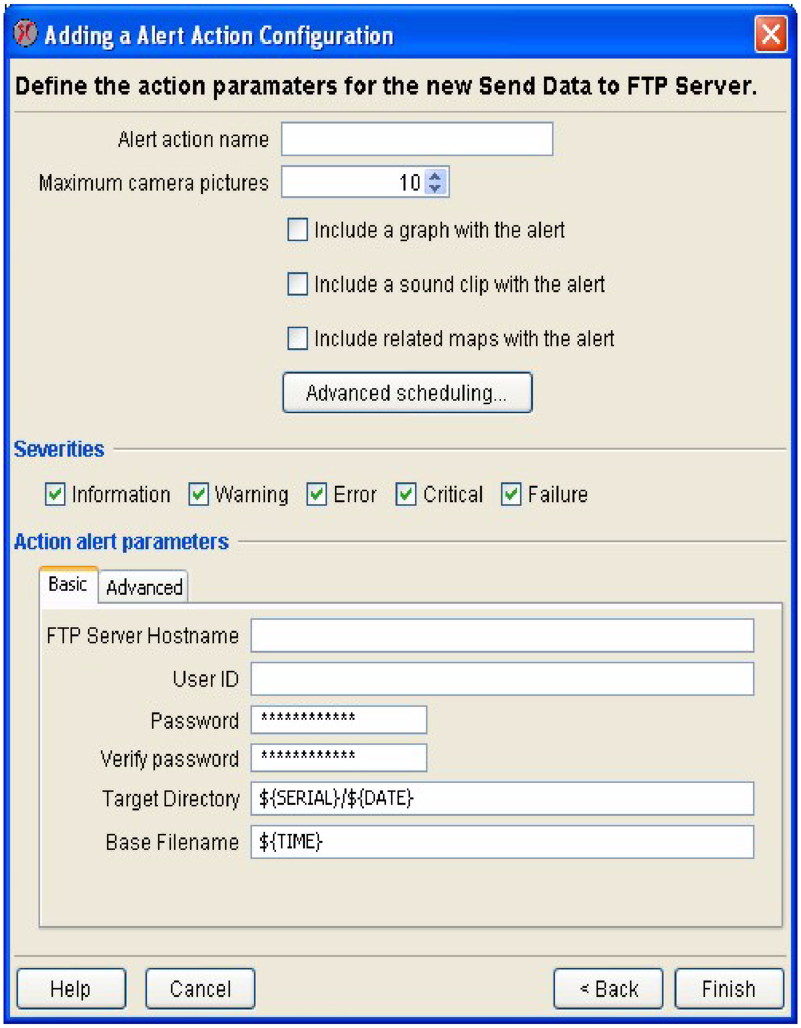
If you are creating an Alert Action that will use the Send Data to FTP Server alert notification method:

1. Launch the Alert Actions task.
2. Select Send Data to FTP Server from the Alert Actions drop box. Any selected devices that have previously been configured with an alert action that uses the Send Data to FTP Server alert

notification method are displayed in the pane.

– To edit previously created Alert Actions, select the one or more entries from the Send Data to FTP Server alert pane and then click Edit.

– To create a new Send Data to FTP Server Alert Action, click Add, select one or more NetBotz devices from the device selection list, and click Next.



Adding a Alert Action Configuration

Define the action paramaters for the new Send Data to FTP Server.

Alert action name

Maximum camera pictures 10

□ Include a graph with the alert

□ Include a sound clip with the alert

□ Include related maps with the alert

Severities

☑ Information ☑ Warning ☑ Error ☑ Critical ☑ Failure

Action alert parameters

FTP Server Hostname

User ID

Password ************

Verify password ************

Target Directory ${SERIAL}/${DATE}

Base Filename ${TIME}

3. Type in the Alert Action Name field a name for this alert action.

4. Type in the Maximum Camera Pictures field (or use the arrow buttons in the field to select) the maximum number of available images that will be included with the generated data. Note that, depending on the Total Number of Pictures setting (located in the camera configuration task), additional images may be captured by the device. The Maximum Camera Pictures setting specifies only how many of the pictures captured by the device will be included in data.

5. If you want a graph of the sensor values associated with the alert to be included in the data, check the Include a Graph with the Alert check box.

6. If you want audio captured by the Camera Pod to be included in the data check the Include a Sound Clip with the Alert check box.

7. Specify Advanced Scheduling for the Alert Action (optional). By default, all Alert Actions are assumed to be active 24 hours a day, 7 days a week. However, you can specify that an Alert Action

will be active only when alert conditions occur during specific time ranges. To configure Advanced Scheduling:

a. Click Advanced Scheduling.... The Advanced Scheduling window opens.

b. By default, all time periods in the schedule are set to Enabled. To disable the Alert Action for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Alert Action for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Alert Action task.

8. Check the check boxes in the Severities check box group that correspond to the alert severities for which alert notifications will be sent.

9. The bottom of the pane features a Basic and an Advanced tabbed pane. On the Basic pane, type the appropriate information in the following fields:

   – Type in the FTP Server Hostname field the TCP/IP hostname or IP address of the FTP server to which the data will be delivered.

   – Type in the User ID and Password fields the User ID and Password needed to deliver post data to the FTP server at the specified FTP Server Hostname.

   – Type the Password again in the Confirm Password field.

   – Type in the Target Directory field the relative directory path to be used for storing the data on the FTP server. This should always be a path relative to the default directory associated with the user ID used to log on to the FTP server. If the directories on the path do not exist they will be created automatically.

   – Type in the Base Filename field the base filename to be used for storing the data on the FTP server. The alert data will be stored in a file with this name, followed by the ".nbalert" file extension. Pictures from alerts will be stored in files with this name, followed by the ".*n*.jpg" file extension, where *n* is the picture number (1, 2, 3, etc.).

Note

The Target Directory and Base Filename fields accept BotzWare macros.

11. If desired, click the Advanced tab and provide information for use in delivering the data to a backup FTP server. This backup server would be used only if attempts to deliver the alert data to the primary FTP server failed.

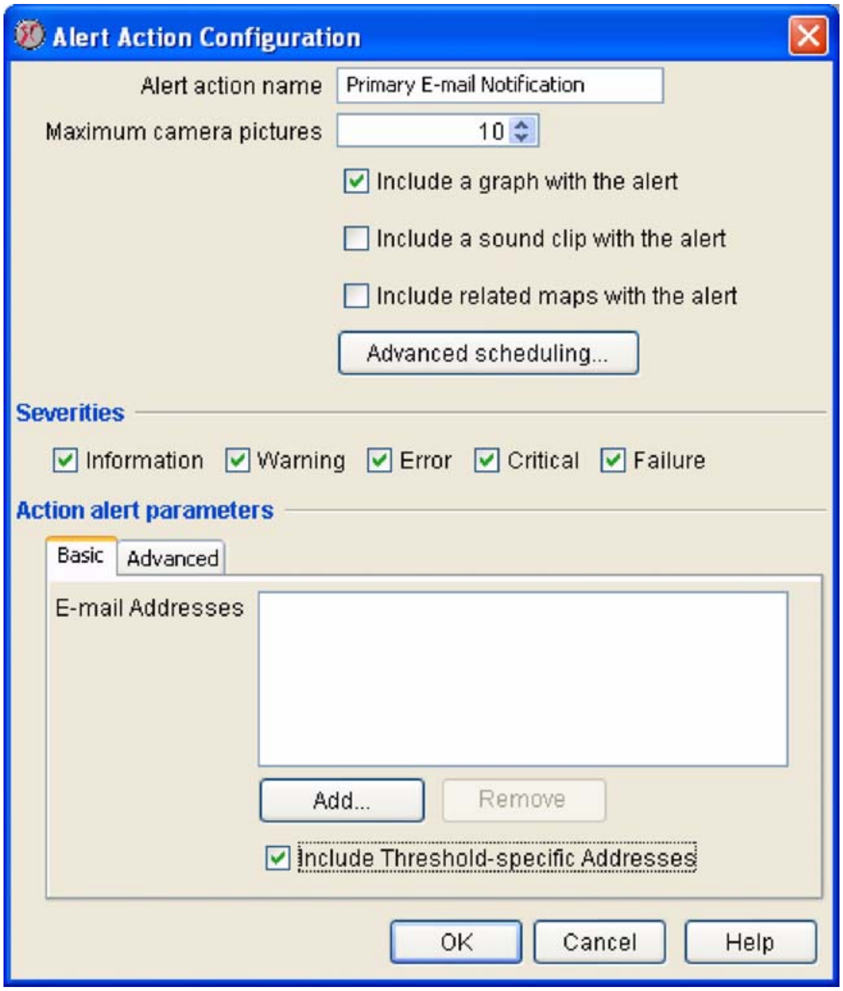
12. If you have installed the BotzWare Premium Software Module 2.3 installed, you can choose to send images captured by the device cameras as JPEGs, M-JPEG AVI Files, or Signed M-JPEG AVI files. M-JPEG AVI files are motion picture that can be played using standard media player software (such as Windows Media Player). Signed files provide proof that the generated images have not been tampered with or altered in any way, and are therefore more likely to be admissible as evidence in legal proceedings. To specify the format in which captured images will be sent, select the Advanced tab and then select the desired format from the Picture Export Format drop box.

13. Click OK to save this Alert Action.

Creating a Send E-mail Alert Action

If you are creating an Alert Action that will use the Send E-Mail alert notification method:

1. Launch the Alert Actions task.
2. Select Send E-Mail from the Alert Actions drop box. Any selected devices that have previously been configured with an alert action that uses the Send E-Mail alert notification method are displayed in the pane.
   - To edit previously created Alert Actions, select the one or more entries from the Send E-Mail alert pane and then click Edit.
   - To create a new Send E-Mail Alert Action, click Add, select one or more NetBotz devices from the device selection list, and click Next.



Alert Action Configuration

Alert action name: Primary E-mail Notification

Maximum camera pictures: 10

☑ Include a graph with the alert

☐ Include a sound clip with the alert

☐ Include related maps with the alert

Severities

☑ Information ☑ Warning ☑ Error ☑ Critical ☑ Failure

Action alert parameters

E-mail Addresses

☑ Include Threshold-specific Addresses

3. Type in the Alert Action Name field a name for this alert action.
4. Type in the Maximum Camera Pictures field (or use the arrow buttons in the field to select) the maximum number of available images that will be included with the generated e-mail. Note that, depending on the Total Number of Pictures setting (located in the Camera Pod 120s configuration task), additional images may be captured by the device. The Maximum Camera Pictures setting specifies only how many of the pictures captured by the device will be included in e-mailed alert notifications.
5. If you want a graph of the sensor values associated with the alert to be included in the e-mail, check

the Include a Graph with the Alert check box.

6. If you want audio captured by the Camera Pod to be included in the data check the Include a Sound Clip with the Alert check box.
7. Specify Advanced Scheduling for the Alert Action (optional). By default, all Alert Actions are assumed to be active 24 hours a day, 7 days a week. However, you can specify that an Alert Action will be active only when alert conditions occur during specific time ranges. To configure Advanced Scheduling:
   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.
   b. By default, all time periods in the schedule are set to Enabled. To disable the Alert Action for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Alert Action for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.
   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Alert Action task.
8. Check the check boxes in the Severities check box group that correspond to the alert severities for which e-mail notifications will be sent.
9. Add to the E-mail Addresses field the addresses of the recipients to whom the e-mail notification will be sent. Click Add..., type in the e-mail address to which the alert notification will be sent, and then click OK.
10. If desired, check the Include Addresses from Thresholds check box to include threshold-specific e-mail recipients.

Note

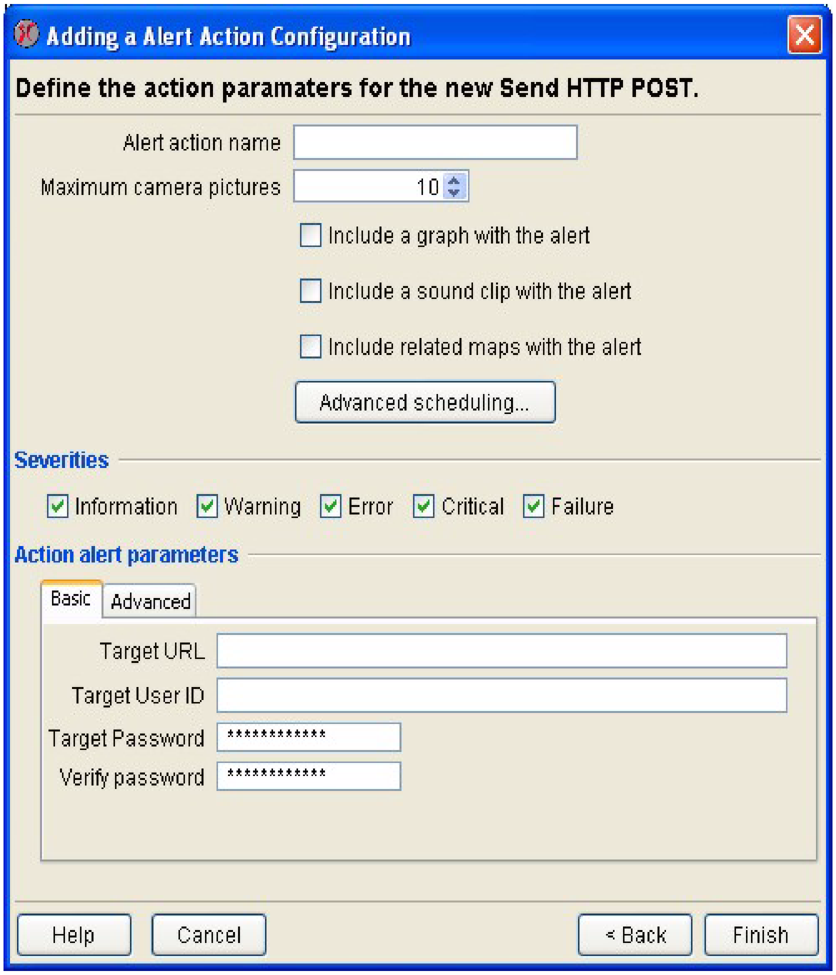
- If the E-mail Addresses field is left blank and you uncheck the Include Addresses from Thresholds check box then no e-mail notifications will be sent
- If the E-mail Addresses field is left blank and you check the Include Addresses from Thresholds check box then e-mail notifications will be sent only if the threshold that is exceeded has a Threshold-Specific Address List.

12. If you do not want e-mail notifications to be sent when sensor readings that previously triggered an alert return to a “normal” state, select the Advanced tab and then check the Do Not Send Return-To-Normal Messages check box.
13. Some e-mail services attempt to control spam e-mail by automatically deleting e-mail messages that contain header information that is not absolutely necessary for message delivery, such a header data that indicates that the message is “High Priority.” To include only the header information that is necessary to ensure delivery of the e-mail message, select the Advanced tab and then check the Minimize Header Usage check box.
14. If you have installed the BotzWare Premium Software Module 2.3 installed, you can choose to send images captured by the device cameras as JPEGs, M-JPEG AVI Files, or Signed M-JPEG AVI files. M-JPEG AVI files are motion picture files that can be played using standard media player software (such as Windows Media Player). Signed files provide proof that the generated images have not been tampered with or altered in any way, and are therefore more likely to be admissible as evidence in legal proceedings. To specify the format in which captured images will be sent, select the Advanced tab and then select the desired format from the Picture Export Format drop box.
15. Click OK to save this Alert Action.

Creating a Send HTTP Post Alert Action

If you are creating an Alert Action that will use the Send HTTP Post alert notification method:

1. Launch the Alert Actions task.
2. Select Send HTTP Post from the Alert Actions drop box. Any selected devices that have previously been configured with an alert action that uses the Send HTTP Post alert notification method are displayed in the pane.
   - To edit previously created Alert Actions, select the one or more entries from the Send HTTP Post alert pane and then click Edit.
   - To create a new Send HTTP Post Alert Action, click Add, select one or more NetBotz devices from the device selection list, and click Next.



Adding a Alert Action Configuration

Define the action paramaters for the new Send HTTP POST.

Alert action name

Maximum camera pictures 10

□ Include a graph with the alert

□ Include a sound clip with the alert

□ Include related maps with the alert

Severities

☑ Information ☑ Warning ☑ Error ☑ Critical ☑ Failure

Action alert parameters

Target URL

Target User ID

Target Password ************

Verify password ************

3. Type in the Alert Action Name field a name for this alert action.
4. Type in the Maximum Camera Pictures field (or use the arrow buttons in the field to select) the maximum number of available images that will be included with the generated HTTP post. Note that, depending on the Total Number of Pictures setting (located in the camera configuration task), additional images may be captured by the device. The Maximum Camera Pictures setting specifies only how many of the pictures captured by the device will be included in HTTP post.
5. If you want a graph of the sensor values associated with the alert to be included in the HTTP post,

check the Include a Graph with the Alert check box.

6. If you want audio captured by the Camera Pod to be included in the data check the Include a Sound Clip with the Alert check box.
7. Specify Advanced Scheduling for the Alert Action (optional). By default, all Alert Actions are assumed to be active 24 hours a day, 7 days a week. However, you can specify that an Alert Action will be active only when alert conditions occur during specific time ranges. To configure Advanced Scheduling:
   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.
   b. By default, all time periods in the schedule are set to Enabled. To disable the Alert Action for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Alert Action for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.
   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Alert Action task.
8. Check the check boxes in the Severities check box group that correspond to the alert severities for which HTTP post notifications will be sent.
9. The bottom of the pane features a Basic and an Advanced tabbed pane. On the Basic pane, type the appropriate information in the following fields:

   – Type in the Target URL field the URL (including host, port, and any of the common parameters supported by the device) of the system to which HTTP post data will be posted.

   – Type in the Target User ID and Target Password fields the User ID and Password needed to post data to the server at the specified Target URL.

   – Type the Target Password again in the Confirm Password field.

   If desired, click the Advanced tab and fill type the appropriate information in the following fields:

   – Type in the Backup Target URL field the URL (including host, port, and any of the common parameters supported by the device) of a system to which HTTP post data will be posted if posting to the primary Target URL fails.

   – Type in the Backup User ID and Backup Target Password fields the User ID and Password needed to post data to the backup server at the specified Backup Target URL.

   – Type the Backup Target Password again in the Confirm Password field.

   – Type in the SSL Verify Options field any desired SSL verification options.
10. Click OK to save this Alert Action.

Creating a Send Short Message E-mail Alert Action

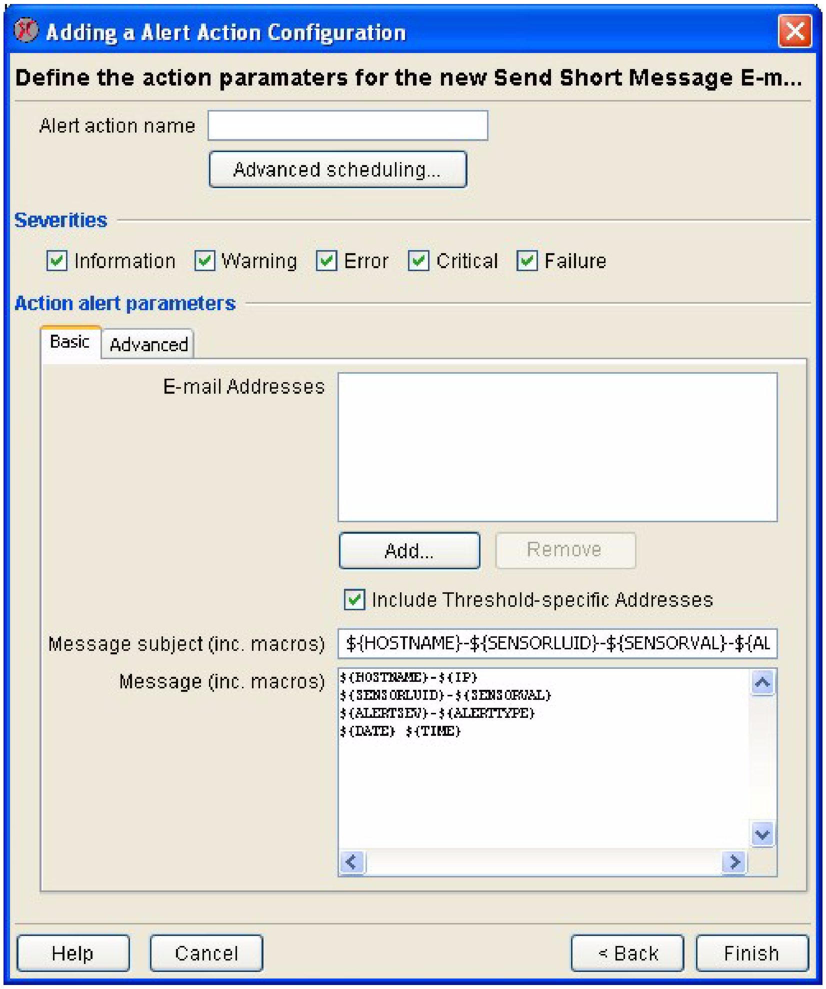
If you are creating an Alert Action that will use the Send Short E-Mail Message alert notification method:

1. Launch the Alert Actions task.
2. Select Send Short E-Mail Message from the Alert Actions drop box. Any selected devices that have previously been configured with an alert action that uses the Send Short E-Mail Message alert

notification method are displayed in the pane.

– To edit previously created Alert Actions, select the one or more entries from the Send Short E-Mail Message alert pane and then click Edit.

– To create a new Send Short E-Mail Message Alert Action, click Add, select one or more NetBotz devices from the device selection list, and click Next.



Adding a Alert Action Configuration

Define the action paramaters for the new Send Short Message E-m...

Alert action name

Severities

☑ Information ☑ Warning ☑ Error ☑ Critical ☑ Failure

Action alert parameters

E-mail Addresses

☑ Include Threshold-specific Addresses

Message subject (inc. macros): ${HOSTNAME}-${SENSORLUID}-${SENSORVAL}-${AL

Message (inc. macros):

```
${HOSTNAME}-${IP}
${SENSORLUID}-${SENSORVAL}
${ALERTSEV}-${ALERTTYPE}
${DATE} ${TIME}
```

3. Type in the Alert Action Name field a name for this alert action.

4. Specify Advanced Scheduling for the Alert Action (optional). By default, all Alert Actions are assumed to be active 24 hours a day, 7 days a week. However, you can specify that an Alert Action will be active only when alert conditions occur during specific time ranges. To configure Advanced Scheduling:

   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.

   b. By default, all time periods in the schedule are set to Enabled. To disable the Alert Action for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Alert Action for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.

   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Alert Action task.

5. Check the check boxes in the Severities check box group that correspond to the alert severities for

which SNMP trap notifications will be sent.

6. Add to the E-mail Addresses field the addresses of the recipients to whom the e-mail notification will be sent. Click Add..., type in the e-mail address to which the alert notification will be sent, and then click OK.
7. If desired, check the Include Addresses from Thresholds check box to include threshold-specific e-mail recipients.

Note

- If the E-mail Addresses field is left blank and you uncheck the Include Addresses from Thresholds check box then no e-mail notifications will be sent
- If the E-mail Addresses field is left blank and you check the Include Addresses from Thresholds check box then e-mail notifications will be sent only if the threshold that is exceeded has a Threshold-Specific Address List.

9. Type in the Message Subject field the text that will be used for the Subject of the short-format e-mail message.
10. Type in the Message field the text that will be used for the body of the short-format e-mail message.

Note

The Message Subject and Message fields accept BotzWare macros.

11. Set Advanced Alert Action settings, if desired.
    – Click the Advanced tab, and the use the controls to specify a Message Size Limit for e-mail messages generated by this alert action. This ensures that no message larger than the value you specify will be sent to the recipients.

    – Some e-mail services attempt to control spam e-mail by automatically deleting e-mail messages that contain header information that is not absolutely necessary for message delivery, such a header data that indicates that the message is “High Priority.” To include only the header information that is necessary to ensure delivery of the e-mail message, select the Advanced tab and then check the Minimize Header Usage check box.
12. Click OK to save this Alert Action.

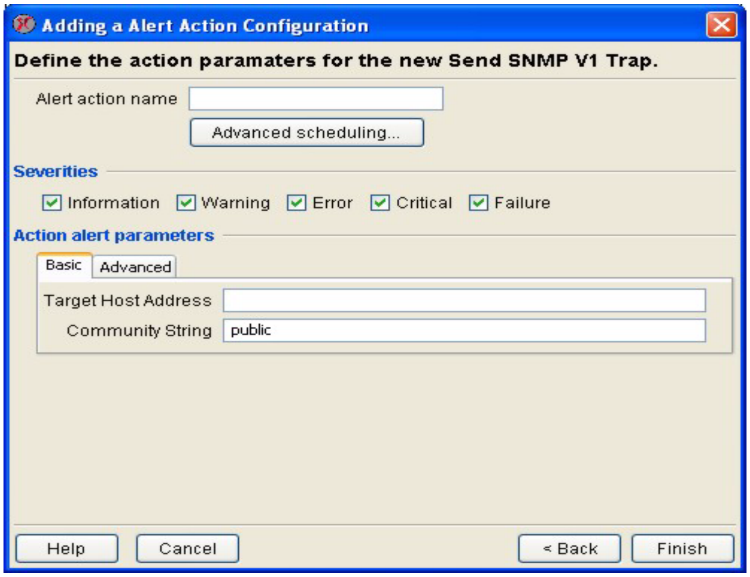
Creating a Send SNMP v1 Trap Alert Action

If you are creating an Alert Action that will use the Send SNMP v1 Trap alert notification method:

1. Launch the Alert Actions task.
2. Select Send SNMP v1 Trap from the Alert Actions drop box. Any selected devices that have previously been configured with an alert action that uses the Send SNMP v1 Trap alert notification

method are displayed in the pane.

- To edit previously created Alert Actions, select the one or more entries from the Send SNMP v1 Trap alert pane and then click Edit.
- To create a new Send SNMP v1 Trap Alert Action, click Add, select one or more NetBotz devices from the device selection list, and click Next.



Adding a Alert Action Configuration

Define the action paramaters for the new Send SNMP V1 Trap.

Alert action name

Severities

☑ Information ☑ Warning ☑ Error ☑ Critical ☑ Failure

Action alert parameters

Target Host Address

Community String: public

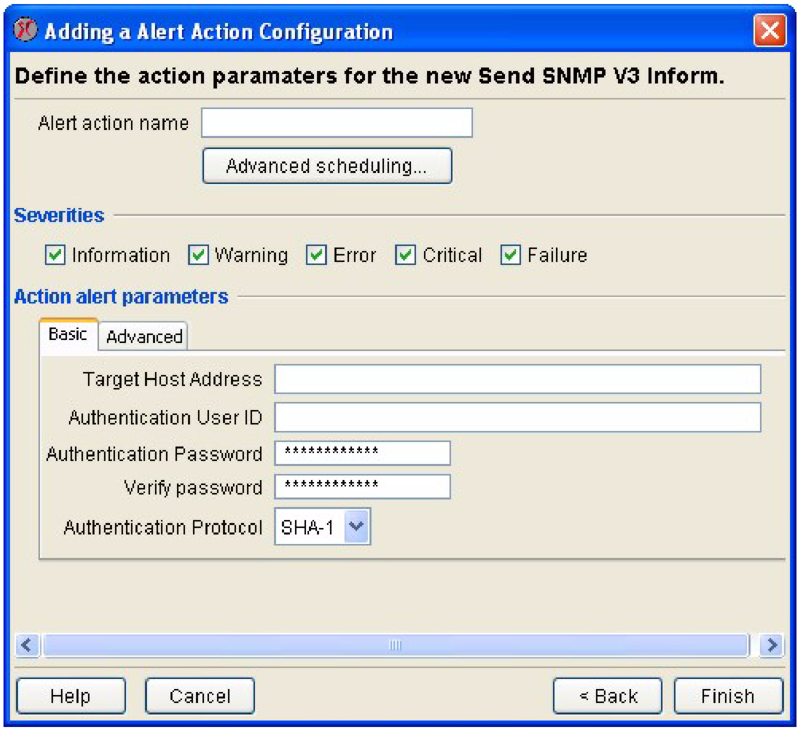
3. Type in the Alert Action Name field a name for this alert action.
4. Specify Advanced Scheduling for the Alert Action (optional). By default, all Alert Actions are assumed to be active 24 hours a day, 7 days a week. However, you can specify that an Alert Action will be active only when alert conditions occur during specific time ranges. To configure Advanced Scheduling:
   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.
   b. By default, all time periods in the schedule are set to Enabled. To disable the Alert Action for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Alert Action for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.
   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Alert Action task.
5. Check the check boxes in the Severities check box group that correspond to the alert severities for which SNMP trap notifications will be sent.
6. Type in the Target Host Address field the Hostname or IP address of the SNMP based management system.
7. Type in the Community String field the target-specific community string that will be used when sending traps to the Target Host Address.
8. Click OK to save this Alert Action.

Creating a Send SNMP v3 Inform Alert Action

If you are creating an Alert Action that will use the Send SNMP v3 Inform alert notification method:

1. Launch the Alert Actions task.
2. Select Send SNMP v3 Inform from the Alert Actions drop box. Any selected devices that have previously been configured with an alert action that uses the Send SNMP v3 Inform alert notification method are displayed in the pane.
   – To edit previously created alert actions, select the one or more entries from the Send SNMP v3 Inform pane and then click Edit.

   – To create a new Send SNMP v3 Inform alert action, click Add, select one or more devices from the device selection list, and click Next.



Adding a Alert Action Configuration

Define the action paramaters for the new Send SNMP V3 Inform.

Alert action name

Severities

☑ Information ☑ Warning ☑ Error ☑ Critical ☑ Failure

Action alert parameters

Target Host Address

Authentication User ID

Authentication Password ************

Verify password ************

Authentication Protocol SHA-1

3. Type in the Alert Action Name field a name for this alert action.
4. Specify Advanced Scheduling for the Alert Action (optional). By default, all Alert Actions are assumed to be active 24 hours a day, 7 days a week. However, you can specify that an Alert Action will be active only when alert conditions occur during specific time ranges. To configure Advanced Scheduling:
   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.
   b. By default, all time periods in the schedule are set to Enabled. To disable the Alert Action for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Alert Action for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.
   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Alert Action task.
5. Check the check boxes in the Severities check box group that correspond to the alert severities for

which SNMP trap notifications will be sent.

6. Type in the Target Host Address field the Hostname or IP address of the SNMP based management system.
7. On the Basic Tab:
   a. Type in the Authentication User ID field the user ID that will be used when sending informs to the Target Host Address.
   b. Type in the Authentication Password field the password that will be used when sending informs to the Target Host Address.
   c. Select from the Authentication protocol drop box the protocol that will be used when sending informs to the Target Host Address.
8. If desired, set additional settings on the Advanced tab:
   a. Specify an Inform Port Number. Valid port numbers can be from 1 to 65,535. Default is 162.
   b. Select from the Encryption Protocol drop box the encryption method that will be used when sending informs.
   c. Specify an Encryption Password. If this field is left blank, the Authentication Password (specified on the Basic tab) is used.
9. Click OK to save this Alert Action.

Creating a Send Wireless SMS Message Alert Action

If you are creating an Alert Action that will use the Send Wireless SMS Message alert notification method:

1. Launch the Alert Actions task.
2. Select Send Wireless SMS Message from the Alert Actions drop box. Any selected devices that have previously been configured with an alert action that uses the Send Wireless SMS Message alert notification method are displayed in the pane.
   – To edit previously created Alert Actions, select the one or more entries from the Send Wireless SMS Message alert pane and then click Edit.
   – To create a new Send Wireless SMS Message Alert Action, click Add, select one or more NetBotz devices from the device selection list, and click Next.
3. Type in the Alert Action Name field a name for this alert action.
4. Specify Advanced Scheduling for the Alert Action (optional). By default, all Alert Actions are assumed to be active 24 hours a day, 7 days a week. However, you can specify that an Alert Action will be active only when alert conditions occur during specific time ranges. To configure Advanced Scheduling:
   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.
   b. By default, all time periods in the schedule are set to Enabled. To disable the Alert Action for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Alert Action for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.
   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Alert Action task.
5. Check the check boxes in the Severities check box group that correspond to the alert severities for

which SNMP trap notifications will be sent.

6. Type in the Destination Addresses field the addresses (such as e-mail addresses or telephone numbers of SMS-enabled devices) of the recipients to whom the wireless SMS message alert notification will be sent.
7. Type in the Message field the text that will be used for the body of the short-format e-mail message.

Note

The Message field accepts BotzWare macros.

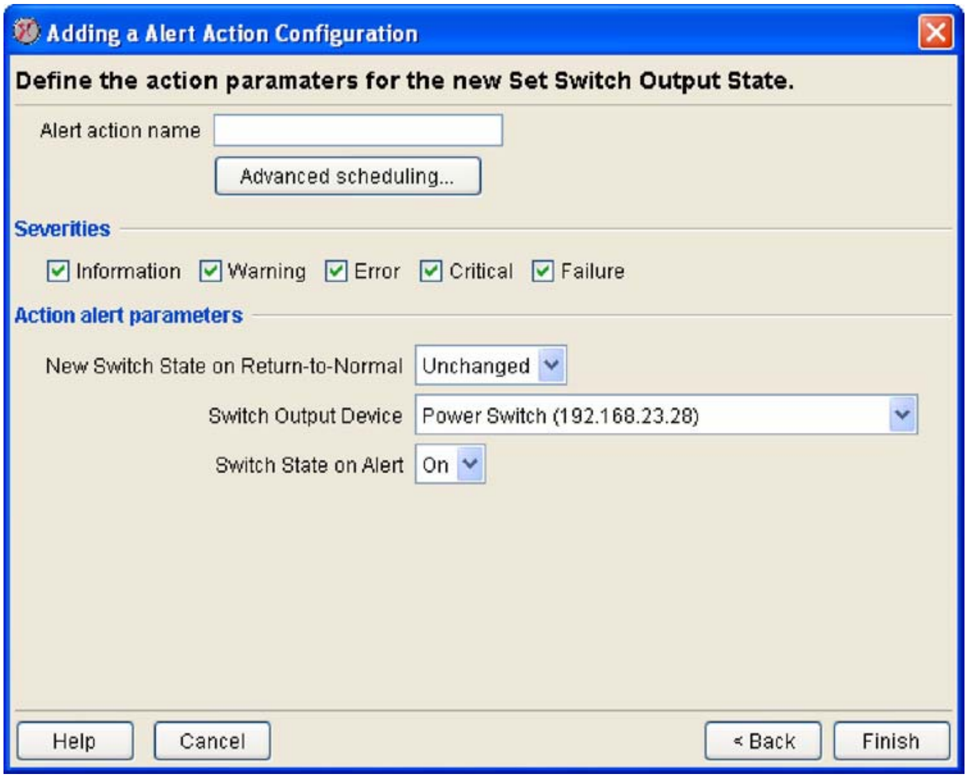
9. Set Advanced Alert Action settings, if desired. Click the Advanced tab, and the use the controls to enable of disable sending of Return-to-Normal alert notifications using this alert notification method, to specify a Message Size Limit for alert notifications generated by this alert action (maximum value is 160 characters), and to specify a Message Validity Period for this message (values range from 5 minutes to 3 days. Once the validity period expired the SMS service will no longer attempt to deliver the message).
10. Click OK to save this Alert Action.

Creating a Set Switch Output State Alert Action

If you are creating an Alert Action that will use the Set Switch Output State alert notification method:

1. Launch the Alert Actions task.
2. Select Set Switch Output State from the Alert Actions drop box. Any selected devices that have previously been configured with an alert action that uses the Set Switch Output State alert notification method are displayed in the pane.
   – To edit previously created Alert Actions, select the one or more entries from the Set Switch Output State alert pane and then click Edit.

– To create a new Set Switch Output State Alert Action, click Add, select one or more NetBotz devices from the device selection list, and click Next.



Adding a Alert Action Configuration

Define the action paramaters for the new Set Switch Output State.

Alert action name

Severities

☑ Information ☑ Warning ☑ Error ☑ Critical ☑ Failure

Action alert parameters

New Switch State on Return-to-Normal: Unchanged

Switch Output Device: Power Switch (192.168.23.28)

Switch State on Alert: On

3. Type in the Alert Action Name field a name for this Alert Action.

4. Specify Advanced Scheduling for the Alert Action (optional). By default, all Alert Actions are assumed to be active 24 hours a day, 7 days a week. However, you can specify that an Alert Action will be active only when alert conditions occur during specific time ranges. To configure Advanced Scheduling:
   a. Click Advanced Scheduling.... The Advanced Scheduling window opens.
   b. By default, all time periods in the schedule are set to Enabled. To disable the Alert Action for a currently enabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Disable. To enable the Alert Action for a currently disabled period of time, highlight the period of time by clicking-and-dragging over the desired time range, and then click Enable.
   c. When you have finished creating your Advanced Schedule, click OK to save the schedule and return to the Alert Action task.

5. Check the check boxes in the Severities check box group that correspond to the alert severities for which switches will be triggered.

6. Select from the Switch Output Device drop box the Switch Relay device that will be triggered by this alert action. All Switch Relay devices that are defined for use with this device appear in this selection list.

7. Select from the Switch State on Alert drop-box the state (“On” or “Off”) to which the Switch Relay device will be set when an alert occurs.

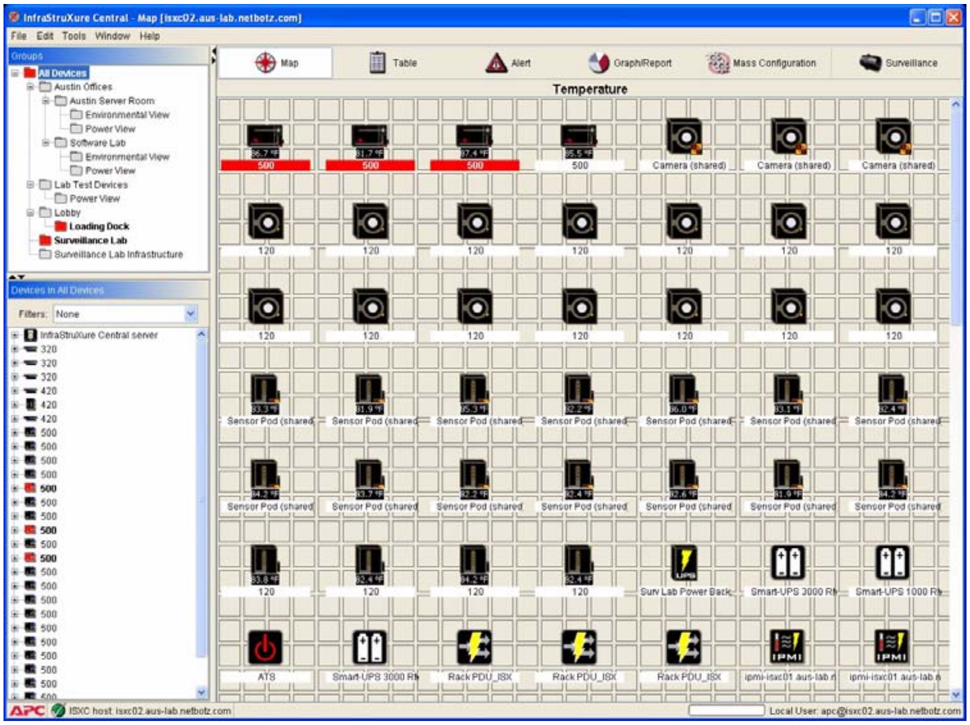
8. Select from the New Switch State on Return to Normal drop-box the state (“Unchanged,” “On,” or “Off”) to which the Switch Relay device will be set when the violated threshold returns to a normal

state.

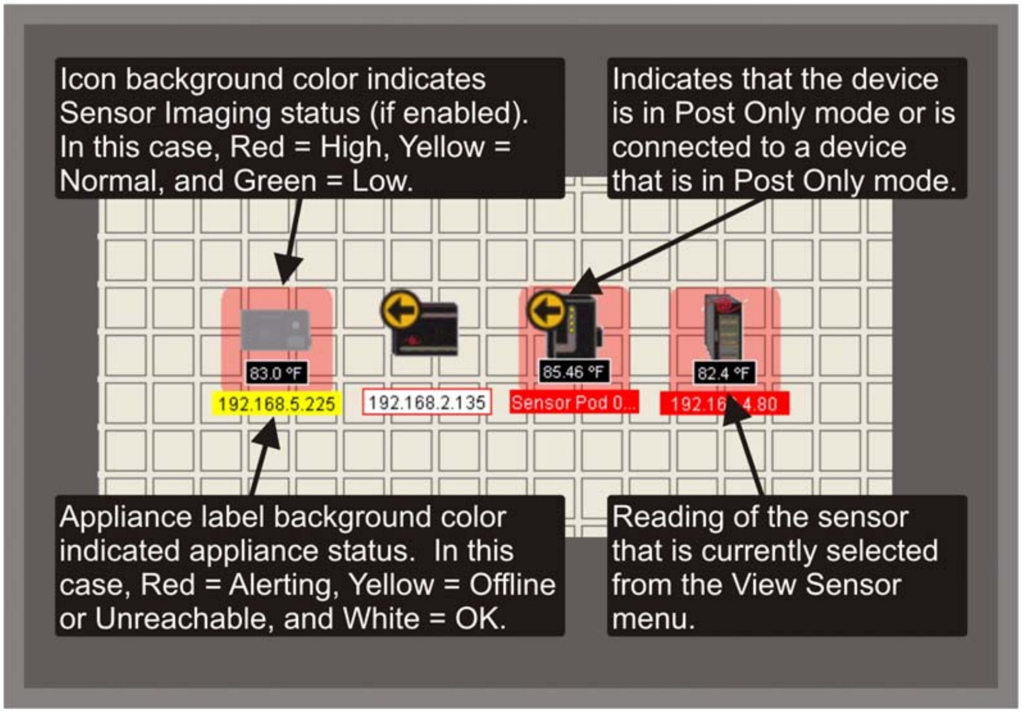
9. Click OK to save this Alert Action.

Using the Map View

The InfraStruXure Central Map View presents all devices in the currently selected device group in an easy-to-monitor graphic display. Colors are used to indicate the current state of each devices in the device group, alerts or network outages are easily noted, and the current reading of a selected sensor is displayed for all devices. You can also use custom background graphics and rearrange the contents of the device group to better represent the physical environment in which the devices are installed, making it easier to locate problem areas in your installation.



To use the Map view, select a device group from the Device Group Navigation pane and then click the Map tab. The devices that are part of the selected device group appear in the Map view window. Each device is shown as an icon, along with a display name (IP address, location value, MAC address, or hostname, depending on your Client Preferences), and a current sensor reading. Also, any devices that are in Post Only mode, or that are connected to devices that are in Post Only mode, are indicated with a small yellow and black arrow icon as shown below:



Icon background color indicates Sensor Imaging status (if enabled). In this case, Red = High, Yellow = Normal, and Green = Low.

Indicates that the device is in Post Only mode or is connected to a device that is in Post Only mode.

Appliance label background color indicated appliance status. In this case, Red = Alerting, Yellow = Offline or Unreachable, and White = OK.

Reading of the sensor that is currently selected from the View Sensor menu.

The sensor that is currently selected is shown above the Map view, in the center of the Action/Information pane. If you select one or more devices from the Device Selection pane, the icons for the selected devices are selected in the Map view as well. To access other InfraStruXure Central Map View functions, right-click on the Map view to open the Map View context menu. The following selections are available from this context menu:

Context Menu Selection	Description
New...	Adds a user-specified management device or SNMP device. For more information, see “Adding New Devices” on page 111. **Note:** If the added device does not meet the configuration criteria for inclusion in the currently selected device group, the device group will not be shown. However, the device will be automatically added to any dynamically defined device groups with appropriate configuration criteria.
Delete device	Deletes all selected devices. **Note:** Deleting a device purges all data associated with the device from the InfraStruXure Central database and also deletes the device from any other device groups in which it exists, including other device groups to which you may not have access. Improper use of this function could result in loss of data and could also impact other InfraStruXure Central users.

Context Menu Selection	Description
Delete monitored device	Deletes all selected monitored devices (such as Sensor Pod 120s or Camera Pod 120s). **Note:** Deleting a monitored device purges all data associated with the monitored device from the InfraStruXure Central database and also deletes the monitored device from any other device groups in which it exists, including other device groups to which you may not have access. Improper use of this function could result in loss of data and could also impact other InfraStruXure Central users.
Find Device...	Simplifies finding specified devices. Type in the IP address, host name, or location information for the device you are trying to find. If it is located on the currently selected map it will be selected for you automatically.
Change Icon	Each device displayed in the Map View is represented by a default device type icon. If desired, you can use the Change Icon selection to specify a unique device-specific icon instead of the default icon.
Use Sensor Imaging	Use this control to enable or disable Map View sensor imaging.
Sensor Imaging Preferences	Use this control to specify sensor imaging settings. Sensor imaging enables you to see at a glance the general state of each of your devices. Once you have defined a range of values for the currently selected sensor, the background color behind a device icon will change to reflect where it’s current sensor reading falls in the sensor imaging range. By setting imaging values that range from the optimal value to a value that equals the value at which an alert will be triggered you can spot “trouble spots” in your installations before alerts start going off.
Selection	Use this control to quickly select or un-select all devices in the Map View.
Sort by Alert	When enabled, the Sort by Alert function automatically sorts the devices in your map, displaying any devices that are offline first, followed by any devices that are reporting an alert, followed finally by device that are online and in a normal state.
Edit Map	Use the selections available from the Edit Map menu to create a custom map, delete a previously saved custom map, specify icon preferences, add a custom background image to your Map, and to specify sensor display preferences. For more information, see “Editing Map Settings” on page 252.
View Current Sensors	Opens a window that displays the current sensor readings and image capture for the selected device.
Launch Browser	Opens your system's web browser and directs it at the URL of the selected device.
Request Device Scan	Select this to cause InfraStruXure Central to initiate a scan of the selected SNMP device immediately.

Context Menu Selection	Description
Mass Configuration	Use this flyout menu to quickly select and start Mass Configuration tasks on the selected devices.
Filters	Enables you to create, edit, or delete filters. These filters are used to determine which devices are included in the Map and Table View. For more information, see “Using Filters” on page 57.
Tutorial	Select Tutorial to display the InfraStruXure Central tutorial. Once you have opened the tutorial it will automatically start each time you start the InfraStruXure Central console until you un-check the **Show this at next startup** check box.
Help	Select Help to view the InfraStruXure Central online help.

Editing Map Settings

Creating Custom Maps

Once you have selected **Edit Custom Map** from the Edit Map menu item, you can drag and drop any devices that are shown on the map to specific locations. This can be helpful if you have many devices and want to arrange them in a manner that is similar to their physical location within your installation.

When you have finished editing the map, click **Save Custom Map** to save the locations. To revert to the default Map view, click **Delete Custom Map**.

Changing the Map Background

To add a background image to a Map, click **Change Background**, select the image you wish to use, and then click **OK**.

Setting Icon Preferences

You can customize the appearance of the icons in the Map View by right-clicking in the Map View and selecting Edit Map>Icon Preferences. This will open the Icon Preferences window. This window consists of two panes:

- Icon Display: Enables you to select whether the device label is displayed horizontally and below the device icon or vertically and to the right of the icon.
- Icon Sizing: Features two slider controls that enable you to adjust the vertical and horizontal sizing of the device icons.

Adjust the icon preferences as desired and then click OK to save your settings.

Setting Sensor Display Preferences

Use Sensor Display Preferences to specify the default sensor value that will be shown for all devices in the Map view, and to select device-specific sensor display values for selected devices that override the default sensor value.

By specifying device-specific sensor displays, you can ensure that devices that report sensor data that does not correspond with the selected default sensor type will show meaningful data. For example, if you select “Temperature” as a default sensor display, devices that do not include temperature sensors (such as camera pods, for example) would not typically show a current sensor reading of any sort. However, if you specify a device-specific sensor value display for your camera pods (such as camera motion sensor, for example) then the current sensor value for the selected sensor will be shown by the device icon instead of the default sensor value.

- To specify a default sensor display select the **Default** tab, select the desired default sensor from the Default Sensor Type tree view, and then click **OK**.
- To specify device-specific sensor value displays, select the **Selected** tab, select one or more devices from the **Selected Devices** selection list, select the desired sensor from the **Sensor Types** tree view on the right, and then click **OK**.

Using Sensor Imaging

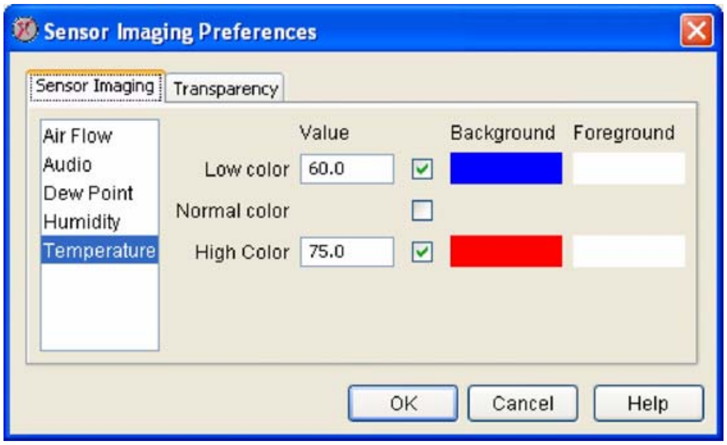
Sensor Imaging enables you to see at a glance the general state of each of your devices. Once you have defined a range of values for the currently selected Display Sensor, the color of the device icon will change to reflect where it's current sensor reading falls in the display imaging range. By setting imaging values that range from the optimal value to a value that equals the value at which an alert will be triggered you can use display imaging to spot “trouble spots” in your facilities before alerts start going off.

Sensor Imaging is enabled by default, with a default value range pre-configured for each of the device sensors. To enable or disable Sensor Imaging:

1. Right-click on the Map View. This will open a context menu.
2. Click Use Sensor Imaging > On (or Off).

Depending on your environment and needs, you may wish to change the Sensor Imaging values for your devices. To review or change your Sensor Imaging settings:

1. Right-click inside the Map View. This will open a context menu.
2. Click Sensor Imaging Preferences. The Sensor Imaging Preferences window opens.
3. Select a sensor from the Sensor List selection list to view its current Sensor Imaging configuration. Once you select a sensor, the high and low values used to define the Senor Imaging range for that sensor are displayed in the Low Color and High Color fields. Also, the colors that are currently defined for the Low, Normal, and High Sensor Imaging states are shown in the Low Color, Normal Color, and High Color drop boxes.



	Value		Background	Foreground
Low color	60.0	☑	🟦	⬜
Normal color		☐		
High Color	75.0	☑	🟥	⬜

If the sensor value that is reported by a device is less than the value you specify for the sensor in the Low Value field then a semi-transparent block of the Low Color will appear behind the device icon. If the sensor value that is reported by a device is higher than the value you specify for the sensor in the High Value field then a semi-transparent block of the High Color will appear behind the device icon. If the value falls between or equals either the Low and High values then a semi-transparent block of the Normal Color will appear behind the device icon.

If you want to change any of these settings for a sensor, simply select the sensor, specify new low and/or high values, and select new Sensor Imaging colors as desired. You can also use the slider control in the Transparency tab to adjust the transparency of the Sensor Imaging color blocks that appears behind the icon in the Map view.

4. When you are finished, click OK to save your new Sensor Imaging configuration.

Map Sharing

InfraStruXure Central supports Map Sharing. Map Sharing enables you to create a custom device group map that will be automatically shared with any users that are authorized to access the device group. When you create a shared map, other InfraStruXure Central users that view the device group will automatically inherit the position of device icons on the map and the background image you select.

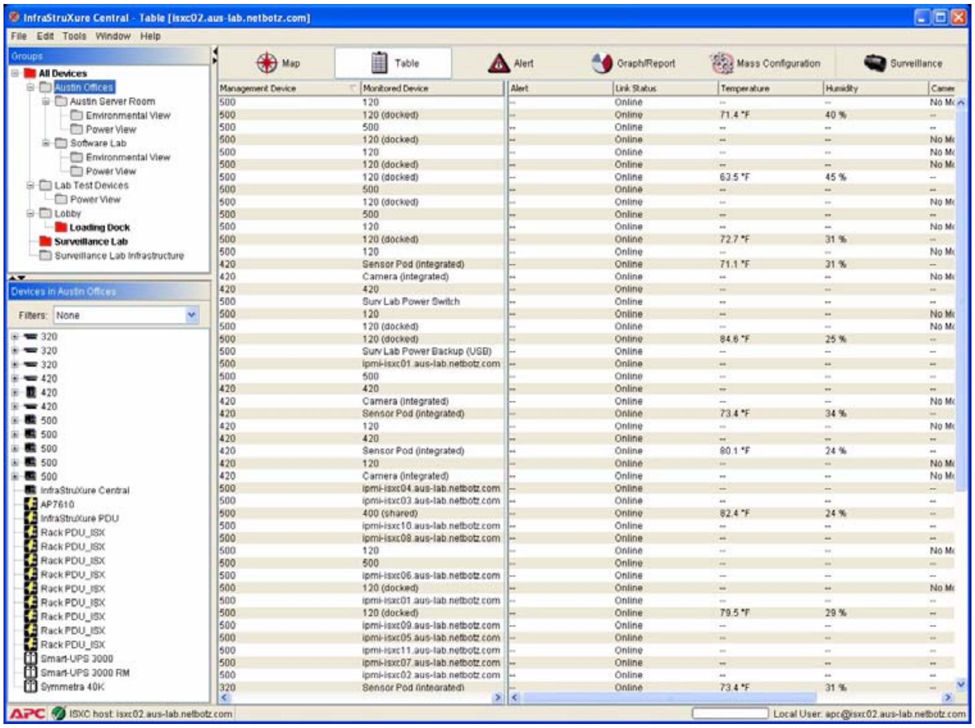
The following usage rules apply to Shared Maps:

- Only Administrator-level user accounts (accounts that have both Read/Write access to User Administration and Write access to the device group for which a map will be shared) can create a shared map.
- Once created, only a user with Administrator-level access to a device group with a shared map can delete that map. If multiple Administrator-level users can access a device group any of those users can delete a shared map, even if they did not create the shared map.
- If you are using a map that has been shared by your Administrator, you can edit contents of that device group. However, any changes you make to the device group will be seen only on your system and will not be shared with other users.
- Once a map is shared, only an Administrator-level user can make changes to the shared map and re-share it so that other device group users inherit the new shared map settings.
- Users that edit a shared map but who do not re-share it (either because they are not Administrator-level users, or because they are Administrators but choose not to share the map) will not inherit changes made to their maps by other Administrators unless they use Delete Custom Map command to remove the files associated with their custom version of the shared map from the server.

Administrator-level users that have created a shared map, and who have then made changes to the map without re-sharing their changes will have a custom version of the map for themselves, just as users without Administrator-level access have when they save changes made to a shared map. In this case if you want to delete the shared map you must first use Delete Custom Map to delete your local version of the map files. Once these files are deleted you will automatically inherit the shared map. Then, if you use Delete Custom Map again you will delete the shared map for all other users.

Using the Table View

The InfraStruXure Central Table view presents all currently selected devices in an easy-to-monitor and read table display. Colors are used to indicate the current state of each device, making alerts or offline devices easy to spot. You can also use Table Preferences to specify the data that is displayed for each device.



Management Device	Monitored Device	Alert	Link Status	Temperature	Humidity	Camer
500	120	--	Online	--	--	No M
500	120 (docked)	--	Online	71.4 °F	40 %	--
500	500	--	Online	--	--	--
500	120 (docked)	--	Online	--	--	No M
500	120	--	Online	--	--	No M
500	120 (docked)	--	Online	--	--	No M
500	120 (docked)	--	Online	63.5 °F	45 %	--
500	500	--	Online	--	--	--
500	120 (docked)	--	Online	--	--	No M
500	500	--	Online	--	--	--
500	120	--	Online	--	--	No M
500	120 (docked)	--	Online	72.7 °F	31 %	--
500	120	--	Online	--	--	No M
420	Sensor Pod (integrated)	--	Online	71.1 °F	31 %	--
420	Camera (integrated)	--	Online	--	--	No M
420	420	--	Online	--	--	--
500	Surv Lab Power Switch	--	Online	--	--	--
500	120	--	Online	--	--	No M
500	120 (docked)	--	Online	--	--	No M
500	120 (docked)	--	Online	84.6 °F	25 %	--
500	Surv Lab Power Backup (USB)	--	Online	--	--	--
500	ipmi-isxc01.aus-lab.netbotz.com	--	Online	--	--	--
500	500	--	Online	--	--	--
420	420	--	Online	--	--	--
420	Camera (integrated)	--	Online	--	--	No M
420	Sensor Pod (integrated)	--	Online	73.4 °F	34 %	--
420	120	--	Online	--	--	No M
420	420	--	Online	--	--	--
420	Sensor Pod (integrated)	--	Online	80.1 °F	24 %	--
420	120	--	Online	--	--	No M
420	Camera (integrated)	--	Online	--	--	No M
500	ipmi-isxc04.aus-lab.netbotz.com	--	Online	--	--	--
500	ipmi-isxc03.aus-lab.netbotz.com	--	Online	--	--	--
500	400 (shared)	--	Online	82.4 °F	24 %	--
500	ipmi-isxc10.aus-lab.netbotz.com	--	Online	--	--	--
500	ipmi-isxc08.aus-lab.netbotz.com	--	Online	--	--	--
500	120	--	Online	--	--	No M
500	500	--	Online	--	--	--
500	ipmi-isxc06.aus-lab.netbotz.com	--	Online	--	--	--
500	120 (docked)	--	Online	--	--	No M
500	ipmi-isxc01.aus-lab.netbotz.com	--	Online	--	--	--
500	120 (docked)	--	Online	79.5 °F	29 %	--
500	ipmi-isxc09.aus-lab.netbotz.com	--	Online	--	--	--
500	ipmi-isxc05.aus-lab.netbotz.com	--	Online	--	--	--
500	ipmi-isxc11.aus-lab.netbotz.com	--	Online	--	--	--
500	ipmi-isxc07.aus-lab.netbotz.com	--	Online	--	--	--
500	ipmi-isxc02.aus-lab.netbotz.com	--	Online	--	--	--
320	Sensor Pod (integrated)	--	Online	73.4 °F	31 %	--

To use the Table view, select a device group from the Group Navigation pane and then click the Table button. Data about all devices in the selected device group are displayed in a table. Problems, such as device outages or alert conditions, are indicated by a user-defined color (red by default; for information on how to change the default colors see Client Preferences) in the appropriate field. If you select one or more appliances from the Device Selection pane the entries for the selected appliances in the Table view are selected as well.

To access other InfraStruXure Central Table view functions, right-click on the Table view to open the Table View context menu. The following selections are available from this context menu:

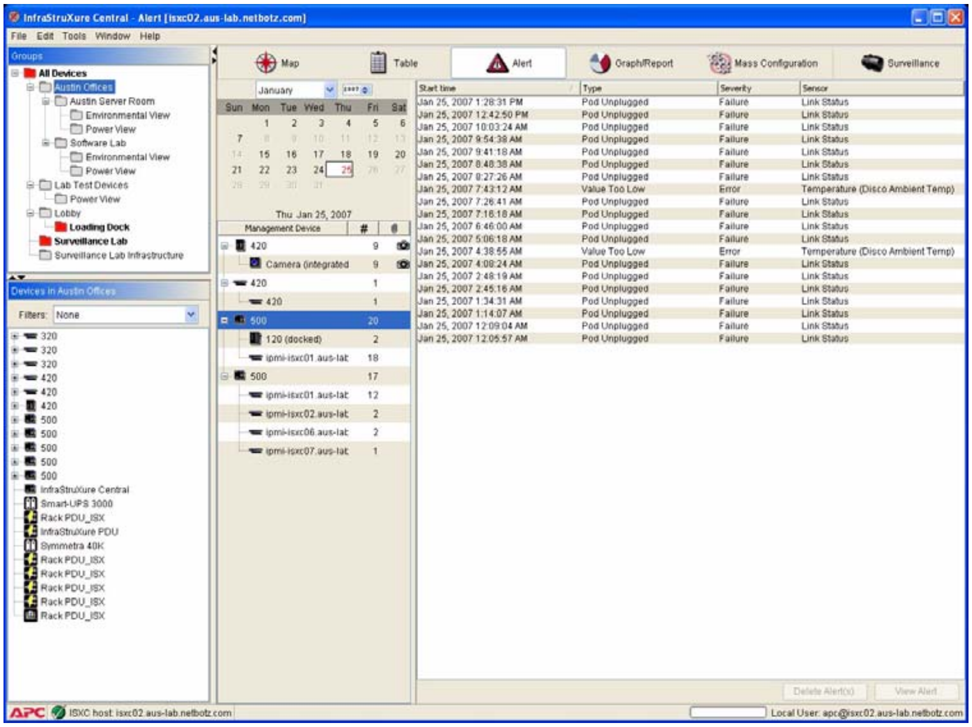
Context Menu Selection	Description
New...	Adds a user-specified management device or SNMP device. For more information, see “Adding New Devices” on page 111. **Note:** If the added device does not meet the configuration criteria for inclusion in the currently selected device group, the device group will not be shown. However, the device will be automatically added to any dynamically defined device groups with appropriate configuration criteria.

Context Menu Selection	Description
Delete Device	Deletes all selected devices from the current Map. **Note:** Deleting a device purges all data associated with the device from the InfraStruXure Central database and also deletes the device from any other device groups in which it exists, including other device groups to which you may not have access. Improper use of this function could result in loss of data and could also impact other InfraStruXure Central users.
Delete Monitored Device	Deletes all selected monitored devices (such as Sensor Pod 120s or Camera Pod 120s) from the currently selected group. **Note:** Deleting a monitored device purges all data associated with the monitored device from the InfraStruXure Central database and also deletes the monitored device from any other device groups in which it exists, including other device groups to which you may not have access. Improper use of this function could result in loss of data and could also impact other InfraStruXure Central users.
Table Preferences	Use this control to specify what device data will be displayed for each device in the Table view.
Export Table	Use this control to export the appliance data displayed in the table to a delimited value file.
View Current Sensors	Opens a window that displays the current sensor readings and image capture for the selected appliance.
Request Device Scan	Select this to cause InfraStruXure Central to initiate a scan of the selected SNMP device immediately.
Launch Browser	Opens your system's web browser and directs it at the URL of the selected device.
Filters	Enables you to create, edit, or delete filters. These filters are used to determine which devices are included in the Map and Table View. For more information, see “Using Filters” on page 57.
Tutorial	Select Tutorial to display the InfraStruXure Central tutorial. Once you have opened the tutorial it will automatically start each time you start the InfraStruXure Central console until you un-check the **Show this at next startup check box.**
Help	Select Help to view the InfraStruXure Central online help.

Using the Alert View

The InfraStruXure Central Alert View enables you to easily view a summary of all alert events that were reported by any selected devices on a user-specified day. Any alert events that were active on the specified date as displayed, as are any alert events that were resolved on the selected date, regardless of when the alert event began. Alert events begin at the time a specified threshold is exceeded and end when the alerting sensor has returned to a “normal” state. Therefore, depending on the nature of the alert, an alert event can continue for more than one day.

Alerts that contain picture data can also be viewed, provided that the alert has been posted to the InfraStruXure Central server using the device HTTP post support or by using the Send to InfraStruXure Central or Send HTTP Post alert actions, available using the Alert Action task.



Thu Jan 25, 2007

Management Device	#	📎
420	9	📷
Camera (integrated	9	📷
420	1	
420	1	
500	20	
120 (docked)	2	
ipmi-isxc01.aus-lat	18	
500	17	
ipmi-isxc01.aus-lat	12	
ipmi-isxc02.aus-lat	2	
ipmi-isxc06.aus-lat	2	
ipmi-isxc07.aus-lat	1	

Start time	Type	Severity	Sensor
Jan 25, 2007 1:28:31 PM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 12:42:50 PM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 10:03:24 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 9:54:38 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 9:41:18 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 8:48:38 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 8:27:26 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 7:43:12 AM	Value Too Low	Error	Temperature (Disco Ambient Temp)
Jan 25, 2007 7:26:41 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 7:16:18 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 6:46:00 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 5:06:18 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 4:38:55 AM	Value Too Low	Error	Temperature (Disco Ambient Temp)
Jan 25, 2007 4:08:24 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 2:48:19 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 2:45:16 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 1:34:31 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 1:14:07 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 12:09:04 AM	Pod Unplugged	Failure	Link Status
Jan 25, 2007 12:05:57 AM	Pod Unplugged	Failure	Link Status

To see a summary of all alert events that were active and/or resolved on a particular date, select the desired date using the calendar control in the Alerts View. Dates on which no alert events have occurred are grayed out in the calendar.

Once you have selected a date, a list of the devices that have reported alert events appears below the calendar control. If a device is not listed, then either no alert events were active on the selected device on the selected date or you have not configured InfraStruXure Central to collect data from a device group that includes the device, so alert event data has not been collected from the device and added to the database. The number of alert events that were active on each device on the selected date appears in the # column beside the device entry. If the alert includes picture data, graphs, audio clips, or other attachments, a number representing the number of attachments included in the alert appears in the attachment column (labeled with the image of a paper clip) beside the device entry. If a device has a pod or other device connected that has reported an alert event it will be nested underneath the device to which it is connected.

To see a list of the alert events that occurred on a device on the selected date, select the device. A list of all alert events associated with the selected device appears in a table in the Alert View pane.

Alert events that are presently ongoing and have not yet been resolved will be displayed with a red background, regardless of the date that is selected. For example, if you select a date from a week past and an alert event is shown that started on the selected date but which has not yet been resolved, it will appear with a red background. This indicated that this alert event continues to be unresolved, even though the date you are viewing in the Alert view is from a time in the past.

Each alert event entry in the table includes a column for the Start Time for the alert event (the time at which the alert event began. Note that an alert event may have begun on days prior to the selected date), the alert Type, the Severity value associated with the alert event, and the Sensor on the selected device that reported the alert condition. For additional information about a single alert event hover over an entry and the Start Time, Resolve Time (time at which the alert event resolved, if applicable), Type, Severity, Sensor, and a Description of the alert event appear in a hover help.

To see the complete contents of an alert event, double-click on the alert event entry. An Alert Details window appears, featuring detailed information about the alert event. All Alert Details windows will feature the Start Time, Resolve Time, Type, Severity, Sensor, and Description of the alert event, as well as the IP address, hostname, and Location data (if available) associated with the device that reported the alert event. Depending on the sensor or device that generated the alert event additional alert event data (including camera images, graphs, and audio) may be available as well. If a graph is available, the portion of the graph that corresponds to the period of time in which the alert event occurred will be shown in red.

To delete alert events from the database, select one or more alert events and then click on Delete Alert(s). Note that only resolved alert events can be deleted. If any of the selected alert events are not yet resolved the Delete Alert(s) button will not be available for use.

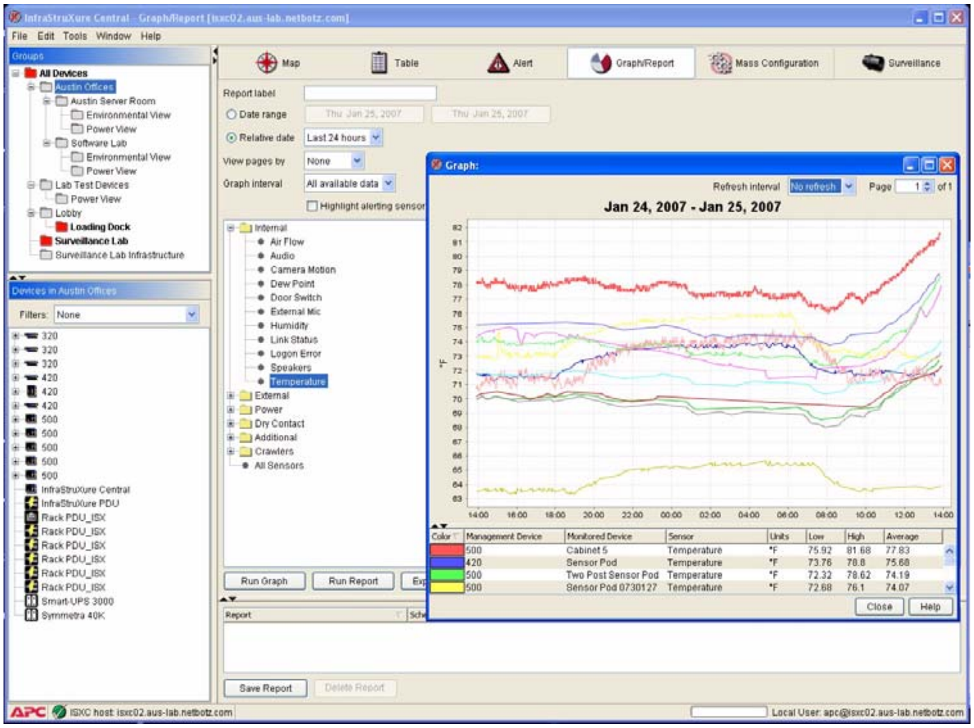
Displaying Alert Images as a Movie

If you have installed the InfraStruXure Central Surveillance license key you can play images that have been captured as part of an alert as a movie. If the InfraStruXure Central Surveillance is installed, buttons for Stop (■), Play (▶), Faster Playback (▶▶), and Slower Playback (◀◀) will be available beneath the alert image.

To play the alert images, click the Play button (▶). Playback will loop until you click the Stop (■) button. Use the Faster Playback (▶▶) and Slower Playback (◀◀) buttons to adjust the playback speed.

Using the Graph/Report View

The InfraStruXure Central Graph/Report view enables you to generate reports, for a user-specified time period, from the data collected from the sensor data collected by one or more devices. The data can be plotted in a graph to simplify data collation and comparison, or it can be can be collated into a single report to simplify data collation, collection, and comparison. Report data (or from a selected portion of the report) can be exported to a server and saved for future reference. Report data can also be exported as a delimited value text file.



Report label

○ Date range Thu Jan 25, 2007 Thu Jan 25, 2007

● Relative date Last 24 hours

View pages by None

Graph interval All available data

□ Highlight alerting sensors

Refresh interval No refresh Page 1 of 1

Color	Management Device	Monitored Device	Sensor	Units	Low	High	Average
🟥	500	Cabinet 5	Temperature	°F	75.92	81.68	77.83
🟦	420	Sensor Pod	Temperature	°F	73.76	78.8	75.68
🟩	500	Two Post Sensor Pod	Temperature	°F	72.32	78.62	74.19
🟨	500	Sensor Pod 0730127	Temperature	°F	72.68	76.1	74.07

To use the Graph/Report view:

1. Select a device group from the Group Navigation pane, or one or more devices from the device selection window, and then click the Graph/Report button.
2. If you would like to name this report so you can save it and re-run it later, type a name in the Report label field.

Note

You must provide a report label to save reports for use later.

3. Specify the time period for which the report will be run by selecting either the Date Range or

Relative Date radio button.

- If you select Date Range, and use the two calendar controls to specify the date range for the graph.
- If you select Relative Date, select the time period prior to the present (Today, Last 24 Hours, Last Week, etc.) for which data will be collected.

4. Select from the View pages by drop box what portion of the total amount of data will be shown in each page of the resulting report or graph.
5. Select from the Graph interval drop box the time interval for which data will be included in the resulting report or graph.
6. Select from the Sensor tree the sensors for which data will be included in the resulting report or graph and then click the right arrow button to add the sensors to the list on the right. To remove sensors from the list, select them and then click the left arrow button.
7. Check the Highlight alerting sensors check box to highlight the names of sensors that are reporting alerts in the graph or report. In a graph, the sensors that are reporting an error will be shown with a heavier line. In a report, the entries in the report that correspond to alert states will be highlighted.
8. Check the Only show alert and clear check box to include only the alert and alert cleared values for the selected sensors. This option is used only when generating a report and has no effect on graphs that are generated using the Graph view.
9. Click the button that corresponds to the graphing or reporting function you wish to perform.
   - Click Run Graph to generate a graph of the collected data. See “Using Graphs” on page 260 for more information.
   - Click Run Report to generate a report from the collected data. See “Using Reports” on page 261 for more information.
   - Click Export Report to export and save the collected data as a delimited text file.

Using Graphs

Each line that is shown in the graph corresponds to a single sensor on a single selected device. A table showing which line color corresponds to which device and sensor appears at the bottom of the Graph/ Report window.

To select a portion of a graph and display only the selected data click and drag a box around the portion of the graph that you want to view. The data points from the selected area of the graph will then be re-graphed. To restore the full-graph, right-click on the graph and select Zoom Out.

The graph can be saved as a graphic file (JPG or BMP format). To save the graph as a graphic file, right-click on the graph and select Save Graph.

Using Reports

Once you have run a report, you can save the report settings for future use. Saved reports can be configured to run automatically according to a user-defined schedule. If desired, results from saved reports can be exported to a user-specified repository automatically as well.

Note

Scheduled reports can only be automatically exported to previously configured export entries. Export entries are created using the Server Administration: Export Administration task, and will not be available for use until they have first been created and saved using the Export Administration task. For more information, see “Export Administration” on page 85.

To save your report settings, click Save Report. The Save Report window appears. The following Save Report controls are available:

Control	Description
Report label	Displays the Report label value (specified in the report's settings in the Graph/Reports view).
Export to Use	Select from this drop box the previously configured export entry that will be used to export this report. Export entries are created using the Server Administration: Export Administration task, and will not be available for selection from the Save Reports window until they have first been created and saved using the Export Administration task. For more information, see “Export Administration” on page 85.
Scheduled check box	Check this check box to enable this report to be run on a user-specified schedule.
Days check boxes	Check the check boxes that correspond to the days of the week on which you want the report run.
Time controls	Use the time controls to specify the time of day at which the report will run.
Delimiter	Select from this drop box the data delimiting character that will be used in the exported report.

Once you have finished editing the report settings click Save Report.

To delete previously saved reports, select the desired report and then click Delete Report.

Using Post Only Mode with InfraStruXure Central

APC NetBotz devices support InfraStruXure Central Post Only Mode. When a device is configured to use Post Only mode, the APC NetBotz device initiates all communications. Typically, InfraStruXure Central periodically queries any APC NetBotz device that it has discovered for status and environmental data information (for more information, see “Data Collection/Monitoring Settings” on page 75). However, when an APC NetBotz device is configured to use Post Only mode the device controls when data is delivered to InfraStruXure Central, posting specified data directly to one or more InfraStruXure Central servers according to user-specified settings.

Post Only Communications Behavior

- Post Only mode is configured on your APC NetBotz devices using the Advanced View. See “Enabling Post Only Mode on Your Devices” on page 264 for instructions.
- When Post Only mode is in effect, all communications between the APC NetBotz monitoring device and InfraStruXure Central is initiated by the device. Alerts are sent immediately, as always: If an alert fails, the monitoring device will hold and re-try. Sensor data is posted to InfraStruXure Central at user-defined intervals.
- If a InfraStruXure Central console user makes a configuration or threshold change to a device that is in Post Only mode, the task will be placed in the Pending Requests queue and will be sent as a reply on the next occasion it receives a sensor data post from the device. The device will then acknowledge the InfraStruXure Central request and confirm that the task has been completed.
- In Post Only mode, the normal definition of Offline does not apply because by definition the device is Online only when it contacts InfraStruXure Central. Therefore, Post Only devices are typically in an Offline/Configurable state, and are considered Offline only if InfraStruXure Central has not received a post from the device within the amount of time specified by the Device Interval setting (for more information, see “Management Device Job Control” on page 89).
- In the InfraStruXure Central Map View, Post Only devices are indicated by a small arrow image that appears over the device icon, as well as over any other devices that are associated with the device (pods and crawlers, for example). If you hover the mouse over the icon, the ‘Last Post’ date and time is shown with the sensor readings.
- The Device Job Control task enables you to check the status of tasks that have been assigned to Post Only devices. You can use the Device Job Control task to delete a pending task. However, if any task is deleted, all other subsequent tasks that are also pending for the same device will also be deleted.
- When a device is using Post Only mode, InfraStruXure Central is aware of the state of the device as of the last post. For example, if the last post was 25 minutes ago, the sensor readings and camera image displayed are also from 25 minutes ago. If changes are made to the device configuration using the Basic View or Advanced View between posts, InfraStruXure Central will assume that the BotzWare settings are correct and synchronize with the new device settings it receives. APC strongly suggests that you restrict Advanced View configuration access to

devices being managed by InfraStruXure Central in general, especially when those devices are in a Post Only mode.

- If desired, you devices can post to multiple InfraStruXure Central servers. This is useful if your company uses a disaster recovery site. In this case, a second InfraStruXure Central system would be set up at the disaster recovery site and it would receive posts from Post Only devices on the same schedule as the main system. In this configuration, **all** management and configuration operations should be executed from the main InfraStruXure Central system.

Enabling Post Only Mode on Your Devices

Note

Post Only mode is supported only on APC NetBotz devices that are running BotzWare 2.2.1 or later. If necessary, be sure to upgrade the BotzWare on your devices before continuing.

To enable Post Only mode on an APC NetBotz device:

1. Start the NetBotz Advanced View (version 2.2 or later) and connect to the device that you want to configure to use Post Only mode.
2. Select from the Tools pull-down menu Advanced > InfraStruXure Central Post Only Mode.
3. The InfraStruXure Central Post Only Mode Configuration window opens.
4. If the device is not yet in Post Only mode, no InfraStruXure Centrals will be shown in the InfraStruXure Central servers selection list. Click Add to add a InfraStruXure Central server to which posts will be sent.
5. A second InfraStruXure Central Post Only Mode Configuration window opens. This window contains the following fields and controls:

Field	Description
InfraStruXure Central Server IP Address/Hostname	The IP address or hostname of the InfraStruXure Central server to which data will be posted.
Port	The IP port on the InfraStruXure Central server over which Post Only communications will occur.

Field	Description
SSL Options	Select from this drop box the selection that corresponds to the SSL communication options that you want to apply to communications between the device and the InfraStruXure Central server. You can choose the following options: • Do not user SSL: Do not use SSL for data delivery, even if supported • Require SSL: No verification: Require SSL support on the server (do not deliver without it), but accept any certificate provided by the server (i.e. self signed certificates will be allowed). • Require SSL - verify certificate: Require SSL support on the server (do not deliver without it), and only accept certificates signed by a trusted certificate authority (i.e. self signed certificates will not be allowed, but Verisign and the like certificates will be accepted even if the hostname does not match the host in the certificate). • Require SSL - verify certificate and hostname: Require SSL support on the server (do not deliver without it), and only accept certificates signed by a trusted certificate authority and which contain a hostname matching that used to contact the server (i.e. only certificates issued by trusted sources and which contain the same hostname as used to access the server are allowed).
Interval Between Posts	Use the controls to specify the number of minutes that will be allowed to pass between automatic sensor data posts to the InfraStruXure Central server. Note that if an alert is reported, the device will post the alert data immediately.
InfraStruXure Central User ID	The user ID of a user account on the InfraStruXure Central server that has Administrator access.
InfraStruXure Central Password	The password that corresponds to the InfraStruXure Central User ID account.

When you have finished providing the needed data, click OK to continue.

6. The InfraStruXure Central server data you entered should now appear in the InfraStruXure Central server selection list. If desired, test the Post Only configuration by selecting the new InfraStruXure Central server entry from the selection list and then clicking Post to InfraStruXure Central Now. After a brief delay, the Status field beside the selected entry should update to indicate that the post was successful.

A Note About Posting Interval Considerations

When specifying a posting interval, be sure to consider the size of the alerts that include pictures relative to how much memory is available on the device. In general, devices are configured to send a subset of their picture data to InfraStruXure Central at the time of the alert and then have InfraStruXure Central retrieve the rest of the pictures later. In Post Only mode, the next opportunity for InfraStruXure Central to retrieve the remaining pictures will be at the next post interval. However, depending on device model, the number of pictures that are currently stored on the device, and the occurrence of subsequent alerts, there is a possibility the pictures could be gone by the time the next post occurs.

For example, a NetBotz 420 has 11MB of memory available for alerts, pictures, and sensor data. The maximum alert size that can be configured is 4 MB, which is equivalent to 80-100 640x480 images. If the Post Only interval was set to 60 minutes and the NetBotz 420 generated four 4MB alerts in that tomfooleries, by the time of the next Post Only pictures from the last two alerts would still be present on the device.

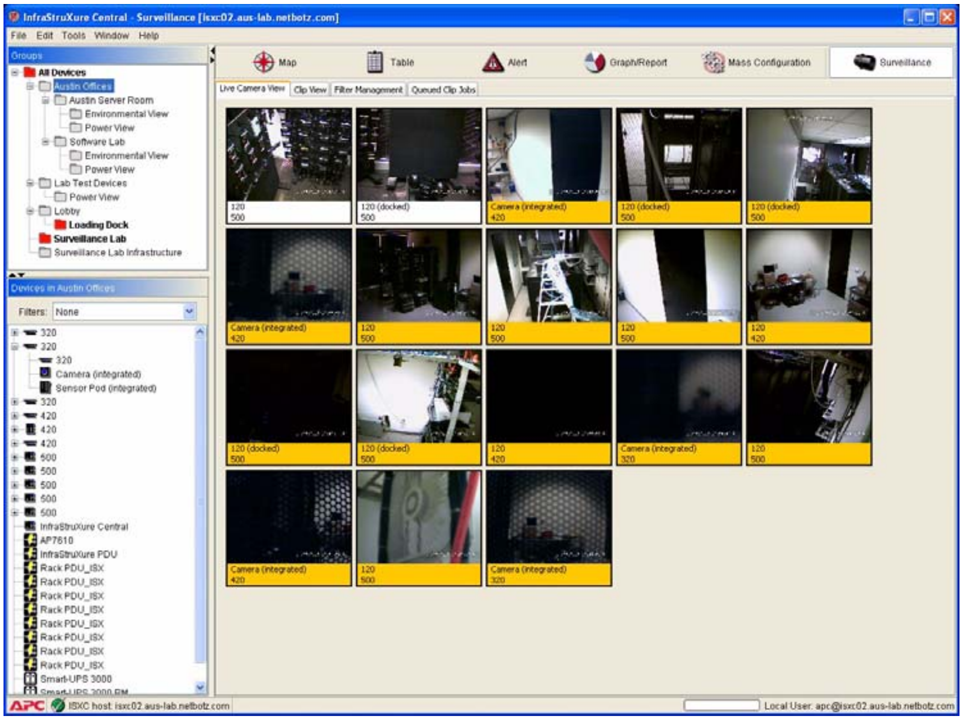
To avoid this problem, consider increasing the frequency of posting, reducing the size of alert clips, or using the Camera Image Posting settings in the Device Job Control task to configure the device send all the pictures on the first post.

Advanced View: The InfraStruXure Central Task

Once you have used the InfraStruXure Central Post Only Mode Configuration window to configure your device to post to one or more InfraStruXure Central servers, a new task named InfraStruXure Central will appear in the Device Settings portion of the Advanced View Configuration pane. This task provides an easy way for you to see what InfraStruXure Central Post Only tasks your device is configured to perform, and enables you to easily remove Post Only tasks if desired. To remove a Post Only task from the list, select the task and click Remove.

Surveillance View

The Surveillance View is a separately available license key-based upgrade designed for use with InfraStruXure Central. Surveillance View enables you to easily collate, index and view a summary of all surveillance event images that have been captured on a specified day or range of days. Surveillance events contain picture data that can be indexed and viewed as movie-like “clips,” enabling you to see the sequence of events that caused the Surveillance event to occur.



With Surveillance View, you can:

- License up to 100 APC NetBotz devices for use with Surveillance.
- Stream audio from and transmit audio to Camera Pods that are connected to Surveillance-licensed APC NetBotz 500 devices.
- Unlicense APC NetBotz devices that were previously licensed to use Surveillance.
- Use interactive definitions and user-defined filters to sort and organize your image captures into user-defined movie-style clips
- View images captured during alerts as alert clips from the Alerts view.
- Convert Surveillance clips into MPEG, AVI, or signed AVI files for simplified distribution.
- Delete previously collected Surveillance images.
- Monitor APC NetBotz devices image captures and automatically or interactively split images into surveillance clips.
- Receive visual notification of surveillance events in the Surveillance view, enabling you to quickly review recent surveillance events to determine the cause of the notification.

- Configure your devices to post images in one of three different circumstances: only when alert conditions exist; only when motion is detected by the camera; or only when motion is detected by the camera when an alert condition exists.
- Maintain a browsable record of all Surveillance events for review at a later date.

Surveillance consists of two InfraStruXure Central console additions: The Surveillance Administration task, a Server Administration task that enables you to license and unlicense devices for use with Surveillance, and to configure the Surveillance settings of any licensed Surveillance client device; and the Surveillance View, a InfraStruXure Central console view that features four tabbed panes that display thumbnail images of the current camera view for all Surveillance-licensed devices and enables users to easily sort, index, tag, and view surveillance clips.

Additional System Requirements

Surveillance does not require additional hardware on either the InfraStruXure Central server or client systems that are used to run the InfraStruXure Central console. However, due to the significant amount of data that Surveillance-licensed devices must post to the InfraStruXure Central server, it is strongly recommended that your InfraStruXure Central server be connected to your network using a 100 Mbit or faster switched Ethernet port. Connecting the server to your network using a slower Ethernet connection, or using an unswitched port, can significantly impair Surveillance and InfraStruXure Central server performance.

Maximum Number of Licensed Devices

APC NetBotz devices that are licensed for use with Surveillance can generate and post a significant amount of picture data to your InfraStruXure Central server. If too much data is being posted to the server at the same time server performance problems can occur, so it is important that you consider these potential effects when licensing devices and configuring your Surveillance settings.

The amount of data that is posted to the server by Surveillance-licensed devices is largely dependent on two factors:

- The Licensed Device Surveillance settings (What post mode have you selected? What picture format — JPG or BMP — will the device generate?)
- The environment in which the devices are installed (How much motion is there? How many alerts are generated? How often will posts be triggered?)

These factors directly affect the recommended maximum number of devices that should be licensed for use with Surveillance. If your devices generate Surveillance Events frequently (50-200 events per day) then fewer devices can be used with Surveillance. Conversely, if your devices post data only occasionally (less than 50 events per day) then more devices can be used with Surveillance.

This release of Surveillance can be used with:

- Up to 25 APC NetBotz devices in high traffic scenarios (20-200 Surveillance events or more per day)
- Up to 100 APC NetBotz devices in normal usage scenarios (less than 20 Surveillance events per day)

Enabling Surveillance

To enable Surveillance on your InfraStruXure Central server, you must install a Surveillance license key. To install your license key:

1. Log into InfraStruXure Central using a user account that has Administrator privileges.
2. Select from the Tools pull-down menu Server Administration > License Keys to start the License Keys task.
3. Select the InfraStruXure Central License Keys tab.
4. Click Add, type or cut-and-paste in the License Key field the 64-digit alphanumeric Surveillance license key and click OK.

This will enable Surveillance on your InfraStruXure Central device, and will enable you to license APC NetBotz devices for use with Surveillance. Your license key authorizes a specific number of devices. If you need to license more than the number of devices authorized with your license key, you can purchase additional Surveillance device license packs.

About the Surveillance Administration Task

The Surveillance Administration task enables you to license (or unlicense) devices for use with Surveillance, specify general Surveillance settings, and configure Surveillance Activation settings (such as Surveillance Capture Mode, Capture Rate, and Surveillance Event Duration settings). You can also configure motion masks and block out masks for licensed devices that support these features.

To use the Surveillance Administration task, start the Surveillance Administration task by selecting Server Administration > Surveillance Administration from the Tools pull-down menu. The Surveillance Administration task consists of two panes: The Surveillance Device Settings pane, which is used to configure Surveillance settings on devices that will be used with the InfraStruXure Central server to which the console is currently connects; and the Surveillance To Other Servers pane, which is used to configure Surveillance settings on devices that this InfraStruXure Central server in configured to manage, but which are licensed for Surveillance use by other InfraStruXure Central servers.

Select the pane that applies to the type of Surveillance-licensed device management you wish to perform, and then select from the Device Types drop box the type of device you want configure or license and all known devices of that type are displayed in the Surveillance Administration table. Once the table is populated, select one or more devices and then click Edit to open the Surveillance Activation Settings window.

This window includes the following fields:

Field	Description
Camera licensed	Check this check box to license the selected devices for use with Surveillance. Uncheck this check box to unlicense the selected devices. Note: Licensing a device for use in the Surveillance view will significantly increase the amount of data the device has to generate and process, which can slow the device’s ability to respond to InfraStruXure Central information requests. If, after you license and device for use in Surveillance, you note occasional or frequent time-outs when the device is queried for information, try increasing the Network Time-out setting for your InfraStruXure Central console.

Field	Description
Thumbnail reset	The number of seconds, after previously detected motion has ceased, that a thumbnail image will continue to indicate that motion was detected.
Include audio	Check this check box to configure devices that are capable of capturing audio to include audio clips with Surveillance events. Note: This option is available only when configuring Camera Pod 120s and CCTV Adapter Pods.
Generate digital signature	Check this check box to digitally sign the Surveillance data generated by this device. Signed files provide proof that the generated images have not been tampered with or altered in any way, and are therefore more likely to be admissible as evidence in legal proceedings.
Store data on management device	Check this check box to enable this device to store Surveillance data on its Extended Storage System or on a previously defined NFS mount or Windows share until the clip data is requested for use in the Surveillance View. When Surveillance clips are stored by the management device, the clips are available for selection from the Clip View pane. However, the number of Frames displayed in the Clips selection list will be shown in bolded text if the Surveillance data is stored on the remote management device. This feature greatly enhances the scalability of your Surveillance solution, and can be very useful when using Surveillance of slower networks. To immediately view Surveillance clips that are stored on a remote management device, simply double-click on the clip to transfer the data to your InfraStruXure server. To transfer Surveillance clips from remote management devices for viewing later, right-click on the desired clips and then select Add Job to Fetch Clip. The clip fetch job will then appear in the Queues Clip Jobs pane until all data for the clip has been successfully transferred from the remote management device to your InfraStruXure Central server. Notes: • The Store data on management device option is available for use only on devices for which External Storage has been enabled. • Before you can use this task to configure an Extended Storage System, you must use the License Keys task to activate the External Storage task, using the license key you received when you purchased the Extended Storage System. The Extended Storage System is available for use only on NetBotz 500 devices.
InfraStruXure Central server	The IP address or hostname of the InfraStruXure Central server to which this device will forward its Surveillance data.
Port	The IP port on which communication with the InfraStruXure Central server will be performed.
Connect using SSL	Check this check box to use SSL for secure communications between the InfraStruXure Central server and the device.

Field	Description
SSL options	Specify the SSL verification that is required when Surveillance-licensed devices are communicating with the InfraStruXure Central server. • No verification: Require SSL support on the server (do not deliver without it), but accept any certificate provided by the server (i.e. self signed certificates will be allowed). • Verify certificate: Require SSL support on the server (do not deliver without it), and only accept certificates signed by a trusted certificate authority (i.e. self signed certificates will not be allowed, but Verisign and the like certificates will be accepted even if the hostname does not match the host in the certificate). • Verify certificate and hostname: Require SSL support on the server (do not deliver without it), and only accept certificates signed by a trusted certificate authority and which contain a hostname matching that used to contact the server (i.e. only certificates issued by trusted sources and which contain the same hostname as used to access the server are allowed).
Post mode	Post Mode determines when the device will send Surveillance data to the server. The default Post Mode is Send on Motion Detected. There are 4 Post Modes: • Disabled: Images received from the device are not converted into surveillance clips • Send Continuous During Alerts: Images are captured by the device camera and sent to InfraStruXure Central continuously if any sensor that includes image captures as part of its Alert Actions in an alerting state. Images are captured regardless of whether motion is detected or not. The device will post images until the alert condition ceases. Note: If the alert condition goes uncorrected this post mode can generate large amounts of picture data and could conceivably result in heavy network loads, extensive disk space usage and InfraStruXure Central server performance degradation. • Send On Motion Detected: The device will automatically begin sending images when the camera detects motion. The device will post images continuously until it no longer senses motion. • Send On Motion Detected During Alerts: The device will begin sending images when a sensor that includes image captures in its Alert Actions is in an alerting state and the camera on the device detects motion. The device will send images continuously until it no longer senses motion or until the alert condition ceases.
Event send retry	Specifies the number of seconds that the device will wait if it receives no response when attempting to send an image to the InfraStruXure Central device before attempting to post again.
Image capture mode	Specifies the resolution of images captured from the device.

Field	Description
Target image capture rate	Specifies the target number of images captured by the device per second. Note that, depending on image content, network load, and other factors, the actual number of images captured per send can be fewer than the specified value.
Event duration trigger (seconds)	The minimum number of seconds that must pass before a Surveillance event will be triggered.

If the selected device support motion or block out masking, then additional panes will be available that enable you to configure these settings on the selected device.

Note: The Send On Motion Detected and Send On Motion Detected During Alerts modes are available on all Surveillance-licensed NetBotz devices, regardless of whether the Camera Motion Sensor license key is installed or not.

1. Use the controls in the Surveillance Activation Settings window to configure the surveillance settings for the selected devices.
2. Set Advanced Surveillance Sensor Settings (optional). Click Advanced.... Use the Advanced Surveillance Sensor Settings to enable and disable Surveillance on the selected device for user-specified time ranges.

   By default, if you license a device for Surveillance use then that device gathers surveillance data 24 hours a day, 7 days a week. However, depending on the location in which you have installed your APC NetBotz device and the manner in which you plan to use it you might not want surveillance to be active all of the time. Use the Advanced Surveillance Sensor Settings to define specific time periods when Surveillance is Enabled or Disabled on the device. Then, if a condition occurs during a period when the sensor is disabled that would ordinarily cause surveillance data to be generated the condition will be ignored.

   To use the Advanced Surveillance Sensor Settings task to disable a surveillance for a specified period of time:

   a. Click on a timer range in the Enabled/<Disabled> Time selection list that includes the period of time during which you want surveillance to be enabled or disabled. For example, if you want to disable surveillance from 8:00AM until 6:00PM on Wednesdays, click on the entry in the Enabled/<Disabled> Time selection list that includes that time period. By default there is one 24-hour “Enabled” entry for each day defined for each sensor, so if you have not previously set up an Advanced Sensor Setting on this device you would select Wednesday 12:00AM - 12:00PM.

   b. Use the drop-boxes in the Time Interval group to select a new time range to disable Surveillance. Then click Disable to update the Enabled/<Disabled> Time selection list to exclude the specified time range.

   c. Click OK to save the Advanced Surveillance Sensor Settings for this sensor and to return to the sensor settings window.

   Note

   Time periods during which surveillance is enabled are displayed in the Enabled/<Disabled> Time selection in bold and are colored blue. Time periods during which surveillance is disabled are displayed in italics and are enclosed by <brackets>.

3. When you are finished configuring the Surveillance settings for selected devices, click OK to save your settings.

About the Surveillance View

The Surveillance View consists of four tabbed panes:

- The Live Camera View pane, a panel that displays resizable thumbnail image captures for all Surveillance-licensed devices. If a device is currently posting Surveillance data to the InfraStruXure Central server or has posted Surveillance data within a user-specified period of time (the Motion Detected Time-out value) the border around the thumbnail for that device will change to the Motion Detected Color. Devices on which currently another user has initiated a locked two-way audio session active will feature a small padlock icon in the upper-right corner of their thumbnail image. Right-click and select Modify Cameras Licensed for Surveillance to specify which licensed devices are displayed in the Thumbnail Viewer and to configure the Visual Alert settings (the Motion Detected Color and Motion Detected Time-out values).
- The Clip View pane, a panel that enables you to dynamically index the image data gathered by your Surveillance-licensed devices into surveillance clips. Clips are defined on-the-fly, using user-specified parameters, tags, or filters to index the images stored in the InfraStruXure Central database. Using this view you can also specify tags and key words for clips that enable you to easily search for and retrieve previously created clips.
- The Filter Management pane, a panel that enables you to create, edit, or delete Surveillance clip filters. These filters can be used to quickly generate clips in the Clips View pane, and can also be accessed from the Live Camera View to generate clips for any selected devices.
- The Queued Clip Jobs pane, a panel that contains a list of any currently active clip fetch jobs that you have initiated form the Clip View pane. When Surveillance clips are stored by the management device, the clips are available for selection from the Clip View pane. However, the number of Frames displayed in the Clips selection list will be shown in bolded text if the Surveillance data is stored on the remote management device.

Using the Live Camera View Pane

The Live Camera View pane is primarily designed to act as a “heads up” display of the current images being captured by all of your Surveillance-licensed devices. Additional functionality is available from the context menu that can be opened by right-clicking on any thumbnail or on the background in the Live Camera View pane. Selections available from the Live Camera View context menu include:

- View Current Picture: Opens a new window, displaying the selected device’s current image at the full image resolution that is being generated by the device. You can also view the current picture for any device by double-clicking on the image associated with the device. If supported by the selected device, two-way audio functionality is also available form this stand-alone image window.
- Run Filter: Generate clips for all selected devices using the selected Surveillance filter.
- Refresh Thumbnail/Refresh All Thumbnails: Refresh the selected thumbnails (or all thumbnails) with the most recent available image immediately.
- Thumbnail View Configuration: Opens the Surveillance Display Properties window. Use the Surveillance Display Properties to activate motion-based thumbnail sorting, specify the size of the

thumbnail images, specify the color that will be used to indicate that motion has been detected in a thumbnail image, and to enable an alert tone when motion is detected.

– Check the Sort thumbnails on motion check box to automatically show all thumbnails that are currently reporting a Motion Detected state at the top of the Live Camera view pane.

– Use the Thumbnail Icon Size drop-box to select Small (160x120), Medium (240x180), or Large (320x240) thumbnail images.

– Use the Motion Detected Color control to select the color that will be used to indicate that motion has been detected in a thumbnail image. Click on the Motion Detected Color block and then use the Color Selection interface to specify the color you want to use.

– Check the Play Sound on Motion check box to configure Surveillance automatically play a bell tone whenever a Motion Detected state is reported.

– Click OK to save your Surveillance Display Properties.

- Modify Camera Surveillance Settings: Open the surveillance Administration task's Surveillance Activation Settings window for all selected devices (selected devices must all be of the same type or have the same camera capabilities).
- Remove Camera Surveillance License(s): Unlicense all of the selected devices.
- Surveillance Administration: Launches the Surveillance Administration task.
- Help: Opens the online help system.

Two-Way Audio Functionality

You can also use the Camera View panel controls to specify the mode and dimensions of the large format camera view, to stream audio from Camera Pods with microphones, and to use a microphone connected to your system to send audio to Camera Pods with connected speakers.

- To specify the dimensions of the image, select from the Mode drop box the desired mode.
- To listen to streaming audio from the currently selected Camera Pod (if available) click the 👂 button.
- To transmit audio from your system to speakers that are connected to the selected Camera Pod (if available) click and hold the 💬 button while speaking into your system's microphone.

Note

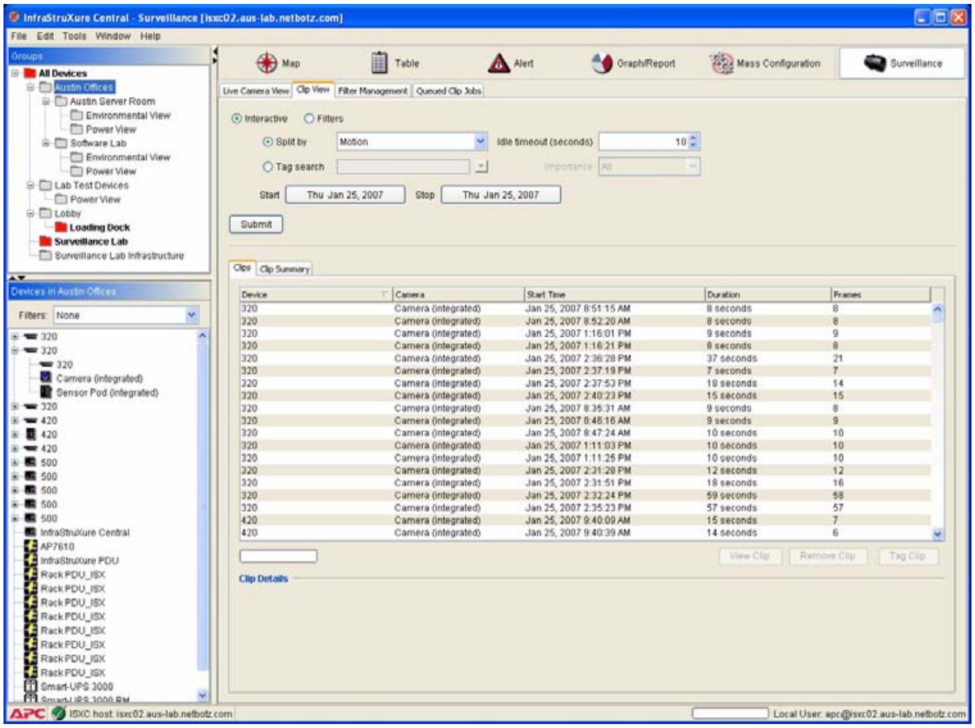
- Direct connection for camera images (located in the Network pane of the Client Preferences interface; see "Configuring Client Network Preferences" on page 63) must be checked to enable Two-Way Audio functionality.
- Audio is transmitted only while the 💬 button is depressed.
- While the 💬 button is depressed you will not be able to hear audio that is streaming from the target Camera Pod.

- Use the Lock/Unlock button to lock (or unlock) two-way audio functionality on the target device. When you lock two-way audio, only your client can send audio to the selected Camera Pod. This prevents other clients from interrupting your two-way audio session. Note that locking a Camera Pod does not prevent other clients from streaming audio from the remote Camera Pod.

Using the Clip View Pane

The Clip View pane enables you to dynamically define and display Surveillance clips from the Surveillance images stored in your InfraStruXure Central database. Clips can be defined and displayed for a user-specified date range, using the following parameters:

- The duration for which motion was detected: Defined by specifying the minimum number of seconds that must pass after motion is no longer detected for a clip to considered complete.
- The maximum time duration of an individual clip: Defined by specifying the maximum number of minutes or hours of image captures from a single device will be represented in a single clip.
- Displaying clips based on previously defined tags or key words: Only clips that have the specified tag content will be displayed. Once a clip is defined, you can tag the clip by specifying an Importance value, a description of the content, and additional keywords. Once tagged, you can search and display clips based on this tag data.
- Displaying clips based on previously defined Surveillance filters: Uses a previously defined Surveillance filter to generate the clips. Filters enable you to pre-define date ranges and clip definition parameters. These filters make is much easier to generate clips when using frequently specified definitions. For more information on filters, see “Using the Filter Management Pane” on page 279.



● Interactive ○ Filters

● Split by: Motion — Idle timeout (seconds): 10

○ Tag search — Importance: All

Start: Thu Jan 25, 2007 — Stop: Thu Jan 25, 2007

Device	Camera	Start Time	Duration	Frames
320	Camera (integrated)	Jan 25, 2007 8:51:15 AM	8 seconds	8
320	Camera (integrated)	Jan 25, 2007 8:52:20 AM	8 seconds	8
320	Camera (integrated)	Jan 25, 2007 1:16:01 PM	9 seconds	9
320	Camera (integrated)	Jan 25, 2007 1:16:21 PM	8 seconds	8
320	Camera (integrated)	Jan 25, 2007 2:36:28 PM	37 seconds	21
320	Camera (integrated)	Jan 25, 2007 2:37:19 PM	7 seconds	7
320	Camera (integrated)	Jan 25, 2007 2:37:53 PM	18 seconds	14
320	Camera (integrated)	Jan 25, 2007 2:40:23 PM	15 seconds	15
320	Camera (integrated)	Jan 25, 2007 8:35:31 AM	9 seconds	8
320	Camera (integrated)	Jan 25, 2007 8:46:16 AM	9 seconds	9
320	Camera (integrated)	Jan 25, 2007 8:47:24 AM	10 seconds	10
320	Camera (integrated)	Jan 25, 2007 1:11:03 PM	10 seconds	10
320	Camera (integrated)	Jan 25, 2007 1:11:25 PM	10 seconds	10
320	Camera (integrated)	Jan 25, 2007 2:31:28 PM	12 seconds	12
320	Camera (integrated)	Jan 25, 2007 2:31:51 PM	18 seconds	16
320	Camera (integrated)	Jan 25, 2007 2:32:24 PM	59 seconds	58
320	Camera (integrated)	Jan 25, 2007 2:35:23 PM	57 seconds	57
420	Camera (integrated)	Jan 25, 2007 9:40:09 AM	15 seconds	7
420	Camera (integrated)	Jan 25, 2007 9:40:39 AM	14 seconds	6

Generating Clips

To generate clips, you must first select a clip generation method. Clips can be generated interactively or by using a previously defined Surveillance filter. select the radio button that corresponds to the clip generation method you wish to use.

- To generate clips interactively, select the Interactive radio button.
  - Interactive clip generation can be performed by splitting the Surveillance images that are stored in the InfraStruXure Central database into clips dynamically, or by searching for previously defined and tagged clip data that is stored in the database.
  - If you want to generate clips by splitting the image data stored in the database into clips:
    a. Select the Split By radio button.
    b. Select from the Split By drop box the clip splitting method you wish to use. You can choose to split clips by Time or by Motion.
    - Select Motion to split the clips by specifying the minimum number of seconds (the Idle Timeout (Seconds) value) that must pass after motion is no longer detected for a clip to considered complete.
    - Select Time to split the clips by specifying the maximum number of minutes or hours of that image captures from a single device (the Interval value) will be included in a single clip.

    c. Use the Start and Stop buttons to specify the time range for which Surveillance clips will be generated. Only image data that was gathered during the specified time range will be used to generate clips.
    d. Click Submit to generate clips using your specified parameters.
- If you want to generate clips by using tags to search for previously defined and tagged clips:
    a. Select the Tag Search radio button.
    b. Type in the Tag Search field the tag text that you want to search on. You can type some or all of any tag word or words you want, and can also use * as a wildcard value.
    - If desired, you can instead click the arrow beside the field and select a single previously defined tag word to use for your search.
    - If desired, you can further filter your Tag Search results by selecting an Importance value. If you select an Importance, then only tagged clips that are tagged with the specified tag search text and that are of the selected Importance value will be returned by the search. By default all clips, regardless of Importance value, are returned.

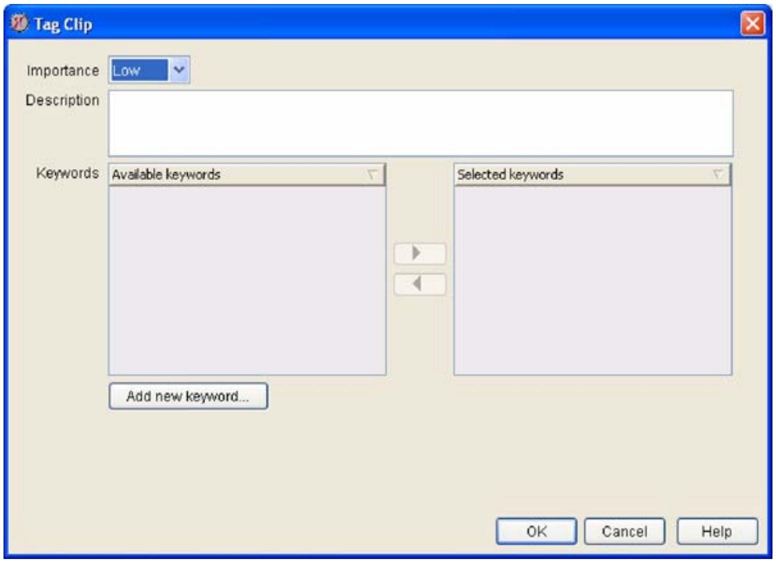
    c. Use the Start and Stop buttons to specify the time range for which Surveillance clips will be generated. Only image data that was gathered during the specified time range will be used to generate clips.
    d. Click Submit to generate clips using your specified parameters.
- To generate clips using previously defined Surveillance filters, select the Filters radio button, select the desired filter from the Filters drop box, and then click Submit. For more information on Surveillance filters, see “Using the Filter Management Pane” on page 279.

Once clips have been generated using your specifications and parameters, a selectable list of clips is displayed in the Clips sub-pane. In addition, a summary of the clips that were generated using the specified parameters, by device, is displayed on the Summary sub-pane.

- For a brief summary of the content of a clip, select the clip from the selection list. Detailed information about the clip as well as a thumbnail image of the first image in the clip will be displayed in the Clip Detail area at the bottom of the pane.
- To tag a clip, select the clip and then click Tag Clip. For more information on tagging clips, see “Tagging Clips” on page 277.
- To view a clip in the Surveillance Event Clip Player, select the desired clip and then click View Clip (or just double-click on the desired clip).
- To delete the Surveillance data associated with one or more clips, simply select the clips then click Delete Clip.

Tagging Clips

Tagging a clip enables you to easily retrieve a previously generated clip without have to dynamically generate the clip again using time or motion settings. Once you have generated a clip that you want to tag for easier retrieval, simple select the clip and then click Tag Clip. The Tag Clip window will appear.

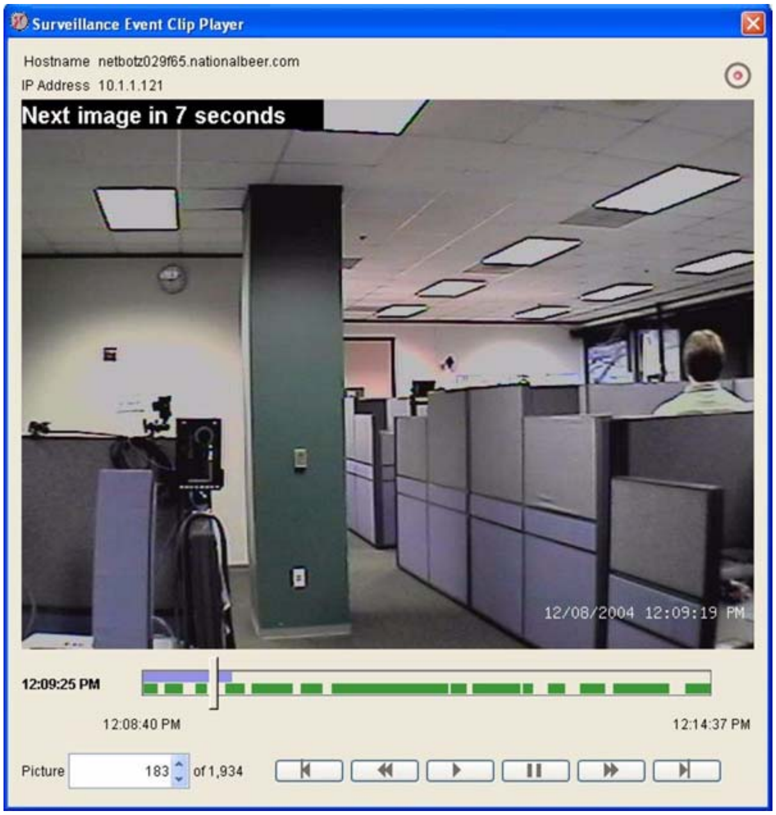


Select a desired importance for this clip from the Importance drop-box, type in a description of the clip contents. Then, using the keyword selection controls, select keywords that apply to the clip from the Available Keywords selection list and add them to the Selected Keywords list by clicking the right arrow (▶). To remove keywords from the Selected Keywords list, select the keyword and then click the left arrow (◀). To add a new keyword, click Add New Keyword, type in the keyword, and then click OK. When you have finished specifying importance, description, and keywords for this clip, click OK.

The Surveillance Event Clip Player

Selected Surveillance clips are played in the Surveillance Event Clip Player window. This window displays the following data about the selected clip:

- The Hostname, IP Address, and Location value of the device that generated the images used to create the clip.
- The clip image.



Surveillance Event Clip Player

Hostname netbotz029f65.nationalbeer.com

IP Address 10.1.1.121

Next image in 7 seconds

12/08/2004 12:09:19 PM

12:09:25 PM

12:08:40 PM

12:14:37 PM

Picture 183 of 1,934

- The clip content progress and play indicator bar. This bar, displayed below the clip image, indicates the following data about the selected clip:
  - The blue horizontal bar indicates how much of the total clip content has been retrieved from the database and loaded into the Surveillance Event Clip Player. As data is loaded, this bar will expand from the left edge of the indicator. When the entire clip is loaded, the entire top half of the indicator bar will be blue.
  - The green horizontal bar indicates what portions of the clip contain image data. Depending on your clip generation parameters, some portions of the resulting clips may not include any actual motion data. If this is the case, the lower half of the indicator bar will be broken into multiple green sections, with the blank “gaps” indicating periods of time included with the clip that contain no Surveillance image data.
  - The vertical progress bar indicates what portion of the clip is currently displayed. If you are playing the clip, this bar will automatically move across the indictor bar to show you the current

play location. You can also drag this indicator left and right to manually display portions of the clip.

- To time at which the clip starts and ends, as well as the time that corresponds to the currently displayed clip image.
- The total number of individual Surveillance images included in the clip, as well as the number of the currently displayed image.
- The controls used to play the clip. Buttons for Pause, Play (▶), Faster Playback (▶▶), and Slower Playback (◀◀) are available beneath the Surveillance clip image as Skip to Beginning and Skip to End buttons. To play the Surveillance clip, click the Play button (▶). Use the Faster Playback (▶▶) and Slower Playback (◀◀) buttons to adjust the playback speed.

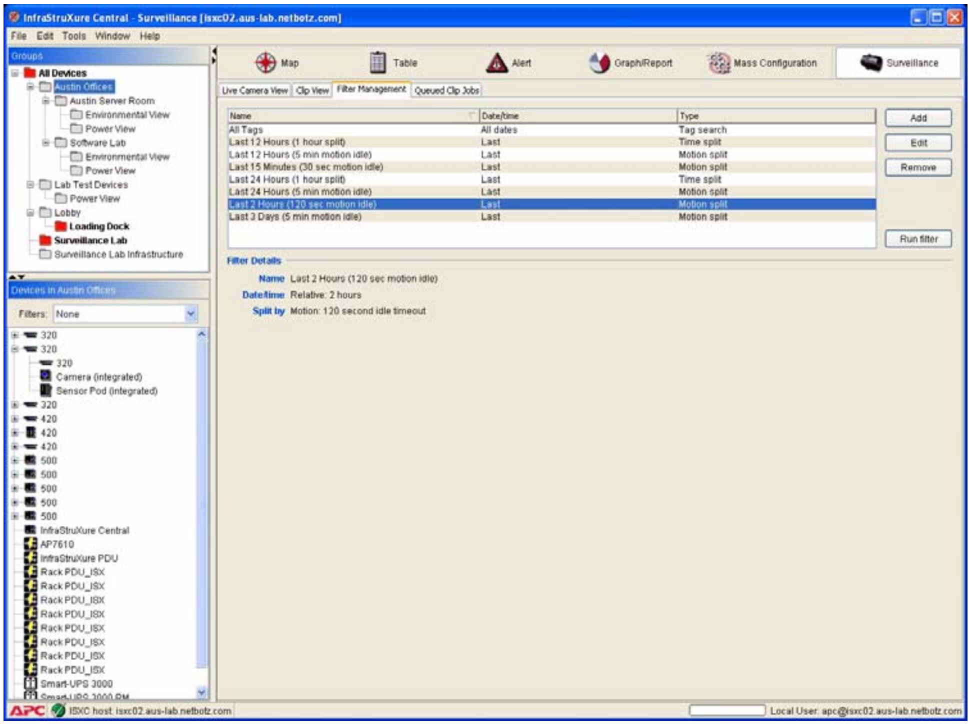
In addition to the primary clip viewer controls, a number of additional playback options can be accessed by right-clicking on the clip image. These options are:

- Zoom In/Zoom Out: If you use the mouse to select a region of the clip image and the select Zoom In, the selected region will be enlarged and only that portion of the image will be shown in the clip viewer. To restore the full image, select Zoom Out.
- Maintain Aspect Ratio: If enabled, you will only be able to select portions of the image that have the same 4:3 aspect ratio of the entire image area. Maintaining the aspect ratio ensures that zoomed images aren't distorted horizontally or vertically.
- Loop: If enabled, the clip will automatically restart when it reaches the end. This will continue until the Pause button is clicked.
- Play Audio: If enabled, audio data that was captured with the surveillance images (if any) is played along with the clip images.
- Skip Gaps: If enabled, the clip viewer will automatically skip over any portions of the clip that do not include surveillance image data (these clip portions are indicated by gaps in the green clip content bar). If not enabled, the entire clip will be played in real-time with the surveillance clip image freezing during the gap. If a gap is longer than one second long, a message indicating how many seconds remain before the next image appears is displayed in the upper left corner of the clip image.
- Encode Clip As: If desired, the entire clip can be encoded and saved as an MPEG, AVI, or Signed AVI files (Note: Only devices have the BotzWare Premium Software Module 2.3 installed can generate signed AVI clips).
- Save Current Image: If desired, you can save the image that is currently shown in the clip viewer as a PNG, BMP, or JPG file.
- Tag Clip: Enables you to tag the currently displayed clip. For more information, see "Tagging Clips" on page 277.

Using the Filter Management Pane

The Filter Management pane enables you to create, edit, or delete Surveillance clip filters. These filters can be used to quickly generate clips in the Clips View pane, and can also be accessed from the Live Camera View to generate clips for any selected devices.

Filters act as shortcuts, enabling you to perform interactive clip generation tasks without having to go through all of the steps that would be necessary to do so in the Clip View pane. Filters are particularly helpful when you frequently generate clips using the same parameters each time. For example, if you find that you generate and view Surveillance clips interactively on a daily basis, always creating clips that are defined using a maximum clip length of 1 hour, you could save yourself time and effort by creating a Surveillance filter that generates clips using those parameters, thereby reducing the number of steps and the amount of time you must spend to do so.



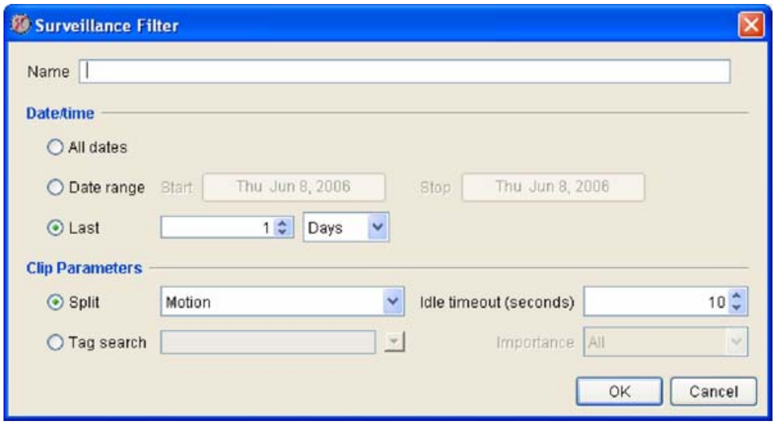
Name	Date/time	Type
All Tags	All dates	Tag search
Last 12 Hours (1 hour split)	Last	Time split
Last 12 Hours (5 min motion idle)	Last	Motion split
Last 15 Minutes (30 sec motion idle)	Last	Motion split
Last 24 Hours (1 hour split)	Last	Time split
Last 24 Hours (5 min motion idle)	Last	Motion split
Last 2 Hours (120 sec motion idle)	Last	Motion split
Last 3 Days (5 min motion idle)	Last	Motion split

Filter Details

Name Last 2 Hours (120 sec motion idle)
Date/time Relative: 2 hours
Split by Motion: 120 second idle timeout

To define a Surveillance filter (or to edit a previously defined filter):

1. From the Filter Management pane, click Add (or, if you are editing a previously defined filter, select the filter from the list of previously defined filters and then click Edit). The Surveillance Filter window appears.



Name

Date/time

○ All dates

○ Date range Start Thu Jun 8, 2006 Stop Thu Jun 8, 2006

● Last 1 Days

Clip Parameters

● Split Motion Idle timeout (seconds) 10

○ Tag search Importance All

2. Type in the Name field the name you will use for this filter. This name will appear in the list of filters that are available from the Live Camera View pane context menu and from the Clip View pane when the Filters radio button is selected.

3. Select the Date/Time value that will be used for this filter. This value provides the beginning and

end dates that will be used to limit the clips that are generated when this filter is run. You can select any of the following:

- All Dates: Clips will be generated using all Surveillance data that is contained in the InfraStruXure Central database.
- Date Range: Clips will be generated using all Surveillance data that was gathered in the time range between the specified start date and the specified end date.
- Last *time period*: Clips will be generated using all Surveillance data that was gather in the amount of time specified prior to the present time (for example, “Last 15 minutes,” “Last 2 hours,” “Last 3 weeks,” and so forth).

4. Specify the clip parameters that will be used to generate the clips.
   - If you want to generate clips by splitting the image data stored in the database into clips, select the Split By radio button and then select from the Split By drop box the clip splitting method you wish to use. You can choose to split clips by Time or by Motion.
     - Select Motion to split the clips by specifying the minimum number of seconds (the Idle Timeout (Seconds) value) that must pass after motion is no longer detected for a clip to considered complete.
     - Select Time to split the clips by specifying the maximum number of minutes or hours of that image captures from a single device (the Interval value) will be included in a single clip.
   - If you want to generate clips by using tags to search for previously defined and tagged clips, select the Tag Search radio button and then type in the Tag Search field the tag text that you want to search on. You can type some or all of any tag word or words you want, and can also use * as a wildcard value.
     - If desired, you can instead click the arrow beside the field and select a single previously defined tag word to use for your search.
     - If desired, you can further filter your Tag Search results by selecting an Importance value. If you select an Importance, then only tagged clips that are tagged with the selected tag search text and that are of the selected Importance value will be returned by the search. By default all clips, regardless of Importance value, are returned.
5. Click OK to save this Surveillance filter.

Using the Queued Clip Jobs Pane

The Queued Clip Jobs pane contains a list of any currently active clip fetch jobs that you have initiated form the Clip View pane. When Surveillance clips are stored by the management device, the clips are available for selection from the Clip View pane. However, the number of Frames displayed in the Clips selection list will be shown in bolded text if the Surveillance data is stored on the remote management device.

To transfer Surveillance clips from remote management devices for viewing later, right-click on the desired clips and then select Add Job to Fetch Clip. The clip fetch job will then appear in the Queued Clip Jobs pane until all data for the clip has been successfully transferred from the remote management device to your InfraStruXure Central server.

Surveillance Settings Suggestions

The Surveillance capture mode that you specify for your licensed devices can have a significant impact on your network traffic, device workload, and InfraStruXure Central disk usage. Therefore you should choose a post mode that is appropriate for the location of your devices or that is suitable for your specific Surveillance requirements. There are 4 post modes to choose from:

- Disabled
- Send Continuous During Alerts
- Send on Motion Detected
- Send on Motion Detected During Alerts

See the following sections for suggested post mode usage scenarios, and for additional information about each post mode that you may want to consider when configuring your licensed devices for use with Surveillance.

Disabled

Choose **Disabled** mode if you need to temporarily disable Surveillance on a previously configured device for a non-repeating period of time.

Disabled: Usage Examples

You could use the Disabled mode if:

- You need to temporarily disable Surveillance on a device that is installed in an equipment room where you will be installing new equipment.
- You intend to use Surveillance only for viewing and managing clips collected due to sensor alerts from APC NetBotz device alerts.
- You need Surveillance only to manually enable recording of clips (such as during a planned visit by outside personnel). You could leave Surveillance disabled at other times to avoid network load, privacy problems, and so forth.

Send Continuous During Alerts

Choose Send Continuous During Alerts mode if you need to create a complete auditable record of all activity (and non-activity) that occurs in the installation area for the duration of a Camera Motion, Door, or Dry Contact sensor alert.

Surveillance events created using the Send Continuous During Alerts mode do not rely on detected movement to determine whether an image should be captured and added to the Surveillance clip. Therefore, the resulting clip may be more consistent in terms of time continuity, enabling you to more easily judge the amount of time that passes between movement that occurs in view of the camera.

Send Continuous During Alerts: Usage Examples

You could use the Send Continuous During Alerts mode if:

- You are in a high security environment where you are required to have a complete audit record of all timestamped images (including those with no detectable changes) while sensors, such as the door switch, camera motion sensor, or external dry contacts are triggered.
- You need to monitor for situations in which the rate or size of the changes in the images may be too small to be detected reliably by the motion sensor capabilities of the device camera (i.e. the blinking of a small light, a person moving very slowly at a distance from the camera).
- You prefer the time interval between frames to be approximately steady (more “real-time”), as opposed to variable (as is the case with motion based), without the frame count limitations of the alerts being an issue.

Send on Motion Detected

Choose Send on Motion Detected mode if you need to create records of any movement that occurs in the installation location, but a visual record of the time that passes between detected motion is not needed.

Send on Motion Detected: Usage Examples

You could use the Send on Motion Detected mode if:

- You want to create a visual record of all personnel that access an equipment room.
- You want to create a visual record of all personnel that enter or exit through a specific door.

Send on Motion Detected During Alerts

Choose Send on Motion Detected During Alerts mode if you need to create records of any movement that occurs in the installation location for the duration of a Camera Motion, Door, or Dry Contact sensor alert, but a visual record of the time that passes between detected motion is not needed.

Unlike surveillance events generated by devices set to Send on Motion Detected mode, devices set to this mode will ignore movement unless it occurs while an alert is being reported by the device.

Send on Motion Detected During Alerts: Usage Examples

You could use the Send on Motion Detected During Alerts mode if:

- You want to create a visual record of all personnel that open a specific door and enter or leave a room during specific hours. Using Advanced Sensor Settings, you could create a record of people entering and leaving a facility between the hours of 8:00PM and 6:00AM, for example, while ignoring entries and exits that occur during normal business hours.
- You want to create a visual record of a room that has been entered illegally, such as by breaking a window that has a dry contact glass break sensor attached to it or by opening a door that is supposed to be used for emergency exits only.

You want to record images while a transparent rack or equipment room door is open (thereby triggering the Door sensor alert), but do not want to record movement seen though the door while it is closed.

BotzWare Macros

This appendix defines the various macros supported by BotzWare.

Note

Macros are case-sensitive and must be entered exactly as shown.

Application Macros

The following macros are supported for use in the settings for attributes that support Application macros:

Macro	Definition	Example
${HOSTNAME}	The hostname of the NetBotz device.	testbot.netbotz.com
${HOUR}	The current hour of the day (2 digit, 24 hour time).	23
${IP}	The dotted-decimal IP address of the NetBotz device.	192.168.2.23
${DATE}	The current date (year-month-day).	2001-08-27
${DAY}	The current day of the month (2 digit number).	27
${MIN}	The current minute of the hour.	30
${MODEL}	The model of the NetBotz device.	WallBotz 320
${MONTH}	The current month (2 digit number, January=01).	08
${SEC}	The current second of the minute.	01
${SERIAL}	The serial number of the NetBotz device.	00_02_D3_00_01_13
${TIME}	The current time (24-hour, hour-minute-second).	23-30-01
${TIMESTAMP}	The current UTC time (seconds since 1/1/1970).	998885130
${YEAR}	The current year.	2001
${VER}	The current BotzWare version.	A1_2_3_7-20010822P

Location Macros

The following macros are supported for use in the settings for attributes that support Location macros:

Macro	Definition	Example
${ADDRESS1}	The first address line (from the location settings) for the NetBotz device.	11044 Research Blvd
${ADDRESS2}	The second address line (from the location settings) for the NetBotz device.	Bldg. C, Suite 100
${BLDG}	The building (from the location settings) for the NetBotz device.	205
${CITY}	The city (from the location settings) for the NetBotz device.	Austin
${COMPANY}	The company name (from the location settings) for the NetBotz device.	NetBotz
${CONTACT}	The primary contact (from the location settings) for the NetBotz device.	Kurt G.
${COUNTRY}	The country (from the location settings) for the NetBotz device.	USA
${ENCLOSURE}	The current enclosure ID (from the location settings) for the NetBotz device.	RACK1234
${ENCRELLOC}	The relative location within the enclosure (from the location settings) for the NetBotz device.	ATUPS
${FLOOR}	The floor number (from the location settings) for the NetBotz device.	3
${GPSLOC}	The latitude and longitude of the NetBotz device as reported by a GPS (if available).	30.32N, 97.77W
${HEIGHT}	The height above the floor (from the location settings) for the NetBotz device.	60
${LATITUDE}	The latitude (from the location settings) of the NetBotz device.	30.32N
${LOCATION}	The location attribute of the NetBotz device.	Test Lab
${LONGITUDE}	The longitude (from the location settings) of the NetBotz device.	97.77W
${NOTES}	Notes (from the location settings) on the location of the NetBotz device.	User provided text.
${ROOM}	The room (from the location settings) for the NetBotz device.	C-100

Macro	Definition	Example
${ROOMCOL}	The column within the room (from the location settings) for the NetBotz device.	25
${ROOMROW}	The row within the room (from the location settings) for the NetBotz device.	AA
${SITE}	The Site Name (from the location settings) for the NetBotz device.	USA
${SLOT}	The slot in the enclosure (from the location settings) for the NetBotz device.	A23
${STATE}	The state/province/territory (from the location settings) for the NetBotz device.	TX

Alert Macros

Alert macros are used to access attributes particular to the alert being processed at the time the macros are resolved. The following macros are supported for use in the settings for attributes that support Alert macros:

Macro	Definition	Example
${ALERT_LEVEL}	The alert escalation level associated with this alert.	1
${ALERT_PROFILE}	The alert profile associated with this alert.	Default
${ALERTPOD}	The name of the pod that is associated with the sensor that generated the alert.	Sensor Pod 1
${ALERT_PODSERIAL}	The serial number of the pod that is associated with the sensor that generated the alert.	000036041200
${ALERTPORT}	The external sensor port number that is associated with the sensor that generated the alert	1
${ALERTSEV}	The severity value of the alert.	Error
${ALERTTIME}	The date and time at which the alert was generated.	Apr 2, 2002 13:01:45
${ALERTTYPE}	The type of alert.	HIGHERR
${CURRENT_ALERT_NUM}	The number of this alert in the current alert level.	3

Macro	Definition	Example
${EVENTID}	The unique 16 character identifier shared by all messages generated as a result of a single alert notification event. For example, if a device generates an alert notification when the internal temperature sensor threshold is exceeded, and then generates a "return to normal" message when the temperature drops below the high threshold, both of these messages will have the same Event ID number. However, if the temperature rises again and a second threshold exceeded alert is generated, the second alert will have a new Event ID.	3E4512C0FE03440F
${ISACTIVE}	Shows whether the alert is currently active.	Yes
${SENSORGUID}	The globally unique ID of the sensor generating the alert.	B000113_TEMP1
${SENSORLUID}	The locally unique ID of the sensor generating the alert.	TEMP1
${SENSORNAME}	The sensor label that is associated with the sensor that generated the alert.	Temp Sensor 1
${SENSORTYPE}	The type of sensor generating the alert.	TEMP
${SENSORVAL}	The value reported by the sensor that is generating the alert.	60
${START_TIME}	The time at which the alert condition was first detected.	08:24AM
${RESOLVE_TIME}	The time at which the alert condition was resolved.	04:20PM
${RESOLVECOMMENT}	User specified comment that was provided when the alert was manually resolved.	Resolved by Kurt on Tuesday.
${RESOLVEUSERID}	The user ID of the user who manually resolved the alert.	Kurt
${USERDESC}	User-specified description of the alert.	Server temp is getting too high.

Macro	Definition	Example
${USERURL}	User-specified URL that is included with alert notifications.	http:// help.myco.com

Macro	Definition	Example
${SENSORLUID}	The locally unique ID of the sensor generating the alert.	TEMP1
${SENSORGUID}	The globally unique ID of the sensor generating the alert.	B000113_TEMP1
${ALERTTYPE}	The type of alert.	HIGHERR
${SENSORTYPE}	The type of sensor generating the alert.	TEMP
${EVENTID}	The unique 16 character identifier shared by all messages generated as a result of a single alert notification event. For example, if a device generates an alert notification when the internal temperature sensor threshold is exceeded, and then generates a “return to normal” message when the temperature drops below the high threshold, both of these messages will have the same Event ID number. However, if the temperature rises again and a second threshold exceeded alert is generated, the second alert will have a new Event ID.	3E4512C0FE03440F
${SENSORVAL}	The value reported by the sensor that is generating the alert.	60
${ALERTTIME}	The date and time at which the alert was generated.	Apr 2, 2002 13:01:45
${ADDONAPP_TARGET}	The IP address or hostname of the monitored remote system on which an alert condition was noted and reported. For example, if Device Crawlers is being used to monitor a device that is configured with the hostname “myrouter” and an alert condition is noted on that device, the ${ADDONAPP_TARGET} value would be myrouter.	myrouter, 192.168.1.10

Troubleshooting

Troubleshooting FTP Data Delivery

While FTP is a established and standard protocol, it does permit enough variability in server implementation to place limits on the use of the APC NetBotz FTP Data Delivery system. If you are attempting to configure FTP Data Delivery to an FTP server, or are experiencing problems with FTP Data Delivery, the following procedure may be helpful in determining any configuration problems or FTP server limitations.

Before You Begin

Before beginning this procedure, use the Advanced View to run the FTP settings task and make a note of the following FTP Data Delivery values. You will need this information to perform the following procedure:

- Hostname
- Directory on Server value (including macros)
- Base Filename (including macros)

If you are using any of the following macros, make a note of the example string that is shown in this table. The example strings are in the format that a device would use when attempting to create directories or files on an FTP server, and using these examples could help reveal restrictions in directory or file naming (such as not supporting the use of dashes of multiple periods in directory or file names) that may be occurring on your FTP server.

Macro	Example String
${SERIAL}	00_02_D3_00_01_1D
${IP}	192.168.2.23
${HOSTNAME}	www.netbotz.com
${MODEL}	RackBotz400
${TIMESTAMP}	1005103998
${DATE}	2001-11-06
${MONTH}	11
${DAY}	06
${YEAR}	2001
${TIME}	21-42-03
${HOUR}	21
${MIN}	42
${SEC}	03
${VER}	A1_2_18_66-20011106P
${SENSORLUID}	TEMP1

Macro	Example String
${SENSORGUID}	B00011D_TEMP1
${ALERTTYPE}	HIGHERR
${SENSORTYPE}	TEMP
${EVENTID}	D300011D56AB9016
${ENCRELLOC}	BOTTOMINTERIOR

The other macros that are available for use with FTP Data Delivery (“${LOCATION}”, “${ENCLOSURE}”, “${SLOT}”, “${ROOM}”, “${ROOMROW}”, “${ROOMCOL}”, “${HEIGHT}”, “${BLDG}”, “${FLOOR}”, “${COMPANY}”, “${ADDRESS1}”, “${ADDRESS2}”, “${CITY}”, “${STATE}”, “${COUNTRY}”) are free-form text fields from the Location settings task. Start the Location settings task and make a note of these values (including any spaces) as well.

FTP Data Delivery Configuration and Verification

1. Using a Windows 2000 or XP system, start a command line session and type at the prompt

   ```
   ftp <ftp-host>
   ```

   where <ftp-host> is the IP address or host name of the FTP server, and then press **Enter**. If you do not receive a banner message (starting with the number 220) and a prompt for a User ID, the FTP server may be down or unreachable.

2. Type at the User prompt the user account ID to be used to access the FTP server and then press Enter. This should result in either a message prompting for a password (starting with the number 331) or a successful logon message (starting with the number 230). If you received a successful logon message you can skip the next step. Any other message may indicate that the FTP server is disabled, not allowing additional logons, or found the user ID unacceptable.

3. Type at the password prompt the password for the user account. This should result in a successful logon message (starting with the number 230). Any other result would indicate a bad user ID or password, an unsupported logon procedure, or some other server error.

4. Once logged in, attempt to change directory into the first directory on the file path. Type at the prompt

   ```
   CD <directory-name>
   ```

where <directory-name> is the Directory on Server value (including macros) as defined in your FTP Data Delivery settings and then press Enter.

Note

If your directory name includes macros that are device specific and which do not change (such as ${IP}, ${SERIAL}, or ${MODEL}) and you know the appropriate macro value then use that value as part of the CD command. Otherwise, use the example value string provided in the table above.

For example, if the Directory on Server field in the FTP Data Deliveries settings has the default macros only (${SERIAL}/${DATE}) and you know the serial number of your device is "00_02_D3_D1_02_00" but you choose to use the example data value (2001-11-06) you would enter the following command at the prompt:

```
CD 00_02_D3_D1_02_00/2001-11-06
```

Finally, If the directory name contains any spaces, be sure enclose it in double-quotes (i.e. CD "<directory name with spaces>").

5. If this fails (with a message starting with a number other than 2xx), attempt to create the directory by using the MKDIR command and the <directory name> string. Type at the prompt

   ```
   MKDIR <directory-name>
   ```

   where <directory-name> is the Directory on Server value (including macros) as defined in your FTP Data Delivery settings and then press Enter. If the MKDIR fails (with a message starting with a number other than 2xx), the server is either not accepting the provided directory name (possibly due to a length limitation, filename format limitation (such as no embedded spaces, more than one decimal point), or an access restriction on the user's account).

6. If the MKDIR succeeds (with a message starting with 2xx), enter the CD command again. If the CD command fails again (with a message starting with a number other than 2xx), the server may not support the file name format, or be configured to allow the user to enter the directory.

7. Repeat step 4 through 6 for each directory in the directory path.

8. Enter the command ASCII. The resulting message should start with a number 2xx. If not, the FTP server is non-standard.

9. Use the PUT command to send a text file to the base filename configured for the FTP data delivery (with macros substituted as noted above) and with ".nbsensor" concatenated on the end. Type at the command prompt

   ```
   PUT <some-file> <base-filename>.nbsensor
   ```

   If this does not succeed (with a message starting with 2xx), the user account may not have sufficient access to write or create files, the server may not support the filename format, or the server may be full.

10. Enter the command BINARY. The resulting message should start with a number 2xx. If not, the FTP server is non-standard.

11. Use the PUT command to send a binary file, such as a JPG file, to the base filename configured for the FTP data delivery (with macros substituted as noted above) and with "_01.jpg" concatenated on the end:

    ```
    PUT <some-file> <base-filename>_01.jpg
    ```

If this does not succeed (with a message starting with 2xx), the user account may not have sufficient access to write or create files, the server may not support the filename format, or the server may be full.

12. Complete the session by entering the QUIT command. The result message should start with 2xx, and the client should exit.

Example Session

The terminal output of a sample session, using the default configuration parameters for the Periodic FTP Data Delivery and the example string values noted above, follows:

```
C:\>ftp hoss.netbotz.com

Connected to hoss.netbotz.com.

220 hoss.netbotz.com FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30:36
EST 2000) ready.

User (hoss.netbotz.com:(none)): netbotz

331 Password required for netbotz.

Password: password

230 User netbotz logged in.

ftp> cd 00_02_D3_00_01_1D

550 00_02_D3_00_01_1D: No such file or directory.

ftp> mkdir 00_02_D3_00_01_1D

257 “/export/homes/debbiej/00_02_D3_00_01_1D” new directory created.

ftp> cd 00_02_D3_00_01_1D

250 CWD command successful.

ftp> cd 2001-11-06

550 2001-11-06: No such file or directory.

ftp> mkdir 2001-11-06

257 “/export/homes/debbiej/00_02_D3_00_01_1D/2001-11-06” new directory
created.

ftp> cd 2001-11-06

250 CWD command successful.

ftp> ascii

200 Type set to A.

ftp> put botz.txt 21-42-03.nbsensor

200 PORT command successful.

150 Opening ASCII mode data connection for 21-42-03.nbsensor.

226 Transfer complete.

ftp: 934 bytes sent in 0.00Seconds 934000.00Kbytes/sec.

ftp> binary

200 Type set to I.

ftp> put campic.jpg 21-42-03_01.jpg

200 PORT command successful.
```

```
150 Opening BINARY mode data connection for 21-42-03_01.jpg.
226 Transfer complete.
ftp: 7729 bytes sent in 0.01Seconds 515.27Kbytes/sec.
ftp> quit
221-You have transferred 8661 bytes in 2 files.
221-Total traffic for this session was 9673 bytes in 2 transfers.
221-Thank you for using the FTP service on hoss.netbotz.com.
221 Goodbye.

C:\>
```

A Note for FTP Server Administrators

The APC NetBotz FTP Data Delivery mechanism requires and uses the following low-level FTP commands:

- USER
- PASS
- XMKD
- XCWD
- PASV
- STOR
- TYPE I
- TYPE A
- QUIT

All of these commands must be supported and usable by the user account configured for use by the APC NetBotz FTP Data Delivery mechanism.

Troubleshooting Network Connectivity Problems

Network connectivity issues can be caused by many circumstances that may have nothing to do with the APC NetBotz device itself. Network-attached devices should function normally if the device can be PINGed and normal SNMP traffic is possible between the device IP address and the system that is running the console software. Also, if you are using an SNMP network management system normal SNMP traffic must be possible between the device IP address and the Trap Target IP address.

If you are encountering problems in communicating with a network attached device, try the following:

- Ping the device IP address from the system on which you are running the console software.
- If you are using an SNMP-based network management system, attempt to retrieve the value of one of the standard MIB II objects (such as SysUptime) from both the device and from the device that the Device Crawlers or Device Scanner is attempting to monitor.
- If Device Crawlers or Device Scanner are configured by hostname (as opposed to IP address) ensure that the DNS server is configured on the device, that the DNS server is up and running, and that a lookup for the SNMP device hostname is resolved properly by the DNS server.

If you are unable to perform one or more of these basic network connectivity tasks, the problem probably is occurring as a result of a faulty network configuration and is not due to a device failure: see Basic Network Troubleshooting, below, for some tips on how to troubleshoot network problems. If, however, you are able to perform these tasks and are still encountering network connectivity issues with your device, contact the support staff for instructions.

Basic Network Troubleshooting

- Check your Ethernet cabling.
  - Inspect your Ethernet cable. Make sure it is a Category 5 UTP cable, and that there are no visible breaks or cuts in the cable.
  - Check the RJ45 plugs on each end of the cable. Make sure no wires have been pulled out of the plugs.
  - Make sure your cable is not draped over a fluorescent light or a power source of any sort.
  - Make sure your cable is plugged into an Ethernet jack and not a phone jack or RJ45 Token Ring port.
  - Make sure your cable is securely plugged into the devices to which you wish to connect. Reseat cables.
- Check your Switch or Router.
  - Check your Switch for FCS or Alignment errors. FCS and Alignment errors and nearly always caused by cabling-related issues.
  - Reduce the amount of network broadcasts that reach the port the NetBotz device is connected to.
  - If network traffic is very high, isolate the device from other traffic/noise on the network by creating a separate VLan for the device.
- Check your device.
  - Make sure the IP address, subnet mask and Gateway addresses you assigned to this device are valid.
- Test the connectivity from your client to the device.
  - Try to ping the device. ICMP must be enabled on your router for this to work.
  - Try to FTP or Telnet to the device. Telnet and FTP ports must be enabled on your router.
  - Telnet to your router, and try to ping the device from the router to see if it is a routing issue.

If you are unable to perform one or more of these basic network connectivity tasks, the problem probably is occurring as a result of a faulty network configuration and is not due to a device failure. If, however, you are able to perform these tasks and are still encountering network connectivity issues with your device, contact the support staff for instructions.

Warranty and Service

Limited warranty

APC warrants the InfraStruXure Central server to be free from defects in materials and workmanship for a period of 2 years (hardware) from the date of purchase. Its obligation under this warranty is limited to repairing or replacing, at its own sole option, any such defective products. This warranty does not apply to equipment that has been damaged by accident, negligence, or misapplication or has been altered or modified in any way. This warranty applies only to the original purchaser.

Warranty limitations

Except as provided herein, APC makes no warranties, expressed or implied, including warranties of merchantability and fitness for a particular purpose. Some jurisdictions do not permit limitation or exclusion of implied warranties; therefore, the aforesaid limitation(s) or exclusion(s) may not apply to the purchaser.

Except as provided above, in no event will APC be liable for direct, indirect, special, incidental, or consequential damages arising out of the use of this product, even if advised of the possibility of such damage.

Specifically, APC is not liable for any costs, such as lost profits or revenue, loss of equipment, loss of use of equipment, loss of software, loss of data, costs of substitutes, claims by third parties, or otherwise. This warranty gives you specific legal rights and you may also have other rights, which vary according to jurisdiction.

Obtaining service

Technical support and software updates are available only with the purchase of a software support contract. To obtain support for problems with your InfraStruXure Central server:

1. Note the serial number. The serial number is located on the rear of the appliance.
2. Contact Customer Support. Customer support for this or any other APC product is available at no charge in any of the following ways:
   – Visit the APC Web site to access documents in the APC Knowledge Base and to submit customer support requests.
     - www.apc.com (Corporate Headquarters)

   – Connect to localized APC Web sites for specific countries, each of which provides customer support information.
     - www.apc.com/support/

- Global support searching APC Knowledge Base and using e-support.
- Regional centers:

Direct Support for APC Security & Environmental Products	877-908-2688 (United States) or +1-401-789-5735
Latin America	+1-401-789-5735
Europe, Middle East, Africa	(353) (91) 702479 (Ireland)
Japan	(0) 35434-2021
Australia, New Zealand, South Pacific area	(61) (2) 9955 9366 (Australia)

- Contact the APC representative or other distributor from whom you purchased your APC product for information on how to obtain local customer support.

3. If you must return the product, the technician will give you a return material authorization (RMA) number. If the warranty expired, you will be charged for repair or replacement.
4. Pack the unit carefully. The warranty does not cover damage sustained in transit. Enclose a letter with your name, address, RMA number and daytime phone number; a copy of the sales receipt; and a check as payment, if applicable.
5. Mark the RMA number clearly on the outside of the shipping carton.
6. Ship by insured, prepaid carrier to the address provided by the Customer Support technician.

Life-Support Policy

General policy

American Power Conversion (APC) does not recommend the use of any of its products in the following situations:

- In life-support applications where failure or malfunction of the APC product can be reasonably expected to cause failure of the life-support device or to affect significantly its safety or effectiveness.
- In direct patient care.

APC will not knowingly sell its products for use in such applications unless it receives in writing assurances satisfactory to APC that (a) the risks of injury or damage have been minimized, (b) the customer assumes all such risks, and (c) the liability of American Power Conversion is adequately protected under the circumstances.

Examples of life-support devices

The term *life-support device* includes but is not limited to neonatal oxygen analyzers, nerve stimulators (whether used for anesthesia, pain relief, or other purposes), autotransfusion devices, blood pumps, defibrillators, arrhythmia detectors and alarms, pacemakers, hemodialysis systems, peritoneal dialysis systems, neonatal ventilator incubators, ventilators (for adults and infants), anesthesia ventilators, infusion pumps, and any other devices designated as “critical” by the U.S. FDA.

Hospital-grade wiring devices and leakage current protection may be ordered as options on many APC UPS systems. APC does not claim that units with these modifications are certified or listed as hospital-grade by APC or any other organization. Therefore these units do not meet the requirements for use in direct patient care.

APC®

Legendary Reliability®

PN: 02418D03