APC

by Schneider Electric

Online Help

InfraStruXure Central

Version 5.0.0

About Help

Help is available at any time, and can be viewed and invoked in a variety of ways. Relevant topics can be printed from the Help browser window.

You can choose to open help in a separate Help browser window by selecting **Help Contents** in the **Help** menu, or you can choose to open the **Help** view for the currently selected view by selecting **Dynamic Help** in the **Help** menu, or by pressing F1. This **Help** view provides access to information directly related to the selected view, and when a different view is selected, it automatically updates to provide access to help for the new view.

Context-sensitive help is also available in displays: clicking the question-mark (?) button in the lower-left corner adds a version of the **Help** view to the display that provides access to information directly related to that display.

Help menu

This menu's options access the online help in a separate Help browser, search and dynamic help in a **Help** view, and copyright and version information.

Help Contents	Opens the online help in a separate Help browser window.
Search Help	Opens the search function in the **Help** view.
Dynamic Help	Opens the **Help** view with access to context-sensitive information about the currently selected view.
About InfraStruXure Central	Opens the "About InfraStruXure Central" display which provides copyright and version information.

"About InfraStruXure Central" display

This display, accessed by selecting **About** in the **Help** menu, provides version and build numbers, as well as copyright information.

Note: Please have the version and build numbers available when contacting APC support.

APC Worldwide Customer Support

Access to customer support for this or any other APC product is available from virtually anywhere in the world.

To access documents in the APC Knowledge Base, to submit customer support requests, or to locate the telephone number for the support you need, please do the following:

1. Go to the APC Support page: http://www.apc.com/support .
2. Select the appropriate country from the **Country** drop-down menu at the top of the page, and do any of the following:
   - Use the available links to access web-based support, including links to a full range of self-help documents, and the APC Knowledge Base.
   - Use the **Phone support** link under **Ask APC** in the left side of the page to access country-specific address, phone, and e-mail information.

   Note: Alternatively, you can contact the APC representative or other distributor from whom you purchased your APC product for information on how to obtain local customer support.

Console features

The InfraStruXure Central server creates a consolidated view of your network's physical infrastructure layer. Real-time device monitoring, custom reporting capabilities, private networking, advanced security and immediate event notification all enable quick assessment and resolution of critical situations.

The InfraStruXure console provides your InfraStruXure Central client access to the server functions and features. This console has has the following major elements:

- **Monitoring** and **Surveillance** perspectives and views
- Six main menus (**File**, **Edit**, **Settings**, **Updates**, **Window**, and **Help**)
  Note: Right-click menus are also available in the perspectives and views.
- A status bar at the bottom of the display

Perspectives and views

The console uses perspectives and views to provide information, and access to major functions.

There are two perspectives you can choose for the console:

- **Monitoring**: provides access to the data and functions you can use to monitor and manage your devices.
- **Surveillance**: provides access to data and functions you can use to monitor and manage the surveillance equipment at monitored devices.
  Note: The surveillance feature is separately-licensed. Its license must be entered at the InfraStruXUre Central server using **License Key** in the "Server Administration Settings" display accessed by **Server Administration Settings** in the **Settings** menu.

When you log on to your InfraStruXure Central server, the console opens with the **Monitoring** perspective displayed; **Monitoring** and **Surveillance** buttons below the main menus allow you to switch between perspectives.

Monitoring

This perspective opens with four views displayed, by default.

- **Device Groups** view: used in this perspective to create the device groups to which monitored devices can be assigned, and to select a device group to view or manage its devices.
- **Device View**: lists the devices assigned to the group selected in the **Device Groups** view, provides information about those devices, and launch to management applications at some of those devices.
- **Map View**: displays icons for the devices in the group selected in the **Device Groups** view, each icon providing quick access to information about its sensor values; the icons, which are displayed against a user-definable background, can be repositioned and resized.
- **Active Alarms** view: provides information about any alarms that exist for the devices assigned to the group selected in the **Device Groups** view.

You can use the **Window** menu to add any other views to the **Monitoring** perspective.

- **Alarm History** view: allows you to review the alarms that occurred during a specified period of time, for all devices within a selected device group, or for a device, or set of devices, selected in that group.

- **Saved Discoveries** view: allows you to run or schedule previously performed or new processes used to discover and add devices to the list of devices the InfraStruXure Central server monitors.
- **SNMP Device Update Status** view: allows you to view information about the status of ongoing update processes for monitored SNMP devices.
- **NetBotz Appliance Update Status** view: allows you to view information about the status of ongoing firmware update processes for monitored NetBotz Appliances.
- **Saved Reports** view: provides a list of saved reports that you can view in graph or table format, as well as edit and delete.

Surveillance

This perspective opens with two views displayed, by default.

Note: For more information about how the identified views are used for surveillance functions, see Surveillance perspective.

- **Thumbnails** view: provides thumbnail views and identification information for the surveillance equipment.
- **Device Groups** view: used in this perspective primarily to select a device group to view the thumbnails for that group's surveillance equipment.

Main menus

A menu bar immediately below the console title bar provides five menus, with options that control or configure InfraStruXure Central features and functions.

Menu	Options
File	**Change Server**: closes the session, and accesses the "InfraStruXure Central Logon" display. **Reboot Server**: reboots the InfraStruXure Central server. **Note:** When a reboot finishes, an e-mail is sent to the **InfraStruXure Central Administrator** users that include an e-mail address as part of their user credentials. **Shut Down Server**: shuts down the InfraStruXure Central server. **Exit**: closes the InfraStruXure Central client.
Edit	**Add Devices**: accesses the "Device Discovery" wizard used by the Device discovery processes. **Client Preferences**: accesses settings specific to the InfraStruXure Central client you use.
Settings	Provides options used to configure the InfraStruXure Central server and client, monitored NetBotz Appliances, and monitored SNMP devices. **Alert Settings**: accesses options used to define the alert notifications generated by the InfraStruXure Central server, as well as to define the alert notifications generated by each monitored NetBotz Appliance. **SNMP Device Settings**: accesses options used to configure various functions for the monitored SNMP devices. **NetBotz Appliance Configuration**: accesses options used to configure various functions at the monitored NetBotz Appliances. **Surveillance Settings**: accesses settings used to configure various functions for the surveillance devices at monitored NetBotz Appliances.

Menu	Options
	Graphing and Reporting: accesses a **Scheduled Export Configuration** option used to schedule when device sensor reports will be automatically exported. **Server Administration Settings**: accesses options used to configure a wide range of InfraStruXure Central server functions.
Updates	Provides options used to update the InfraStruXure Central server and its monitored NetBotz Appliances and SNMP devices. **Schedule Update Checks**: accesses settings used to schedule when the InfraStruXure Central server will check for available APC device firmware updates. **Apply Firmware Updates**: accesses the "Update Device Firmware" wizard used to download firmware updates to monitored NetBotz Appliances or SNMP devices. **Apply Server Updates**: accesses the "Product Update" wizard used to update the InfraStruXure Central server.
Window	Provides a **Restore Default Screen Layout**: option that restores the selected perspective to its default views and layout, and five categories of options that access views of the same name that are used in the **Monitoring** and **Surveillance** perspectives. **Alarms**: **Active Alarms** and **Alarm History** **Devices**: **Device Groups**, **Device View**, **Map View**, and **Saved Discoveries** **Firmware Updates**: **SNMP Device Update Status** and **NetBotz Appliance Update Status** **Reports**: **Saved Reports** only **Surveillance**: **Thumbnails** only
Help	Provides options used to access the help, and information about the application. **Help Contents**: opens the help in a separate window with the top item in the table of contents selected. **Search Help**: opens the search function in the **Help** view. **Dynamic Help**: opens the **Help** view with information about the view selected in the **Monitoring** or **Surveillance** perspective. **About**: opens the "About InfraStruXure Central" display which provides version, build, and copyright information.

Status bar

Reports information about the InfraStruXure Central server. Each type of information can be clicked to access a related view or display.

Information	Description
Device status	How many devices have a warning or critical condition. Clicking this area accesses the **Active Alarms** view.
User	The username you used to log on, and the hostname or IP address of your InfraStruXure Central client.

	Clicking this area accesses the "Logged on Users" display that identifies all users logged on at the server.
Devices	The number of devices the InfraStruXure Central server is monitoring. Clicking this area accesses the **Device View**.
Device discoveries in progress	How many discovery processes are currently in progress. Clicking this area accesses the **Saved Discoveries** view.

"Logged on Users" display

Use this display to review information about the users (**Username**), their **Logon Time**, and the hostname or IP address of their InfraStruXure Central clients (**Client**).

Right-click options common to all views

All views share options accessed by right-clicking within the top border of a view. These options physically affect a view, but not the information the view provides.

Option	Description
Detached	Detaches the view, creating an unanchored, free-floating view.
Restore	Currently disabled.
Move	Allows you to move a view to anywhere else within the selected perspective.
Size	Highlights the side of the view you want to use to resize the view: **Right**, **Left**, **Top**, or **Bottom**. **Note:** The sides of the view which can actually be used to resize that view will be the only enabled options.

Initial setup requirements

The following actions should have been performed during the InfraStruXure Central server installation.

- The server was physically installed.
- The server was connected to a power source.
- The public and private local area network (LAN) settings were defined at the server.
  Note: You can verify these settings are defined correctly by selecting **Server Administration Settings** in the **Settings** menu, and then selecting **Network Settings** in the "Server Administration Settings" display.

With those actions performed, you can log on to the InfraStruXure Central server and configure that server to use all of the InfraStruXure Central server's functions and features to monitor and manage your company-wide physical-infrastructure devices, and other APC, NetBotz, and 3rd-party devices on your networks.

Minimum setup requirements

There are a several actions you must take to configure the server to perform the most basic of functions needed to monitor SNMP devices and NetBotz Appliances.

1. If the InfraStruXure Central client is installed on your machine, go to step 2. Otherwise, do the following:
   a. Use a browser to launch to the IP address or hostname of the server.
   b. Click **Install InfraStruXure Central Client**, and follow the on-screen instructions to install that client.
2. Launch your client and log on at the InfraStruXure Central server using your administrator **Username** and **Password** (**apc** **/apc** are the defaults).
3. Enter InfraStruXure Central licenses, if you want to start monitoring more than 25 devices, or to use the separately-licensed Surveillance feature. Otherwise, go to step 4.
   a. Select **Server Administration Settings** in the **Settings** menu.
   b. Select **License Keys** in the "Server Administration Settings" display.
   c. Enter the license keys.
      Note: You can also enter the license numbers for separately-licensed applications, in addition to Surveillance, such Capacity and Change Manager.
4. Make sure the administrator credentials include the e-mail address of the person you want notified when alarm conditions directly related to InfraStruXure Central server operations occur.
   a. Select **Server Administration Settings** in the **Settings** menu.
   b. Select **Users and User Groups** in the "Server Administration Settings" display.
   c. Select the **InfraStruXure Central Administrator** (**apc**, by default) in the **Users** tab, and click **Edit User**.
   d. Edit the **E-Mail Address** credential, if needed.
      Note: You can change the default **Username** and **Password** values, as well.
5. Define the e-mail settings the InfraStruXure Central server will use to send e-mails to the administrator when alarm conditions related to the server operations occur.
   a. Select **Server Administration Settings** in the **Settings** menu.
   b. Select **E-mail Settings** in the "Server Administration Settings" display.
   c. Define the **Primary** and **Secondary** tab settings, as needed.
6. Enable the SOCKS server feature to enable communication with any devices you want to monitor on the private LAN, if necessary.

   a. Select **Server Administration Settings** in the **Settings** menu.
   b. Select **Server Access** in the "Server Administration Settings" display.
   c. Enable the **SOCKS Server** option in the **SOCKS Proxy** tab.

7. Add a remote NFS or Windows share repository the InfraStruXure Central server can use instead of the local repository.
   a. Select **Server Administration Settings** in the **Settings** menu.
   b. Select **Storage Settings** in the "Server Administration Settings" display.
   c. Use the **Repositories** tab to add a remote repository.
   d. Use the **Purge Settings** tab to define the purge settings you want the repository to use.
8. Define at least one NFS or Windows share location to be used for backup files of the InfraStruXure Central server's configuration data, or its configuration and repositories data.
   a. Select **Server Administration Settings** in the **Settings** menu.
   b. Select **Server Backup/Restore** in the "Server Administration Settings" display.
   c. Identify the NFS or Windows share location at which backup files will be saved.
   d. Schedule how often those files will be created automatically.
      Note: By default, backup files will be created every Friday at 1:00 AM.
9. Discover the SNMPv1 devices, SNMPv3 devices, and NetBotz Appliances you want your server to monitor.
   Note: All three device types require their own discovery process, not only on the public LAN, but on the and private LAN, as well.
   a. Select **Add Devices** in the **Edit** menu, or click the green + icon in the **Devices View**.
   b. Select which type of device you want to discover (SNMPv1, SNMPv3, or NetBotz Appliance), and click **Next**.
   c. Define the parameters to be used for the discovery process.
   d. Run the discovery process.
   e. Repeat steps a through d, as needed, to discover all the types of devices you want the InfraStruXure Central server to monitor (SNMPv1, SNMPv3, and NetBotz Appliance), on both the public and private LANs.
10. Define any or all the alert actions you want available to the InfraStruXure Central server, and to any NetBotz Appliances discovered during step 7, to associate with the default alert profiles used for alert notifications: the InfraStruXure Central server has a default profile it can use for alarms at monitored SNMP devices; each NetBotz Appliance has its own unique default profile it can use for alarm conditions at the devices it monitors.
    Note: An alert action must be available to the InfraStruXure Central server, and to each monitored NetBotz Appliance, for use with their default profiles.
    a. Select **Alert Actions**, an **Alert Settings** option in the **Settings** menu.
    b. In the "Select Alert Action Type" display, select an action.
    c. In the "Select Next Action" display, select an **Create a new alert action**.
    d. In the "Select Next Action Devices" display, select the devices for which the action can be used.
    e. Define the action settings.
    f. In the "Choose Next Action" display, select Configure another alert action to repeat steps b through e, as needed, to finish defining all the alert actions for your InfraStruXure Central server and monitored NetBotz Appliances.
11. Add at least one alert action to the default alert profiles used by alert notifications: the InfraStruXure Central server has a default profile it can use for alarms at monitored SNMP devices; each NetBotz Appliance has its own unique default profile it can use for alarm conditions at the devices it monitors.
    Note: The default profile at a NetBotz Appliance may have been defined already using its **NetBotz Advanced View**, or by another InfraStruXure Central server. However, you can edit it to make sure sure someone in your organization is notified when problems occur.
    a. Select **Alert Profiles**, an **Alert Settings** option in the **Settings** menu.
    b. In the "Select Parent Device" display, select the parent device (InfraStruXure Central server or individual NetBotz Appliance) associated with the default profile you want to configure.
    c. In the "Select Alert Profile" display, select **Default*** and click **Next**.

d. Configure the default profile to include at least one of the alert actions available to the selected parent device.
e. Repeat steps a through d to add at least one alert action to the default profile used by the InfraStruXure Central server, and to the default profile for each monitored NetBotz Appliance.

Other support and feature setup requirements

Once the minimum setup requirements are defined, you can begin to configure the InfraStruXure Central server to use all of its features and functions.

- Create the device groups and subgroups, in the **Device Groups** view, that you can use to group monitored devices that are physically or logically associated with each other, for easier access to information about associated devices.
- Assign devices to the device groups by selecting **Unassigned** in the **Device Groups** view and dragging them from the **Device View** into your groups and subgroups.
- Add the local and remote users that you want to have access to the server, and the local and remote user groups that can be used for easier management of the user's privileges at the device groups by selecting **Server Administration Settings** in the **Settings** menu, and using the **User and User Groups** tabs.
- Customize the **Map View** for a group selected in the **Device Groups** view, by using the **Map View Settings** and **Sensor Label Settings** right-click options in the **Map View**.
- Define any new alert actions you want to use for the alert profiles you will create for the alert thresholds at the InfraStruXure Central server, or at the NetBotz Appliances it monitors, using **Alert Actions**, an **Alert Settings** option in the **Settings** menu.
- Define the alert profiles the InfraStruXure Central server and NetBotz Appliances can use in alert notifications for the alert thresholds they monitor, using **Alert Profiles**, an **Alert Settings** option in the **Settings** menu.
- Define the alert threshold settings you want the InfraStruXure Central server, and NetBotz Appliances, to monitor, using **Alert Thresholds**, an **Alert Settings** option in the **Settings** menu.
- Define the remaining administration settings, as needed, using **Server Administration Settings** in the **Settings** menu.
- Configure the settings the InfraStruXure Central server uses to communicate with its monitored SNMP devices, as needed, using **SNMP Device Settings** in the **Settings** menu.
- Configure settings used by the monitored Network Appliances, as needed, using **NetBotz Appliance Configuration** in the **Settings** menu.
- License your surveillance cameras, if any, using the **Thumbnails** view.
  Note: A surveillance license must be entered in the **License Keys** section of the "Server Administration Settings" display.
- Configure the settings that affect how the surveillance equipment operates, using **Surveillance Settings** in the **Settings** menu.
  Note: At least one camera must be defined as licensed to configure these settings.
- Define the settings for your InfraStruXure Central client, using **Client Preferences** in the **Edit** menu.
- Define how often you want the InfraStruXure Central server to check for firmware updates available from APC, using **Schedule Update Checks** in the **Updates** menu.
- Configure the settings the InfraStruXure Central server will use to log on to the web interface at the monitored devices, using the right-click **Device Launch Settings** option in either the **Device View** or **Map View**.
- Generate and manage graph or table-formatted reports for device sensors, using the **Saved Reports** view, or the right-click **Graphing and Reporting** option in the **Device Groups** view, **Device View**, and **Map View**.

Monitored devices

The InfraStruXure Central server can monitor and manage APC, MGE, NetBotz, and third-party devices. Once these devices have been discovered, you can do the following:

- Review sensor and devices status information about the devices in the **Device View** and **Map View**.
- Review information about existing device alarm conditions in the **Active Alarms** view.
- Review information about historical device alarm conditions in the **Alarm History** view.
- Launch to the remote device management applications.
- Generate reports for sensors at the devices.
- Assign devices to groups and subgroups in the **Device Groups** view.
- Create alert thresholds on device sensors.

Supported devices

The InfraStruXure Central server can monitor APC, MGE, NetBotz, and third-party devices that it can discover on its public and private LANs.

- NetBotz Rack or Wall Appliances (except for 300, 303, 310, 400, and 410 models).
- First generation power distribution units (PDUs) and AP76xx outlet strips, when discovered on the private LAN, only.
- Any APC or third-party device that can communicate with the server using SNMPv1 or SNMP v3 communication, with three levels of support provided.

Basic SNMP support	The InfraStruXure Central server can provide only **Type** (**SNMP Device** only), on-line or communication lost **Status**, **Hostname**, and **Groups** information.
Model ID SNMP support	The InfraStruXure Central server can report **Model** information, in addition to the information provided for basic SNMP support.
Full SNMP support	The InfraStruXure Central server can provide sensor data and alarms information, in addition to the information provided for model ID SNMP support.
Note: Additional sensors can be created on devices using **Supplemental OID**, a "SNMP Device Settings" display option accessed by **Device Settings**, an **SNMP Device Settings** option in the **Settings** menu.	

Device Definition File (DDF)

DDF files include information on which sensors the InfraStruXure Central can report for SNMP devices. The InfraStruXure Central server ships with the DDF files necessary for reporting sensors on all APC devices and some third-party devices. In addition:

- DDF files, for third-party devices, may be available from APC Technical support.
- You can use **Device Definition Files**, a "SNMP Device Settings" display option accessed by **Device Settings**, an **SNMP Device Settings** option in the **Settings** menu, to check the APC website for new or updated DDFs, and download those files to the InfraStruXure Central server.

- APC SNMP devices that use a Network Management Card (NMC) version of 3xx or higher have a DDF file that the InfraStruXure Central must download at discovery time. This DDF file contains information about the alarm conditions the device can report.

Launch to device feature

An InfraStruXure Central server has the ability to launch to any discovered device that supports an HTTP/HTTPS web interface.

You an access the devices web interface by doing one of the following actions in either the **Device View** or **Map View**:

- Double-click the device in the **Device View**.
- Highlight the device in the **Device View**, and press Enter.
- Right-click the device in either the **Device View** or **Map View**, and select **Launch to Device**.

An error will occur when the HTTP/HTTPS protocol or port definitions defined for this device at the InfraStruXure Central server do not match the protocol and port definitions required by that device. To check or set the HTTP/HTTPS settings, right-click the device and select **Device Launch Settings** to access the "Device Launch Settings" display.
Note: You can select multiple devices in either the **Device View** or **Map View** to use the "Device Launch Settings" display to define identical HTTP/HTTPS protocol and port definitions for those devices.

"Device Launch Settings" display

Use this display to define how InfraStruXure Central server will use an Internet browser to communicate with the device or devices selected by **Device Launch Settings**, a right-click option in the **Device** and **Map Views**.

Element	Description
HTTP	Click to select the HTTP protocol for browser communication.
HTTPS	Click to select the security-enhanced HTTPS protocol for browser communication.
Port	Identify the number of the port use for browser communication at a selected device: **80** is the default for **HTTP**; **443** is the default for **HTTPS**.

Device and Map Views

Two views provide access to information about the monitored devices, one in a table format (**Device View**), and one as icons on a graphic background (**Map View**), with a unique **Map View** available for each group in the **Device Groups** view, except for **Unassigned**, which uses the default **Map View** only.

Note: Both views are included in the **Monitoring** perspective, by default, and can be accessed from the **Window** menu, if needed.

Device View features

This view uses a table format to provide access to information about the monitored devices. It also is used to manage which devices are assigned to which device groups, a function that cannot be performed in a **Map View**.

In addition to managing the devices in the device groups, the **Device View** has the following features:

- The device list provides information about each device in the device group selected in the **Device Groups** view.
  - You can click the **Menu** icon to define which columns appear in the view.
  - You can click a column title to sort the list in ascending or descending order based on that column's information.
  - A **Search** field and **Clear** button allow you to filter the device list to display only the devices that include your typed text.
  - You can select a device, or devices, to filter the **Active Alarms** view to show only the alarms for selected devices.
    Note: When a NetBotz Appliance is selected, the **Active Alarms** view will display its alarms, including all alarms associated with the devices it monitors.
  - You can double-click a device to log on to its web interface, if it has one.
    Note: A right-click **Device Launch Settings** option defines the **HTTP/HTTPS** and **Port** settings used to communicate with a device's web interface.
- Right-click options, and icon buttons at the top of the view, perform the following functions:
  - Initiate a device discovery process used to add SNMP devices or NetBotz Appliances to be monitored by the InfraStruXure Central server (**Add Devices** option or the green + icon).
  - Delete devices that you no longer want the InfraStruXure Central server to monitor (**Delete Devices** option or the x icon).
  - Generate a report or graph for the historical values of the sensors at selected devices (**Custom Device Report** option or graph icon).
  - Access the **Alarm History** view to review historical alarm data for any selected devices (**Show Alarm History** option).
  - Define the port and protocol settings to be used by the InfraStruXure Central server to communicate with the web interface at selected devices (**Device Launch Settings** option).
  - Log on to the web interface at a selected device, if it has one (**Launch to Device** option).
  - Remove selected devices from a shared device group, without causing the InfraStruXure Central server to stop monitoring those devices (**Remove Device from Group** option).
  - Request that the InfraStruXure Central server immediately scan selected devices for sensor values, without waiting until the server would normally scan those devices (**Request Device Scan** option).

- View all the values being reported by the sensors at selected devices (**View Device Sensors** option).
- Add or edit alert thresholds for a selected device, or set of devices (**Alert Thresholds** options).
  Note: For information about these options, see **Alert Thresholds** options, under **Alert Settings** in the **Settings** menu.
- Access a specific configuration option for a selected NetBotz Appliance or Appliances (**NetBotz Appliance Configuration** options).
  Note: For information about these options, see NetBotz Appliance Configuration under Settings menu.
- Access the **Surveillance** perspective with a selected camera highlighted in the **Thumbnails** view (**Show in Surveillance Perspective** option).
  Note: **Show in Surveillance Perspective** is only available when a camera is selected; when multiple cameras are selected, only the camera closest to the top of the **Devices View** is highlighted in the **Thumbnails** view.

NetBotz Appliances in the Device View

A NetBotz Appliance appears in the **Device View** as an expandable listing. When expanded, each device it monitors is listed under the main NetBotz Appliance listing, including an entry that reports the network status of the appliance itself.

- The hostname or IP address of the NetBotz Appliance is reported in the **Parent Device** column for the NetBotz Appliance, and for each associated device.
- You can select the right-click **View Device Sensors** for the main (expandable) listing for a NetBotz Appliance in the **Device View** (or for a NetBotz Appliance icon in the **Map View**), to access information about all sensors for the NetBotz Appliance and any devices that it monitors.
- You can double-click on the main NetBotz Appliance entry, or from any of its associated devices, to launch to the appliance's web interface (or highlight the appliance in the **Device View** or **Map View** and select the right-click **Launch to Device** option).
- You can move copies of any associated device, including the device that represents the appliance, to any other device group; a copy of that device remains associated with the main NetBotz Appliance listing.

Information columns

The **Device View** columns provide information and status for listed devices.

Note: A **Menu** icon at the top of the view allows you to define which columns are displayed.

Column	Description
Type	The type of device, with **SNMP Device** used as a generic identification.
Status	The severity of the most serious alarm condition at a device. **Note:** You can select a device in the **Device View** to access information about its alarms in the **Active Alarms** view. Monitored SNMP devices typically report three status conditions:

	Normal: no alarm conditions exist. **Warning**, a condition exists that may require attention to make sure it does not deteriorate into a critical state. For example, a UPS that is running on battery power during a power failure will shut down its load equipment if its battery power is depleted before power returns to normal. **Critical**: a condition exists that requires immediate attention. For example, a discharged battery can result in the loss of UPS protection during a power failure. NetBotz Appliances typically report two status conditions, in addition to **Normal**: **Error**: a sensor threshold violation exists that requires immediate attention. For example, a high temperature violation that could lead to equipment damage. **Failure**: an operational failure exists that requires immediate attention. For example, communication with a camera pod was lost which could lead to an undetected security violation. **Note:** The status reported for alert threshold violations can be defined by each threshold's severity settings. For example, a door sensor can be set to report **Informational** status for an open door.
Model	The device model, if known. For example, **Windows NT 4.0/2000**, for a workstation, or **Silcon DP310E**, for an APC/MGE UPS.
Hostname	The hostname, or IP address, if no hostname is defined, for a monitored SNMP device or NetBotz Appliance. **Note:** A **Hostname** is provided for SNMP devices monitored by NetBotz Appliances, but not for non-SNMP devices such as sensor and camera pods.
Parent Device	Identifies the InfraStruXure Central server, for SNMP devices directly monitored by the server, or the hostname or IP address for a NetBotz Appliance and its supported devices.
Serial Number	The serial number assigned to a device, if known.
IP Address	The IP address used by a monitored SNMP device or NetBotz Appliance. **Note:** An **IP Address** is provided for SNMP devices monitored by NetBotz Appliances, but not for non-SNMP devices such as sensor and camera pods.
Location	The location associated with a device, if known.
Application Version	The application or firmware version number for a device, if known. For example, **4.7.0.250**, for an InfraStruXure Manager server, or **v2.6.1**, for a Smart-UPS 3000 RM device.

Label	The label defined for a device.
Description	The device description, if known.
Groups	The names of any device groups a device belongs to, including **All Devices** and **Unassigned**.

Button icons (Device View)

In addition to standard minimize and maximize icons, four icons are available to perfom specific **Device View** functions.

Note: Except for the **Menu** icon, right-click options are available to perform the same functions.

Icon	Description
✚	Use this **Add Devices** icon to initiate a device discovery process used to add SNMP devices or NetBotz Appliances to be monitored by the InfraStruXure Central server.
✖	Use this **Delete Devices** icon to delete devices that you no longer want the InfraStruXure Central server to monitor.
📊	Use this **Custom Device Report** icon to create a report or graph for the historical values of the sensors at selected devices (see Reports feature).
▽	Use this **Menu** icon to identify the columns to be included in the device list.

Map View features

This view presents devices as icons on a customizable graphic background.

A unique **Map View** can be created for each group in the **Device Group** view, with each view having the following features:
Note: The **Map View** for the **Unassigned** device group cannot be customized.

- You can create a representation of the monitored devices that makes visual sense, according to your needs.
  Note: By default, the device icons are positioned in a row layout on a tiled background, and identified by a label that is positioned below the icons.
  - You can customize the background, and the size and shape of the icons.
  - You can define where the icon labels that identify the devices are positioned, or disable those labels.
  - You can reposition the icons.
  - You can hover over an icon to view information about the device's sensors.
  - You can show the current value of a sensor at one or more of the device icons.

    - You can use the **Find Device in Map** icon, or right-click option, to search and select devices by IP address, location, hostname, or type.
- You can select a device icon, or icons, to filter the **Active Alarms** view to show only the alarms for selected devices.
  Note: When a NetBotz Appliance is selected, the **Active Alarms** view will display its alarms, including all alarms associated with the devices it monitors.
- Right-click options, and icons at the top of the view, allow you to perform functions related to managing the **Map View** background and icons.
    - Reposition icons within the map (**Edit Map** option or icon), and save the new positions (**Save Map** option or icon).
    - Reset the device icons back to their default positions (**Reset Device Positions** option or icon).
    - Select (**Select All** option) or deselect (**Deselect All** option) all devices in the **Map View**.
    - Select the graphic used for the background, and how it is used, as well as define how icons are displayed (**Map View Settings** option or icon).
    - Select sensor values to be displayed by the icons (**Sensor Label Settings** option or icon).
- Other right-click options allow you to perform functions not directly related to managing the **Map View**.
    - Delete devices that you no longer want the InfraStruXure Central server to monitor (**Delete Devices** option).
    - Initiate the process used to create a report or graph for the historical values of the sensors at selected devices (**Custom Device Report** or graph icon).
    - Access **Alarm History** view to review historical alarm data for any selected devices (**Show Alarm History** option).
    - Define the port and protocol settings to be used by the InfraStruXure Central server to communicate with the web interface at selected devices (**Device Launch Settings** option).
    - Log on to the web interface at a selected device, if it has one (**Launch to Device** option).
    - Request that the InfraStruXure Central server immediately scan selected devices for sensor values, without waiting until the server would normally scan those devices (**Request Device Scan** option).
    - View all the values being reported by the sensors at selected devices (**View Device Sensors** option).
    - Add or edit alert thresholds for a selected device, or set of devices (**Alert Thresholds** options).
      Note: For information about these options, see **Alert Thresholds** options, under **Alert Settings** in the **Settings** menu.
    - Access a specific configuration option for a selected NetBotz Appliance or Appliances (**NetBotz Appliance Configuration** options).
      Note: For information about these options, see NetBotz Appliance Configuration under Settings menu.

Button icons (Map View)

In addition to standard minimize, maximize, zoom, and undo/redo icons, five icons are available to perform specific **Map View** functions.

Note: Right-click options are available to perform the same functions as the five button icons.

Icon	Description
	Use this **Edit Map/Save Map** icon to reposition devices within the map, and save the new positions.
	Use this **Find Device in Map** icon to search and select devices by IP address, location, hostname, or device label.
	Use this **Map View Settings** icon to define settings that affect the background, as well as how icons are displayed in the map.
	Use this **Reset Device Positions** icon to reset the device icons back to their default positions.
	Use this **Sensor Label Settings** icon to select sensor values to be displayed for the **Map View** devices.

Creating a customized background

Use the "Map View Settings" display to create a custom background for a selected device group's **Map View**.

1. Access the "Map View Settings" display by selecting the right-click **Map View Settings** option, or clicking the **Map View Settings** icon, in the **Map View**:
2. In the "Map View Settings" display, select the **Map Icon Settings** option and click **Custom Background**.
3. Click **Custom**, and use the "Open" display to browse to, and open, the.jpg,.png,.bmp, or.gif file you want to use for the background.

   Note: You can click **Save** to save a copy of the selected graphic on your client, if desired.
4. Select how you want the graphic positioned in the **Map View**:
   - **Center Image**: positions the graphic in the center of the view.
   - **Top-Left Image**: positions the graphic in the top-left portion of the view.
   - **Stretch Image**: stretches the graphic, horizontally and vertically, to fill the view.
   - **Tile Image**: includes copies of the graphic as tiles, with the number of tiles dependant on the size of the graphic.
5. Repeat steps 1 through 4 for the **Map Views** of the other device groups.

Customizing the device icons

Use the "Map View Settings" and "Sensor Label Settings" displays to customize how the device icons are displayed in a selected device group's **Map View**.

1. Access the "Map Settings" display by selecting the right-click **Map View Settings** option, or clicking the **Map View Settings** icon, in the **Map View**.
2. In the "Map View Settings" display, select the **Map Icon Settings** option, and do any of the following actions:

   Note: The **Icon Preview** shows how your changes will affect the icons.

- Select whether you want to use **Small** or **Large Icons**.
- Use the **Width** and **Height** options to change the shape of the icon, if desired.
- Select **Show Labels** to have the **Map View**: include device labels.
- When labels are enabled, select whether you want them displayed horizontally at the bottom of the icons (**Horizontal**), or vertically along the right side of the icons (**Vertical**).

3. Repeat steps 1 and 2 for the **Map Views** of any other device groups.

Selecting sensor values for a Map View's devices

Use the "Sensor Label Settings" display to select a sensor to be displayed for all devices that report the sensor, or to select a sensor to be displayed on a specific device or set of devices in a **Map View**.

Selecting a default sensor label for devices

You can select a sensor for all devices to display in a **Map View**, however, only devices that report that sensor will show its value.

1. Select the **Sensor Label Settings** right-click option, or the **Sensor Label Settings** icon at the top of the **Map View**. Select the "Sensor Label Settings" display's **Default** tab.
2. Make sure the **Show Sensor Labels** option is selected.
3. In the "Sensor Label Settings" display's **Default** tab, select the sensor you want to use from the available sensor list, or search for it using the search feature.

   Note: **Show Sensor Labels** must be selected to use the **Default** or **Selected** tabs.

Selecting a sensor label for a selected device or set of devices

You can select a sensor value a device or set of devices, selected in a **Map View**, will report instead of the **Default** sensor.

Note: When multiple devices are selected, if you choose a sensor that is not reported for by some of those devices, those devices will show no value.

1. Select the device or devices in the **Map View**.
2. Select the **Sensor Label Settings** right-click option, or the **Sensor Label Settings** icon at the top of the **Map View**.
3. In the "Sensor Label Settings" display's **Selected** tab, select the sensor value you want the device or set of devices to display, by choosing one of the following options:
   - Select **No Changes**, if you do want the currently selected sensor value or values to remain unchanged.
   - Select **Display the Default Sensor**, if you want the selected device or devices to use the identified default sensor.
   - Select **Chose a Specific Sensor**, and select the sensor you want to use from the available sensor list, or search for it using the search feature.
     Note: If a selected device does not report the sensor you selected, that device will not show a sensor label.

"Map View Settings" display

Use this display to define how the background and icons will appear in a device group's **Map View**.

Map Background Settings option

Click **Default Background**, to use a blank-tiled background, or **Custom Background**, to create and use a custom background.

When you click **Custom Background**, the following elements are activated.

Element	Description
Select Image	Click to browse to and select the graphic you want to use for the background.
Save	Click to save the selected background image as a file at your local machine.
Center Image	Select to center the graphic in the view.
Top-left Image	Select to position the graphic in the top-left section of the view.
Stretch Image	Select to stretch the graphic to fill the view.
Tile Image	Select to use copies of the graphic as tiles in the view, with the number of tiles based on the size of the graphic.

Map Icon Settings option

Use this option to customize how the icons will look in a **Map View**, including whether device labels that will be included with the icons, and where the labels will be positioned.

Element	Description
Icon Preview	Shows the affect of applied **Sizing** and **Icon Labels** definitions on how icons will appear in a **Map View**.
Width	Drag right or left to change the width of the icons.
Height	Drag up or down to change the height of the icons.
Small Icons	Click to use small icons.
Large Icons	Click to use large icons.
Show Labels	Select to include device labels in the **Map View**. **Horizontal** will show the label below the icon, horizontally, and **Vertical** will show the label to the right of the icon, vertically.

"Sensor Label Settings" display

Use this display to define which sensor values to display for devices.

Note: Sensor labels can be selected for the devices managed by a NetBotz Appliance, but not for the NetBotz Appliance itself.

Neither tab can be used until **Show Sensor Labels** is selected.

Default tab

Use this tab to select the default sensor for the **Map View** devices.

Note: Only the devices that report the sensor will show the value as a sensor label.

This tab lists all the sensors for every device in the selected device group's **Map View**. There may be more than one sensor of a given type, as different devices report different sensors. For example, the main input voltage sensor reported by a Smart-UPS is different than the main input voltage phase 1 sensor reported by a Symmetra PX. Thus, if you select main input voltage as the default sensor, only devices that have that exact sensor will report the value.

You can use the **Default** tab to select a different default sensor for the map at any time. Devices displaying the default sensor will update with the new default sensor except for the following:

- Devices that do not report the sensor value.
- Devices that have a different sensor defined on the **Selected** tab.
  Note: You can also use the **Selected** tab to select a new sensor label for one device, or set of devices, without affecting the sensor labels at any other devices.

Selected tab

Use this tab to select a sensor to be displayed as a label on a specific device or set of devices.

Note: When multiple devices are selected, if you choose a sensor that is not reported by one of the devices, that device will not show a sensor label in the **Map View**.

Element	Description
Devices	Lists the devices selected in the **Map View**.
No Changes	Select to make sure no changes are made to the sensor label settings.
Display the Default Sensor: <sensor_name>	Select the default sensor the **Map View** uses.
Chose a Specific Sensor	Select to chose a listed sensor for the selected devices.
Filter	Type in text to filter the **Sensor** list to include only those entries that include your text.
Sensor	Lists all sensors available to the device or devices selected in the **Map View**.

"View Device Sensors" display

Use this display to view sensor data on the selected device. This display can be accessed from the **Device View**, **Map View**, **Active Alarms** view, or **Alarm History** view.

Note: The **Hostname**, **Model**, **Last Contact**, and **Set** elements are not present when more than one device is selected in the **Device View** or **Map View**.

Type	Description
Hostname	Identifies the hostname or IP address of the selected device.
Model	Identifies the model of the selected device, when known.

Last Contact	Identifies when the InfraStruXure Central server last scanned the device for its sensor values.
Set	Select the set of logically grouped sensors you want to view. **Note:** Some devices have sensors that cannot be logically grouped in sets; they list their individual sensors, instead.
Search	Use to search the sensors and sensor values.
List	Shows the sensors and sensor values for the selected device or devices. **Note:** When multiple devices are selected, **Device Label** information is included to identify which device reports a sensor value.

Alarm views

Two views provide information about the alarms that occur at monitored devices, both of which can be accessed from Alarms in the Windows menu: **Active Alarms** view is part of the **Monitoring** perspective's default layout; **Alarm History** view also can be accessed by selecting **Show Alarm History**, a right-click menu option in the **Device View**, **Map View**, or **Device Groups** view.

Alarms displayed in the alarm views

The alarms listed in the alarm views (**Active Alarms** view or **Alarm History** view) depend on whether a device or set of devices are selected in the **Device View** or **Map View**, and, for some devices, whether an alert threshold related to an alarm has been defined at the InfraStruXure Central server.

- When no devices are selected in the **Device View** or **Map View**, the alarms for all devices in a group selected in the **Device Groups** view are listed in an alarms view.
- When a device or set of devices is selected in the **Device View** or **Map View**, only the alarms associated with that device or set of devices are listed in an alarms view.
- When an alert threshold has been defined at the InfraStruXure Central server for a sensor at an SNMP device, two alarms may be listed in an alarms view for the same sensor event:
  - An alarm sent to the InfraStruXure Central server by an SNMP device for a sensor threshold violation.
  - An alarm generated by the InfraStruXure Central server when the data it monitors for that SNMP device sensor violates the alert threshold setting defined at the server for that sensor.
    Note: Not all SNMP devices can send sensor alarms to the InfraStruXure Central server. Also, the sensor thresholds at SNMP devices are independent from the alert threshold settings at the InfraStruXure Central server. The sensor value that triggers a threshold violation at an SNMP device sensor may not trigger an alert threshold violation at the InfraStruXure Central server, and vice versa.

Active Alarms view

This view provides information about the alarms that are active for all devices in a selected device group, or for any device or set of devices selected in the **Device View** or **Map View**.

Button icons (Active Alarms view)

In addition to standard minimize and maximize icons, four icons are available to perform specific **Active Alarms** view functions.

Note: A **Graphing and Reporting** right-click option provides the same functionality as the **Custom Device Report** icon.

Icon	Description
»	Use the **Hide Alarm Details** icon to hide the **Alarm Details** section.
«	Use the **Show Alarm Details** icon to show the **Alarm Details** section.
📊	Use the **Custom Device Report** icon to create a report or graph for the historical values of sensors at devices associated with alarms selected in the alarms view (see Graphing and reporting feature).
▽	Use this **Menu** icon to identify the columns to be displayed in the active alarms list.

Active Alarms list

This **Active Alarms** view section lists active alarms for selected **Device Group** view, **Device View**, or **Map View** devices, and provides information about each alarm.

The view includes a search element that allows you to list only the alarms that match your typed text, and a table that provides information about those alarms.

Column	Description
Clip	Uses a camera icon (📷) to identify alarms that include a surveillance clip.
Description	Describes details for the alarm.
Severity	Describes the severity level associated with the alarm.
Device Hostname	Identifies the hostname or IP address of the device.
Time Occurred	Identifies when the alarm occurred.
Sensor	Identifies the sensor associated with the alarm, when an alert threshold setting is defined for the sensor's alarm. **Note:** For information about the alert threshold settings, see Alert Thresholds, under Alert Settings.

You can use the list, right-click options, and button icons to do the following:

- Select which columns appear in the list (**Menu** icon).
- Click a column title to sort the list in ascending or descending order based on that column's information.
- Access the "View Alarm Details" display for a selected alarm (**View Alarm Details** option, or double-click the alarm).
- Select an alarm in the list and select that device in the **Device View** (**Select Device** option).
- Generate a report for the historical values of the sensors at a selected alarm's device (**Custom Device Report** option or icon).
- View all the values being reported by the sensors at a selected alarm's device (**View Device Sensors** option).
- Log on to the web interface at a selected alarm's device, if it has one (**Launch to Device** option).

Alarm Details section

When displayed, this **Active Alarms** view section provides information about the alarm selected in the active alarms list: clicking the **Show/Hide Alarm Details** icon shows or hides the **Alarm Details** section.

Note: **View Alarm Details**, a right-click menu option in the **Active Alarms** list accesses a display that reports alarm details for a selected device, details that may include a graph and camera clips.

The alarm is identified at the top of the **Alarm Details** section.

Note: This section reports the information available to the InfraStruXure Central server for a device and its alarms. Some devices provide more information than others.

Information	Description
Sensor	The sensor associated with the alarm.
Type	The type of device.
Device	The label information for the device.
Device Location	The location of the device, when available.
Recommended Action	Information about how to clear the alarm, when available.

Alarm History view

This view provides information about the alarms that have occurred during a defined date range, for a selected device or set of devices. The alarms displayed can be active or resolved.

The **Alarm History** view can be accessed in several ways.
Note: The view's title will identify the selected devices or group. For example, **Alarm History for All Devices**, when the **All Devices** group in the **Device Groups** view was selected for the **Alarm History** view, or **Alarm History for Selected Devices**, when multiple devices in the **Device View** or **Map View** were selected for the **Alarm History** view.

- **Alarm History**, an **Alarms** option in the **Window** menu: lists alarms for the selected devices, whether that is all devices in the group selected in the **Device Groups** view, or the device or devices selected in the **Device View** or **Map View**.
  Note: This **Alarm History** option performs this function only when the **Alarm History** view is not currently open. Once that view is open, this option has no affect on that view.
- **Show Alarm History**, a right-click **Device Groups** view option: lists the alarms for all devices in the group selected in the **Device Groups** view.
- **Show Alarm History**, a right-click **Device View** and **Map View** option: lists the alarms for the device or set of devices selected in the view.
  Note: Once the alarms for a device, set of devices, or device group are listed in the **Alarm History** view, they will remain listed in that view until you select a different device, set of devices, or device group and click the associated **Show Alarm History** option.

The **Alarm History** view includes a **Search** text field that allows you to list only those alarms that include your typed text, a **From Date** and **to** date calendar control that allows you to define a new date range for the alarms, and a **Search** button you click to search for alarms associated with the new date range.

The **Alarm History** view also includes a table that provides information about the historical alarms for this view's selected devices.
Note: When you open this view, the date range is set for the last 24 hours by default.

Column	Description
Time Occurred	Identifies when an alarm occurred.
Time Resolved	Identifies when an alarm was resolved, unless it is still active.
Status	Identifies whether an alarm is **Active** or **Resolved**.
Clip	Uses a camera icon to identify alarms that include a surveillance clip.
Description	Describes details for the alarm.
Severity	Identifies the severity level associated with the alarm.
Device Hostname	Identifies the hostname or IP address of the device associated with the alarm.
Sensor	Identifies the sensor associated with the alarm, when an alert threshold setting is defined for the sensor's alarm. **Note:** For more information, see Alert Thresholds, under Alert Settings.

You can use the list, right-click options, and button icons, to do the following:

- Click a column title to sort the list in ascending or descending order based on that column's information.
- Access the "View Alarm Details" display for a selected alarm (**View Alarm Details** right-click option, or double-click the alarm).
- Select an alarm in the list and access the listing for its device in the **Device View** (**Select Device** right-click option).
- Generate a report or graph for the historical values of the sensors at a selected alarm's device (**Custom Device Report** right-click option).
- View all the values being reported by the sensors at a selected alarm's device (**View Device Sensors** right-click option).
- Log on to the web interface at a selected alarm's device, if it has one (**Launch to Device** right-click option).
- Export a copy of the list as a *.csv (the default selection) or *.txt file (**Export Alarm History** () icon).
- Scroll between multiple pages using standard scrolling elements (arrows and page number box).
  Note: A maximum of 500 alarm entries can be reported by a page, with additional pages provided for every additional 500 entries.

"View Alarm Details" display

Use this display, accessed by a **View Alarm Details** right-click option in the **Active Alarms** view and **Alarm History** view, to view **Details** for any active or historical alarm, as well as **Clip** and **Graph** data for that alarm, when available.

Note: The **Clip** option is available only for alarms that include a camera icon in the **Clip** column of an alarm list; the **Graph** option is available only for some of the alarms that list a sensor in the **Sensor** column of an alarms list, and unavailabe for alarms that have no sensor identified in the **Sensors** column.

Clip option

Use this option to view clips that were included with a selected alarm.

A tab identifies each camera that has a clip attached to the alarm. The clip is displayed in the upper portion of the tab, while icons used to view the clip's frames, and to export the clip, and information about the clip are provided in the lower portion.

Element	Description
View Pane	Shows the content of the clip.
Play (▶)/Pause (⏸) icons	Click the **Play** icon to start the clip; click the **Pause** icon to pause the playback on the current image. You may begin playing the clip during the load sequence, if you desire.
Clip slider bar	Drag the control left or right to find a specific frame within the clip. The number to the right of the bar shows the currently displayed frame. You also can click the up and down arrows to the right of the slider bar to advance or rewind the clip by a single frame. The beginning date, ending date, and time of the clip are displayed below the slider bar.
Export Clip icon (⇗)	Click this icon to access the "Export Clip" display. **Note:** For information about the "Export Clip" display, see "Recorded Camera Clips" display under Surveillance perspective.
Audio icon (🔈)	If there is audio associated with the current clip, the audio icon is displayed in black; if there is no audio, the icon is grayed out.
Digital Signature icon (✏)	If the clip has a digital signature associated with it, this icon is displayed in color; if the clip is unsigned, the icon is grayed out.
Status area	Displays the loading status of the selected clip: **Loading** or **Loading Complete**.
Clip information	Displays the following information about the current clip: • **Total Frame Count** • **Duration** • **Resolution**

Details option

Use this option to view information about a selected alarm.

Note: Three elements (**Resolved by**, **Resolved Comment**, and **Resolve Alarm**) are available only for an alarm that must be manually resolved because it is associated with a sensor alert threshold that has **Return-to-Normal Requires User Input** selected in its **Advanced** tab.

Element	Description
Sensor	The sensor associated with the alarm.
Type	The type of device.
Device	The label information for the device.
Device Location	The location of the device, when available.
Time Occurred	When the alarm occurred, by date and time.
Time Resolved	When the alarm was resolved, by date and time, or **Not Yet Resolved**, if still active.
Resolved by	The user who manually resolved an alarm using the "Resolve Alarm" display.
Resolved Comment	Any optional comment made in the "Resolve Alarm" display while manually resolving an alarm.
User-specified URL	The **User-specified URL** in the **Advanced** tab for the alert threshold setting associated with the alarm's sensor, when defined for that threshold. **Note:** For more information, see Alert Thresholds under Alert Settings (Settings menu).
User-specified Description	The **User-specified Description** in the **Advanced** tab for the alert threshold setting associated with the alarm's sensor, when defined for that threshold. **Note:** For more information, see Alert Thresholds under Alert Settings (Settings menu).
Recommended Action	Information about how to clear the alarm, when available.
Resolve Alarm	Click to use the "Resolve Alarm" display to manually resolve an alarm.

"Resolve Alarm" display

Use this display, accessed by the **Resolve Alarm** button for the **Details** option in the "View Alarm Details" display, to manually resolve alarms associated with sensor alert thresholds that have **Return-to-Normal Requires User Input** selected in that threshold's **Advanced** tab only.

Note: Alarms that are not associated with a sensor threshold that has **Return-to-Normal Requires User Input** selected cannot be manually resolved. For more information about the **Advanced** tab, and other threshold settings, see Alert Thresholds under Alert Settings.

You can add **Optional Comment** text before you click **OK** to resolve the alarm.

Graph option

Use this option to view a graph for an alarm associated with a numerical sensor (**Humidity**, **Air Flow**, **Temperature**, etc.).

Note: This is available only for some of the alarms that list a sensor in the **Sensor** column of an alarms list; it is unavailabe for alarms that have no sensor identified in the **Sensors** column.

Each graph has its value measurements labeled up the left side of the graph, and date and time values labeled across the bottom.

Device discovery processes

APC, MGE, NetBotz Appliances, and third-party devices are added to the list of devices that an InfraStruXure Central server monitors by creating and running device discovery processes. As devices are discovered, they are added to the **All Devices** and **Unassigned** device groups in the **Device Groups** view, and displayed in the **Device View** and **Map View** if one of those device groups is selected.

Separate discovery processes exist for each of the following types of devices:

- SNMPv1 devices: APC or third-party devices that use basic SNMP communications.
- SNMPv3 devices: APC or third-party devices that use secured SNMP communications.
- NetBotz Appliances (except for the 300, 303, 310, 400, and 410 models).

You can initiate a discovery process by accessing the "Device Discovery" wizard in the following ways:

- Select **Add Devices** in the **Edit** menu.
- Right-click on any device in the **Device View** or **Map View**, and select **Add Devices**.
- Click the green plus sign (+) icon in the **Device View**.
- Right-click anywhere in the **Saved Discovery** view, and select **Add**.
- Right-click on a discovery process listed in the **Saved Discovery** view, and select **Run**, to rerun that process, or **Edit**, to run an edited version.

Creating a discovery process

You can create discovery processes that can discover the SNMPv1 devices, SNMPv3 devices, or NetBotz Appliances on your networks.

1. Access the "Device Discovery" wizard.
   - Select **Add Devices** in the **Edit** menu.
   - Click the plus sign (+) icon in the **Device View**.
   - Right-click any device in the **Device View** or **Map View**, and select **Add Devices**.
   - Right-click anywhere in the **Saved Discoveries** view, and select **Add**.
2. In the "Choose Discovery Type" display, select the **Device Discovery Type** (**SNMPv1**, **SNMPv3**, or **NetBotz Appliance**), and click **Next**.
3. In the discovery settings display, define the settings to be used, and click **Next**, to schedule or run (or both) the process, or **Finish**, to add the process to the **Saved Discoveries** view without running or scheduling the process.
   - "SNMPv1 Discovery Settings" display:
     1. **IP Range**: the IP addresses the discovery process will search.
     2. **Port**: the port number that the SNMPv1 devices use for communication.
     3. **Timeout**: how long the InfraStruXure Central server will wait for a response, in seconds, when it polls an IP address before it considers the poll failed.
     4. **Retries**: how many times the InfraStruXure Central server will attempt to communicate with a device at an IP address, after the initial failure, before it stops trying to access a device at that address.
     5. **Read Community**: the community name used to read information at the SNMPv1 devices.
     6. **Register for Priority Scanning**: enables the InfraStruXure Central server to be defined as a trap receiver at discovered devices.
     7. **Read Community**: the community name used to register as a trap receiver at an SNMPv1 device.
   - "SNMPv3 Discovery Settings" display:

1. **IP Range**: the IP addresses the discovery process will search.
2. **Username**: the username used for secure communication with discovered SNMPv3 devices.
3. **Authentication Type/ Password**: the authentication protocol and password.
4. **Encryption Type/ Password**: the encryption method and password.
5. **Port**: the port number that the SNMPv3 devices use for communication.
6. **Timeout**: how long the InfraStruXure Central server will wait for a response, in seconds, when it polls an IP address before it considers the poll failed.
7. **Retries**: how many times the InfraStruXure Central server will attempt to communicate with a device at an IP address, after the initial failure, before it stops trying to access a device at that address.
8. **Register for Priority Scanning**: enables the InfraStruXure Central server to be defined as a trap receiver at discovered devices.

- "NetBotz Appliance Discovery Settings" display:
  1. **IP Range**: the IP addresses the discovery process will search.
  2. **Port**: the port used for communication with the NetBotz Appliances.
  3. **Security Mode**: the security mode used for communication with the NetBotz Appliances.
  4. **Credentials**: accesses a display used to manage the credentials that can be used to communicate with NetBotz Appliances.

4. In the "Discovery Scheduling" display, do one or both of the following actions, and click **Finish**, to add the process to the **Saved Discoveries** view.
   - Use the **Enable discovery scheduling** option to schedule the days and times when the discovery process will be run automatically.
   - Use the **Run discovery now** option to run the discovery process when you click **Finish**.

Editing a device discovery process

You can edit the discovery settings and scheduling for any SNMPv1 devices, SNMPv3 devices, or NetBotz Appliances discovery process listed in the **Saved Discoveries** view. You cannot edit the type of device the process will discover.

The difference in the three types of discovery processes is the type of settings used to define the process.

1. Select **Saved Discoveries** view, a **Device** option in the **Window** menu, to access the **Saved Discoveries View**.
2. Right-click a listed discovery process and select **Edit**.
3. In the discovery settings display, edit the settings, as appropriate, and click **Next**, to change the scheduling or run (or both) the edited process, or **Finish**, to save the changes in the **Saved Discoveries** view without running or scheduling the process.
   - "SNMPv1 Discovery Settings" display:
     1. **IP Range**: the IP addresses the discovery process will search.
     2. **Port**: the port number that the SNMPv1 devices use for communication.
     3. **Timeout**: how long the InfraStruXure Central server will wait for a response, in seconds, when it polls an IP address before it considers the poll failed.
     4. **Retries**: how many times the InfraStruXure Central server will attempt to communicate with a device at an IP address, after the initial failure, before it stops trying to access a device at that address.
     5. **Read Community**: the community name used to read information at the SNMPv1 devices.
     6. **Register for Priority Scanning**: enables the InfraStruXure Central server to be defined as a trap receiver at discovered devices.
     7. **Read Community**: the community name used to register as a trap receiver at an SNMPv1 device.

- "SNMPv3 Discovery Settings" display:
    1. **IP Range**: the IP addresses the discovery process will search.
    2. **Username**: the username used for with discovered SNMPv3 devices.
    3. **Authentication Type/ Password**: the authentication protocol and password.
    4. **Encryption Type/ Password**: the encryption method and password.
    5. **Port**: the port number that the SNMPv3 devices use for communication.
    6. **Timeout**: how long the InfraStruXure Central server will wait for a response, in seconds, when it polls an IP address before it considers the poll failed.
    7. **Retries**: how many times the InfraStruXure Central server will attempt to communicate with a device at an IP address, after the initial failure, before it stops trying to access a device at that address.
    8. **Register for Priority Scanning**: enables the InfraStruXure Central server to be defined as a trap receiver at discovered devices.
- "NetBotz Appliance Discovery Settings" display:
    1. **IP Range**: the IP addresses the discovery process will search.
    2. **Port**: the port used for communication with the NetBotz devices.
    3. **Security Mode**: security mode used for communication with the NetBotz Appliances.
    4. **Credentials**: accesses a display that lists credentials that can be used to communicate with NetBotz Appliances, and allows you to manage (edit, create, or delete) the credentials.

4. In the "Discovery Scheduling" display, do one or both of the following actions, and click **Finish**, to add the process to the **Saved Discoveries** view.
    - Use the **Enable discovery scheduling** option to schedule the days and times when the discovery process will be run automatically.
    - Use the **Run discovery now** option to run the discovery process when you click **Finish**.

"Device Discovery" wizard

Use this wizard to create, edit, and run the processes used to discover devices the InfraStruXure Central server can monitor.

You can run a discovery process once, rerun that process whenever you want, or schedule that process to run periodically.

To access the "Device Discovery" wizard, do one of the following actions.

- Select **Add Devices** in the **Edit** menu.
- Right-click on any device in the **Device View** or **Map View**, and select **Add Devices**.
- Click the green plus sign (+) icon in the **Device View**.
- Right-click anywhere in the **Saved Discovery** view and select **Add**.
- Right-click on a discovery process listed in the **Saved Discovery** view and select **Run**, to rerun that process, or **Edit**, to run an edited version.

How you use this wizard will depend, in part, on the type of devices you want to discover: SNMPv1, SNMPv3, or NetBotz Appliances.

"Choose Discovery Type" display

Use this display to select the type of device to be discovered.

Option	Description
SNMPv1	Select to discover devices that use standard SNMP communication.

SNMPv3	Select to discover devices that use secure SNMP communication.
NetBotz Appliances	Select to discover NetBotz Rack or Wall Appliances (except for 300, 303, 310, 400, and 410 models).

"SNMPv1 Discovery Settings" display

Use this display to define the settings used to discover SNMPv1 devices.

Element	Description
IP Range	Define the IP addresses the discovery process will search for SNMPv1 devices. For example: **xxx.xxx.12.6**: searches a single IP address. **xxx.xxx.10-13.20-80**: searches a specific set of IP addresses (20 through 80) at the 10, 11, 12, and 13 subnets. **xxx.xxx.14.***: searches all IP addresses at subnet 14.
SNMPv1 Settings	**Port**: define the port number that the SNMP devices use for communication (**161**, by default). **Timeout**: define how long the InfraStruXure Central server will wait for a response, in seconds, when it polls an IP address before it considers the poll failed (**1**, by default). **Retries**: define how many times the InfraStruXure Central server will attempt to communicate with a device at an IP address, after the initial failure, before it stops trying to access a device at that address (**5**, by default). **Read Community**: define the community name to be used to read information at the SNMP devices (**public**, by default).
Trap Registration	**Register for Priority Scanning**: select to have the InfraStruXure Central server registered as a trap receiver at discovered devices. **Write Community**: identify the community name used to register as a trap receiver at an SNMPv1 device.

"SNMPv3 Discovery Settings" display

Use this display to define the settings used to discover SNMPv3 devices.

Element	Description
IP Range	Define the IP addresses the discovery process will search for SNMPv3 devices. For example:

	xxx.xxx.12.6: searches a single IP address. **xxx.xxx.10-13.20-80**: searches a specific set of IP addresses (20 through 80) at the 10, 11, 12, and 13 subnets. **xxx.xxx.14.***: searches all IP addresses at subnet 14.
SNMPv3 Settings	**Username**: Define the username used for secure communication with discovered SNMP devices. **Authentication Type**/ **Password**: select the authentication protocol (**None**, **MD5** or **SHA**) and password used with that protocol. **Encryption Type**/ **Password**: select the encryption method (**None**, **DES**, or **AES-128**) and password used with the **DES** or **AES-128** method. **Port**: define the port number that the SNMP devices use for communication (**161**, by default). **Timeout**: define how long the InfraStruXure Central server will wait for a response, in seconds, when it polls an IP address before it considers the poll failed (**2**, by default). **Retries**: define how many times the InfraStruXure Central server will attempt to communicate with a device at an IP address, after the initial failure, before it stops trying to access a device at that address (**3**, by default).
Trap Registration	**Register for Priority Scanning**: select to have the InfraStruXure Central server register itself as a trap receiver at discovered devices.

"NetBotz Appliance Device Discovery Settings" display

Use this display to define the settings used to discover NetBotz Appliances.

Element	Description
IP Range	Define the IP addresses the discovery process will search for NetBotz Appliances. For example: **xxx.xxx.12.6**: searches a single IP address. **xxx.xxx.10-13.20-80**: searches a specific set of IP addresses (20 through 80) at the 10, 11, 12, and 13 subnets. **xxx.xxx.14.***: searches all IP addresses at subnet 14.
Port Range	Define the range or port numbers that the discovery process will use to communicate with NetBotz Appliances (**80**, by default). For example:

	80: uses port 80 only. **60-80**: uses ports 60 through 80, inclusive.
Security Mode	Select how the Secure Sockets Layer (SSL) protocol to use for communication with NetBotz Appliances: **None** **Try SSL, fall back to none** **Require SSL, no certificate validation** **Require SSL, validate certificates**
NetBotz Appliance Credentials	Click to use **NetBotz Appliance Credentials**, a **Server Administration Settings** option in the **Settings** menu, to manage the credentials the InfraStruXure Central server uses for communication with NetBotz Appliances.

"Discovery Scheduling" display

Use this display to schedule a discovery process to run periodically, to run a discovery process when you are done defining that process, or both.

Option	Description
Enable discovery scheduling	Select to schedule when a discovery process will run automatically, by the day, or days, of the week, and time of day.
Run discovery now	Select to run the discovery process when you exit the wizard.

Saved Discoveries view

When you create a device discovery process, information about that process is listed in this view.

Note: Wait a few minutes after a discovery process reports it is idle before you consider that it failed to discover all the devices it should have. The InfraStruXure Central server can take more time to list discovered devices in the **Unassigned** group in the **Device Groups** view, than it takes the discovery process to discover those devices.

Column	Description
IP Range	The IP addresses the discovery process will search for devices.
Run Periodically	Whether the process is scheduled to run periodically: **Yes** or **No**.
Type	The devices the process will discover: **SNMPv1**, **SNMPv3**, or **NetBotz Appliance**.
Activity	Whether the discovery process is running or idle.
Last Run	The time at which the last discovery process finished.

This **Saved Discoveries** view also has right-click menu options and button icons that manage the discovery processes.

Option	Description
Add	Accesses the "Device Discovery" wizard to create a new discovery process.
Edit	Accesses the "Device Discovery" wizard to edit a selected discovery process.
Delete	Deletes a selected discovery process.
Run	Runs a selected discovery process.
Stop	Stops a selected discovery process, when that process is running.

Device firmware and server updates

The **Updates** menu provides options you can use to update the InfraStruXure Central server, or to download firmware updates from APC, and then use FTP, to upload them to the network management cards (NMCs) at monitored APC SNMP devices, or HTTP/HTTPS, to upload them to monitored NetBotz Appliances.

Schedule Update Checks (Updates menu)

Use this display to schedule when the InfraStruXure Central server will check the APC updates server for firmware updates that can be used for its monitored devices, either on a one-time or recurring basis.

Available firmware updates are downloaded to the server, and listed in the "Load Firmware Updates" display in the "Update Device Firmware" wizard.
Note: A message near the bottom of the display can report when the next scheduled update check will occur, or that the checking service is disabled.

Type	Description
Check for Updates	Select to use the **Date**, **Time**, and **Recurrence** settings to schedule update checks.
Date	Define the date when the update check will occur.
Time	Define the time of day that update check will occur.
Recurrence	Define how often the update check will occur, either **Once**, at the defined date and time, or recurring **Daily**, **Weekly**, or **Monthly**, starting at the defined date and time.

Status messages: "Schedule Update Checks" display

Four different status messages can appear when you use the display for **Schedule Update Checks** in the **Settings** menu.

Message	Description
The next update check is set to occur on <Date> at <Time>.	Reports the date and time for the next scheduled update check. **Recommended Action**: None
The scheduled update checking service is disabled.	The **Check for Updates** option is not selected. **Recommended Action**: Select to enable scheduling.

Message	Description
Unable to schedule the specified update check.	An unexpected server error occurred. **Recommended Action**: Try again. If the problem persists, contact APC Support (http://www.apc.com/support).
Cannot schedule the updates check. Based on the server's time settings, the selected time is in the past.	You attempted to use an invalid date or time to schedule a check for updates. **Recommended Action**: Use a time setting that is in the future.

Apply Firmware Updates (Updates menu)

Use this option to update the firmware at NetBotz Appliances, using HTTP/HTTPS, or at SNMP devices, using FTP.

Performing a firmware update

You use the "Update Device Firmware" wizard to update firmware at the InfraStruXure Central server's monitored SNMP devices, using FTP, and NetBotz Appliances, using HTTP/HTTPS.

1. In the **Updates** menu, select **Apply Firmware Updates**.
2. In the "Select Update Type" display, select to perform an **APC SNMP Device Update** or **NetBotz Appliance Update**.
3. In the "Load Firmware Updates" display, do one of the following, depending on whether the InfraStruXure server has internet access.
   - Internet access available: click **Check Updates** to check if an any appropriate updates (SNMP devices or NetBotz Appliances) are available from the APC updates server that are more recent than the catalog, if any, currently installed at the InfraStruXure Central server.
   - Internet access unavailable: use the Importing the APC updates catalog task to import the SNMP devices or NetBotz Appliance catalog at the InfraStruXure Central server.
4. In the "Load Firmware Updates" display, click **Next**.

   Note: If no updates are available, click **Finish**.
5. In the "Select Device Updates" display, select the devices you want to update from the devices listed for each available firmware update, and click **Next**.
6. In the "Device FTP Settings" display (SNMP devices) or "Global NetBotz Appliance Credentials" display (NetBotz Appliances), add new settings, or edit existing settings, as needed, and click **Finish**.

   Note: Two options in the Settings menu allow you to manage the FTP and global credentials without accessing this "Apply Firmware Updates" wizard: **Device FTP Settings**, an **SNMP Device Settings** option in the **Settings** menu, and the **NetBotz Appliance Credentials** option in the "Server Administration Settings" display accessed by **Server Administration Settings** in the **Settings** menu.
7. In the **Window** menu, select the appropriate **Firmware Updates** option (**SNMP Device Update Status** or **NetBotz Appliance Update Status**).
8. In the update status view, review the progress for the selected updates.

Importing the APC updates catalog

You can download a copy of the appropriate APC updates catalog (SNMP device or NetBotz Appliance) to your client, and then import that catalog to the InfraStruXure Central server, when that server does not have internet access to the APC updates server.

Note: This procedure assumes your client has internet access to the APC updates server. If not, you will need to download the updates catalog to a machine that does have access, and transfer the file to your client.

1. Access the **Software/Firmware** download page (http://apc.com/tools/download).
2. In the **Filter by Software/Firmware** list, select **Firmware Upgrades - Updates Catalog** and click **Submit**.
3. In the appropriate updates catalog listing (SNMP device or NetBotz Appliance), click **Continue**.
4. In the **APC Login/Registration** page, click **Login**, if you are already registered, or **Register**, to register.
5. In the **Personal Login** page, log in.
6. In the **Software/Firmware** download page, click **Download Now**.
7. Once the updates catalog is downloaded, select **Apply Firmware Updates** in the InfraStruXure Central server's **Updates** menu.
8. In the "Select Update Type" display, select to perform an **APC SNMP Device Update** or **NetBotz Appliance Update**.
9. In the "Load Firmware Updates" display, click **Import**.
10. In the "Open" display, browse to the downloaded APC updates catalog, and click **Open**.
11. Go to step 5 of the Performing a firmware update task to update devices using the imported APC updates catalog.

"Apply Firmware Updates" wizard

Use this wizard to update firmware at the InfraStruXure Central server's monitored SNMP devices, using FTP, and NetBotz Appliances, using HTTP/HTTPS.

Note: Once you initiate a firmware update, you can access status information about the updates using the appropriate **Firmware Updates** option in the **Window** menu (**SNMP Device Update Status** or **NetBotz Appliance Update Status**).

"Select Update Type" display

Use this display to select to perform either an **APC SNMP Device Update** or **NetBotz Appliance Update**.

"Load Firmware Updates" display

Use this display to download firmware updates that are available from the APC updates server directly, when the InfraStruXure Central server (for SNMP device updates) or InfraStruXure Central client (for NetBotz Appliance updates) has internet access, or to upload a copy of the APC updates catalog to the server from your client when the server has no internet access.

Note: For information about the difference in the activity that occurs based on whether the InfraStruXure Central server (SNMP devices) or InfraStruXure Central client (NetBotz Appliances) is driving the firmware updates, see the status message descriptions.

Element	Description
List	Lists the updates that have been downloaded to the server (**Update**), and identifies how many of the server's monitored devices (**Device Count**) can use each update.
Check Updates	Click to download any firmware updates available from the APC updates server for the InfraStruXure Central server's monitored devices, when the server has internet access.
Import	Click to import the APC updates catalog to the server from your client, when the server that has no internet access. **Note:** A copy of the APC updates catalog zip file must already be downloaded to your client from APC.

Status messages: SNMP device load firmware updates:

The status messages that can appear when you use the "Load Firmware Updates" display for SNMP device updates depend on whether you click **Check Updates** or **Import** to provide firmware updates to the InfraStruXure Central server.

Check Updates status messages:

The following status messages can appear when checking the APC updates server for firmware updates for the InfraStruXure Central server's monitored devices.

Message	Description
Checking for firmware updates...	The InfraStruXure Central server is checking the APC updates server for firmware updates. **Recommended Action**: None
Contacting the APC update server...	The server is attempting to connect to the APC updates server. **Recommended Action**: None
Firmware update download in progress...	The server is downloading all available firmware updates from the APC updates server. **Recommended Action**: None
Firmware updates are available.	All available firmware updates have been downloaded to the server, and listed in the table. **Recommended Action**: None
Found firmware updates on the server.	At least one firmware update is available at the APC updates server. **Recommended Action**: None
No firmware updates are available.	No updates are available for any devices the server is monitoring. **Recommended Action**: None

Message	Description
Unable to access the APC update server.	This is basically a network issue. No access to the apc update server. **Recommended Action**: Make sure the server has access to the internet. If no internet access is available to the server, you can use your client to download a copy of the APC updates catalog, and then load it at the server.

Import status messages:

The following status messages can appear when attempting to import an APC updates catalog to the InfraStruXure Central server from your InfraStruXure Central client.

Message	Description
There was an error retrieving the device firmware updates.	A server error occurred. **Recommended Action**: Make sure that the zip file you selected to import to the InfraStruXure Central server from your client is for the APC update catalog. If it is the update catalog file, and the problem persists, contact APC Support (http://www.apc.com/support).
There was an error sending the device firmware updates to the server.	A server error occurred. **Recommended Action**: If the problem persists, contact APC Support (http://www.apc.com/support).

Status messages: NetBotz Appliance load firmware updates:

The status messages that can appear when you use the "Load Firmware Updates" display for NetBotz Appliance updates depend on whether you click **Check Updates** or **Import** to provide firmware updates for the monitored NetBotz Appliances.

Check Updates status messages:

The following status messages appear when using your InfraStruXure Central client to checking the APC updates server for NetBotz Appliance updates that can be uploaded to the InfraStruXure Central server.

Message	Description
Checking for NetBotz Appliance updates...	The InfraStruXure Central client is checking for NetBotz Appliance updates at the APC updates server. **Recommended Action**: None

Message	Description
Uploading the NetBotz Appliance updates...	The client is transferring the NetBotz Appliance updates from the APC updates server to the InfraStruXure Central server. **Recommended Action**: None
Installing the NetBotz Appliance updates...	The client is installing the NetBotz Appliance updates at the InfraStruXure Central server. **Recommended Action**: None
Reviewing the NetBotz Appliance updates...	The client is reviewing the firmware currently used by the NetBotz Appliances monitored by the InfraStruXure Central server to identify which of those appliances can use the newly installed updates. **Recommended Action**: None

Import status messages:

The following status message can appear when attempting to import an APC updates catalog to the InfraStruXure Central server.

Message	Description
There was an error retrieving the device firmware updates.	A server error occurred. **Recommended Action**: Make sure that the zip file you selected to import to the InfraStruXure Central server from your client is for the APC update catalog; if it is, contact APC Support (http://www.apc.com/support).

"Select Device Updates" display

Use this display to select the NetBotz Appliances or SNMP devices at which you want to perform a firmware update.

Element	Description
List	Use this list, which identifies the available updates, and the appliances or devices that can use each, to select the ones you want to update. To select all devices listed for an available update, select the update. To select some, but not all, select the device or devices, but not the update.
Select/Deselect All	Select all the devices for all the updates.

Logon-access displays

The "Apply Firmware Updates" wizard has two displays available for logon-access settings, one for FTP access to SNMP devices, and one for the global credentials used to access NetBotz Appliances.

"Device FTP Settings" display:

Use this display to manage the FTP access values the InfraStruXure Central server uses to log on at SNMP devices during firmware updates.

FTP must be enabled at a device, and the correct FTP username and password for that device must be used, before firmware can be downloaded to that device. By default, the InfraStruXure Central server can download firmware only to devices that use **apc** (lowercase) for the FTP username and FTP password.

Note: Identical versions of this display are available as part of the "SNMPv1 Device Discovery" and "Apply Firmware Updates" wizards, as well as for **Device FTP Settings**, an **SNMP Device Settings** option in the **Settings** menu. A change saved in one display is reflected in all.

Element	Description
List	Lists the access settings the InfraStruXure Central server can use for FTP access to its monitored devices. **Username**: The username used for FTP access to a device. **Port**: The port used for FTP access to a device. **Timeout**: How long the server will wait before it considers that an attempt to access a device has failed. **Retry Limit**: How many times the server will attempt to access a device before it stops trying to access a device. **Note:** The password required for FTP access is listed in the "Edit Device FTP Settings" display.
Add	Click to add an access setting to the list.
Edit	Click to edit a selected access setting.
Remove	Click to delete a selected access setting.

"Edit Device FTP Settings" display:

Use this display to add or edit access settings the InfraStruXure Central server can use for FTP access to monitored SNMP devices.

Note: This display can be accessed from the "Device FTP Settings" displays used by the "Apply Firmware Updates" and "SNMPv1 Device Discovery" wizards, and by **Device FTP Settings**, an **SNMP Device Settings** option in the **Settings** menu.

Element	Description
Username	Identify the name used for FTP access to a device.
Password	Identify the password used for FTP access to a device.
Verify Password	Retype the password.
Port	Select the port the server will use for FTP communication with devices.
Timeout	Identify how long the server will wait before it considers that an attempt to access a device has failed.Click to edit a selected access setting.
Retry Limit	Select the number of times the server will attempt to access a device before it stops trying to access a device.

"NetBotz Appliance Credentials" display:

Use this display to manage the list of credentials used for communication with the NetBotz Appliances.

Note: This display uses the same elements as **NetBotz Appliance Credentials**, a **Server Administration Settings** option in the **Settings** menu. A change made to either, affects both.

Element	Description
List	Lists the available credentials, and identifies **Username**, **Password**, **IP Range**, and **Port Range** values for each. **Note:** A default **NetBotz** credential is provided, as well as a default **APC** credential used to communicate with NetBotz Appliances on the private LAN.
Add	Click to add a new credential.
Edit	Click to edit a selected credential.
Remove	Click to remove a selected credential.

"Add/Edit Credentials" display:

Use this display to add or edit the credentials used for communication with the NetBotz Appliances.

Note: This display is accessed from the "NetBotz Appliance Credentials" display in the "Apply Firmware Updates" wizard, and from the **NetBotz Appliance Credentials** option in the "Server Administration Settings" display.

Element	Description
Username	Identify the username a credential will use to access NetBotz Appliances.
Password	Identify the password a credential will use to access NetBotz Appliances.
Verify Password	Retype the password.

IP Range	Define the range of IP addresses at which the credential can be used to communicate with NetBotz Appliances. For example: **xxx.xxx.12.6**: assigns a credential to a single IP address. **xxx.xxx.10-13.20-80**: assigns a credential to a specific set of IP addresses (20 through 80) at the 10, 11, 12, and 13 subnets. **xxx.xxx.14.***: assigns a credential to all IP addresses at subnet 14.
Port Range	Define the range of ports that a credential uses to access NetBotz Appliances. For example: **80**: uses port 80 only (the default value). **60-80**: uses ports 60 through 80, inclusive.

Status messages: Logon-access displays:

Four status messages can appear when you click **Finish** in the logon-access displays, two for the "Device FTP Settings" display, and two for the "NetBotz Appliance Credentials" display.

"Device FTP Settings" display messages:

For SNMP device updates, when you click **Finish**, the InfraStruXure Central server begins an update process that will update all selected devices.

Message	Description
There was an error starting the device firmware update.	An unknown error occurred. **Recommended Action**: Try again to update the device firmware. If the problem persists, contact APC Support (http://www.apc.com/support).
Unable to start a device firmware update, because an update is already in progress. Would you like to view the status of the update?	At least one firmware update is in progress. **Recommended Action**: Wait until the **SNMP Device Update Status** view reports that all the current updates have finished, and try again.

"NetBotz Appliance Credentials" display messages:

For NetBotz Appliance updates, when you click **Finish**, the InfraStruXure Central client directs the InfraStruXure Central server to transfer one NetBotz Appliance update at a time.

Message	Description
There was an error starting a NetBotz Appliance firmware update. Would you like to continue updating the rest of the appliances?	An unknown error occurred while other NetBotz Appliance updates are waiting to be started. **Recommended Action**: Click **Yes**, to continue with the NetBotz Appliances updates, or **No**, to stop.

	If you stop the updates, or after the last update has started, try again to update the NetBotz Appliance for which an error occurred. If the problem persists, contact APC Support (http://www.apc.com/support).
There was an error starting a NetBotz Appliance firmware update.	An unknown error occurred while no other NetBotz Appliance updates are waiting to be started. **Recommended Action**: Try again to update the NetBotz Appliance. If the problem persists, contact APC Support (http://www.apc.com/support).

Firmware update status views

Two update status views are available using the **Firmware Updates** options in the **Window** menu, one for the **SNMP Device Update Status** view, and one for the **NetBotz Appliance Update Status** view.

Note: Both views provide the same information about their related updates, with one exception: only the **SNMP Device Update Status** view identifies the operating system (**OS**) number of the update. Each view reports its own status messages.

Element	Description
List	Provides information about the update at each device selected for a firmware updates process, either an ongoing process, or the last process performed. **Hostname**: the device hostname or IP address **Model**: device model **Location**: location information for the device **Status**: status of the update **App Version**: application (App) version number of the update **OS Version**: operating system (OS) version number of the update **Note:** Reported for SNMP device updates only. **Time Completed**: when the update finished
Firmware Update Progress	Identifies the number of **Updates in progress**, **Updates completed**, and **Successful updates**.
Cancel Pending Updates	Click to cancel pending SNMP device updates. **Note:** The InfraStruXure Central server can process SNMP device updates for up to 20 devices at a time. This button appears in the **SNMP Device Update Status** view only, and only when more than 20 devices were selected to be updated.

	For example, if 77 devices are selected, **Cancel Pending Updates** appears in the **SNMP Device Update Status** view when the first set of 20 devices begins to be processed. You can click **Cancel Pending Updates** at this point to cancel the remaining 57 updates. If you chose not to cancel the pending updates, the button remains in the view while the second and third sets of 20 devices are processed, and disappears when the last set of 17 devices begins to be processed.

Status messages: SNMP Device Update Status view

Several different status messages can be reported in this view for SNMP device updates initiated by using **Apply Firmware Updates** in the **Updates** menu.

Message	Description
<Cancelled count> firmware updates have been cancelled.	The number of pending firmware updates that were cancelled. **Recommended Action**: None
Attempting to connect to the device...	The server is trying to connect to the device. **Recommended Action**: None
Attempting to log on to the device...	The server is trying to log on to the device. **Recommended Action**: None
Failed to update device: file verification failed for <file type> <file version>.	A problem occurred, after the server transferred the update to the device successfully, that prevented the server from verifying that the update at the device matches the update sent to the device. **CAUTION:** The device will not function correctly if the update at the device does not match the update update from the server. **Recommended Action**: Make sure the access settings have not changed at the server or device, and the FTP service is still enabled at the device. Make sure the device has not been turned off or disconnected from the network. Correct any network connection problem. If the problem persists, contact APC Support (http://www.apc.com/support). **Note:** Once the problem is corrected, select **Apply Firmware Updates** in the **Updates** menu to update the device.

Message	Description
Failed to update device firmware.	An unknown error occurred. **Recommended Action**: Make sure the device is turned on and online, the device's FTP service is enabled, and that the "Device FTP Settings" display settings are correct. Correct any network connection problem. If the problem persists, contact APC Support (http://www.apc.com/support).
Failed to update the device: unable to connect.	A network or FTP communication problem exists. **Recommended Action**: Make sure the device is turned on and online, the device's FTP service is enabled, and that the "Device FTP Settings" display settings used to access the device include the device's correct FTP port number. Correct any network connection problem. If the problem persists, contact APC Support (http://www.apc.com/support). **Note:** Once the problem is corrected, select **Apply Firmware Updates** in the **Updates** menu to update the device.
Failed to update device: unable to log on.	The server does not have the FTP access settings needed to log on to the device, or communication was lost after the connection was successful. **Recommended Action**: Make sure the access settings needed to log on to the device are defined in the "Device FTP Settings" display, and the FTP service is still enabled at the device. Make sure the device has not been turned off or disconnected from the network. Correct any network connection problem. If the problem persists, contact APC Support (http://www.apc.com/support). **Note:** Once the problem is corrected, select **Apply Firmware Updates** in the **Updates** menu to update the device.
Failed to update device: unable to transfer <file type> <file version>.	A problem occurred, after the server logged on to the device successfully, that prevented the server from transferring the update. **Recommended Action**: Make sure the access settings have not changed at the server or device, and the FTP service is still enabled at the device. Make sure the device has not been turned off or disconnected from the network. Correct any network connection problem.

Message	Description
	If the problem persists, contact APC Support (http://www.apc.com/support). **Note:** Once the problem is corrected, select **Apply Firmware Updates** in the **Updates** menu to update the device.
Successfully connected to the device.	Now the server can attempt to log on to the device. **Recommended Action**: None
Successfully logged on to the device.	Now the server can attempt to transfer the update to the device. **Recommended Action**: None
Successfully transferred <file type> <file version> to the device.	Now the server can attempt to verify that the update at the device matches the file used for the update. **Recommended Action**: None
Transferring <file type> <file version> to the device...	The server is trying to transfer the update to the device. **Recommended Action**: None
Unable to log on to the device: waiting to retry...	The server has failed at least one attempt to log on to the device, but has not reached its retry limit. **Recommended Action**: None
Unable to transfer <file type> <file version>: waiting to retry...	The server has failed at least one attempt to transfer the update to the device, but has not reached its retry limit. **Recommended Action**: None
Unable to verify <file type> <file version>: waiting to retry...	The server has failed at least one attempt to verify the update at the device matches the update sent by the server, but has not reached its retry limit. **Recommended Action**: None
Update cancelled.	The update was cancelled. **Recommended Action**: None
Update completed successfully.	The update was successful. **Recommended Action**: None
Update pending...	An update is pending, but not started. **Recommended Action**: None
Update started...	An update has started. **Recommended Action**: None
Verifying transfer of <file type> <file version> to the device...	The server is trying to verify that the update at the device matches update sent by the server. **Recommended Action**: None

Message	Description
Verified update to <file type> <file version>.	The server verified that the update at the device matches the update sent by the server. **Recommended Action**: None
Waiting for <file type> <file version> to load...	The server is waiting for the device to restart, using the update that was transferred. **Recommended Action**: None
Would you like to cancel the pending firmware updates?	You have selected to cancel at least one pending update. **Recommended Action**: Click **Yes** to continue with the cancellation.

Status messages: NetBotz Appliance Update Status view

Several different status messages can be reported in this view for NetBotz Appliance updates initiated by selecting **Apply Firmware Updates** in the **Updates** menu.

Message	Description
Failed to update device firmware.	An unknown error occurred. **Recommended Action**: Make sure the NetBotz Appliance is turned on and online, its HTTP or HTTPS web service is enabled, and the "Global NetBotz Appliance Credentials" display in the "Update Device Firmware" wizard includes the correct **IP Address**, **Port**, **Username**, and **Password** settings. Correct any network connection problem. If the problem persists, contact APC Support (http://www.apc.com/support).
Failed to update the device: unable to connect.	A network or HTTP/HTTPS communication problem exists. **Recommended Action**: Make sure the NetBotz Appliance is turned on and online, its HTTP or HTTPS web service is enabled, and the "Global NetBotz Appliance Credentials" display in the "Update Device Firmware" wizard includes its correct IP address and port settings. Correct any network connection problem. If the problem persists, contact APC Support (http://www.apc.com/support).

Message	Description
	Note: Once the problem is corrected, select **Apply Firmware Updates** in the **Updates** menu to update the device.
Failed to update device: unable to log on.	The server does not have the FTP access settings needed to log on to the device, or communication was lost after the connection was successful. **Recommended Action**: Make sure the "Global NetBotz Appliance Credentials" display in the "Update Device Firmware" wizard includes the correct **Username** and **Password** for the NetBotz Appliance. Make sure the device has not been turned off or disconnected from the network. Correct any network connection problem. If the problem persists, contact APC Support (http://www.apc.com/support). **Note:** Once the problem is corrected, select **Apply Firmware Updates** in the **Updates** menu to update the device.
Transferring update... ({0}%	The update is being transferred, with how much of the transfer has occurred reported as a percentage.
Update completed successfully.	The update was successful. **Recommended Action**: None
Update pending...	The update is pending, but not started. **Recommended Action**: None
Update started...	The update has started. **Recommended Action**: None
Waiting for NetBotz Appliance to load update...	The update still needs to be loaded at the NetBotz Appliance. **Recommended Action**: None

Apply Server Update (Updates menu)

Use this option to update your InfraStruXure Central server when a new version becomes available.

Performing a server update

You use the "Update Device Firmware" wizard to update firmware at the InfraStruXure Central server's monitored SNMP devices, using FTP, and NetBotz Appliances, using HTTP/HTTPS.

1. Before beginning this procedure, you must have recieved an update notification from APC Support, and contacted them to download the appropriate update file.
2. In the **Updates** menu, select **Apply Server Updates**.
3. In the "Apply Server Update" display, click the **Import** button and navigate to the downloaded *.lst file. Click **Open** to list the available updates in the display.
4. Highlight the desired update and click **Install Update**. A dialog opens that states "Installing this InfraStruXure Central update will cause the server to reboot. Would you like to continue?"
5. Click **Yes** to confirm your selection and begin the update process.
6. When the update is complete, users attempting to log in will recieve a message stating that the client and server are different versions. A link will be provided to download the updated client from the InfraStruXure Central server. Click the link to display the download page for the updated client.
7. Download and install the new client and log in to the updated server.
8. Open the **Help** menu and select the **About InfraStruXure Central** menu item. The display should reflect the new server version.

Device groups feature

InfraStruXure Central allows you to logically organize monitored devices into smaller device groups. For example, into all devices within a specific building, or on the same IP segment.

- Device groups can have subgroups. For example, to organize the devices within a building on a floor-by-floor, or datacenter-by-datacenter basis.
- All groups and subgroups must use unique names.
- Device groups use icons to indicate the following about the status of their devices.

✓	All devices are operating normally.
⚠	At least one device has a warning condition.
✖	At least one device has a critical, error, or failure condition.

Device Groups view

This view, which lists the groups to which devices are assigned, is displayed, by default, when the **Monitoring** or **Surveillance** perspective is selected.

Note: For information about how this view is used in the **Surveillance** perspective, see Surveillance.
The **Device Groups** view lists the following types of groups in a hierarchical format.
Note: The **All Devices** and **Unassigned** groups cannot be deleted or renamed.

All Devices	This group includes all discovered devices, including any that have been assigned to a user-defined device group.
Unassigned	This group includes all discovered devices that are not assigned to a user-defined device group.
User-defined device groups	Each group or subgroup includes the devices that have been assigned to that group.

The **Device Groups View**, which interacts with every view except **Camera** view in some way, can be used to do the following:

- Use the **Device View** to assign devices to groups by dragging and dropping from one group to another.
- Access information about the device alarms at any selected group in the **Active Alarms** view.
- Select a device group for which you want to have camera information displayed in the **Thumbnails** view.
- Use the **Thumbnails** view to assign camera devices to groups by dragging and dropping from one group to another.
- Use right-click options, and the lock and graph icons at the top of the view, to perform the following functions.
    - Create a new group, when **All Devices** is selected, or subgroup, when any other group, except **Unassigned**, is selected (**Create Device Group** option).
    - Rename a selected group, other than **All Devices** and **Unassigned** (**Rename Device Group** option).
    - Delete a selected group, other than **All Devices** and **Unassigned** (**Delete Device Group** option).

- Access the **Alarm History** view for any selected group (**Show Alarm History** option).
- Access a 24-hour **Graph View** for up to 50 of a specific sensor type for a selected device group (**Graphing and Reporting** sensor options).
  Note: For more information about this view, see Graph View under Graphing and reporting feature.
- Initiate the process used to create a report or graph for the historical values of the sensors at selected devices (**Custom Device Report** option or graph icon).
- Access the "Map View Settings" display used to customize the background and device icons in the **Map View** for any selected group except **Unassigned** (**Map View Settings** option).
- Access **User and User Groups**, a **Server Administration Settings** option in the **Settings** menu, to manage the device and surveillance privileges a selected group assigns to the users and user groups (**Device Group Privileges** option).
  Note: You can use this right-click option to add new users or user groups, or to edit any user, user group, or authentication server settings.
- Access a specific configuration option for a selected NetBotz Appliance or Appliances (**NetBotz Appliance Configuration** options).
  Note: For information about these options, see NetBotz Appliance Configuration under Settings menu.

Device group management

You can manage the device groups, and the devices assigned to those groups.

- Use the right-click menu in the **Device Groups** view to create, rename, or delete groups.
- Use the **Device View** to define which devices are assigned to which groups.

Managing the device groups

You can create, rename, and deleted device groups.

Creating a device group

1. In the **Device Groups** view, right-click one of the following device groups:
   - **All Devices**, to add a new group.
   - A user-defined group, to add a subgroup to the selected group.
2. Click **Create Device Group**.
3. Enter a unique name for the device group, and click **Finish**.
4. Assign devices to the new group by dragging and dropping devices from the **Device View**.
5. Edit the user and user group privileges for access to the device group's surveillance and device data, as needed.

Renaming a device group

1. In the **Device Groups** view, right-click the group you want to rename.
2. Click **Rename Device Group**.
3. Enter a unique name for the device group, and click **Finish**.

Deleting a device group

1. In the **Device Groups** view, right-click the group you want to delete.
2. Click **Delete Device Group**.
3. Click **Yes** in the "Confirmation" display.

Assigning or moving devices to device groups

You can assign devices to a device group, change the device group assignments by moving devices from one user-defined group to another, or assign devices to multiple device groups.

Moving devices from one group to another group

1. In the **Device Groups** view, select the group in which the devices are currently located (including **Unassigned**).
2. In the **Device View**, highlight the devices you want to move.

   Note: To move a NetBotz Appliance, and its supported devices, highlight its main listing; if you highlight a device associated with a NetBotz Appliance, a copy of that device will move, and a copy remains with the NetBotz Appliance listing.
3. Drag the selected devices from the **Device View** to the desired group in the **Device Groups** view.

   Note: When devices are assigned to a subgroup, those devices are included in its parent group, as well.

Assigning devices to multiple groups

1. In the **Device Groups** view, select a group that contains one or more of the devices you want to assign to multiple device groups.

   Note: For devices in the **Unassigned** group, move them to one of the groups in which you want those devices assigned, then select that group.
2. In the **Device View**, highlight the devices you want to copy to another group.
3. Hold the Ctrl key down, and drag copies of the selected devices from the **Device View** to the desired group in the **Device Groups** view, including all devices associated with a NetBotz Appliance, when that appliance's main listing is selected.

   Note: For a device associated with a NetBotz Appliance, you can drag a copy to another group without using the Ctrl key.
4. Repeat until all devices are in the correct device groups.

Removing devices from device groups

You can remove devices from a group by dragging those devices from that group, or by using the **Delete Devices** right-click option in the **Device View**.

Note: Removing devices from a group does not delete them from InfraStruXure Central server.

Dragging devices out of device groups

When a device is assigned to multiple device groups, you will need to repeat this procedure for each device group.

1. In the **Device Groups** view, select a device group to which the devices are currently assigned.
2. In the **Device View**, highlight the devices you want to remove.
3. Drag the devices to **Unassigned** in the **Device Groups** view.

   Note: If you want to assign those devices to another group, you can drag them to that group instead of to **Unassigned**.

Using the right-click option in the Device View

When a device is assigned to multiple device groups, you will need to repeat this procedure for each device group.

1. In the **Device Groups** view, select a device group to which the devices are currently assigned.
2. In the **Device View**, highlight the devices you want to remove.
3. Right-click one of those devices, and highlight the **Remove the device from group** option.
4. Select the name of the group from which you want the devices moved.

Note: The devices will be moved back to the **Unassigned** group.

Users and User Groups option

You use this **Server Administration Settings** option in the **Settings** menu to manage local and remote user access to the InfraStruXure Central server and its features and functions, and to manage the access those users have to the device and surveillance data available for each device group in the **Device Groups** view.

The **Users and User Groups** option in the "Server Administration Settings" display has three tabs.

Note: **Device Group Privileges**, a right-click option in the **Device Groups** view, also accesses the **Users and User Groups** option in the "Server Administration Settings" display.

Users tab

Use this **Users and User Groups** option to manage the local and remote users that can access the InfraStruXure Central server, and the access each has to the server functions, and to the device and surveillance data available at each device group in the **Device Groups** view.

You can do the following in this tab:

- Add or edit local user settings.
    - The credentials each uses to log on at the server.
    - The user roles, if any, each is assigned at the server.
    - The user groups, if any, to which each is assigned.
    - The access priviliges each has to the device and surveillance data available at each device group.
      Note: A user assigned the **InfraStruXure Central Administrator** role, or included in a users group that has that role, has full access to server, device, and surveillance functions.
- Edit remote user settings.
    - The user roles, if any, each is assigned at the server.
    - The access priviliges each has to the device and surveillance data available at each device group.
- Delete local and remote users.

Managing a local user

Use the "User Configuration" display to add or edit a local user.

Note: To delete a local user, select that user in the **Users** tab, and click **Delete**.

1. In the **Users** tab for the **Users and User Groups** option, click **Add User** to add a local user, or select a listed local user and click **Edit User** to access the "User Configuration" display.
2. In the **User Information** tab:
    a. Configure the user credentials.
    b. If you want the user disabled, deselect **Enable this user**.
3. In the **User Roles** tab, select the role or roles for the user.

    Note: If you select the **InfraStruXure Central Administrator** role, click **OK** to exit the "User Configuration" display: this role provides full access to all server, device, and surveillance functions; settings in the **User Group Memberships** and **Device Group Privileges** tabs will have no affect on the user's privileges.

4. In the **User Group Memberships** tab, select the user groups to which you want the user to belong, if any.

   Note: If you select a user group with **InfraStruXure Central Administrator** identified in its **Roles** column, click **OK** to exit the "User Configuration" display: the **Device Group Privileges** tab settings will have no affect on any users assigned to the users group as this role provides full access to all server, device, and surveillance functions.
5. If you made any change to a tab's settings, click **Apply**.

   Note: You cannot access the **Device Group Privileges** tab without first applying changes made in the other tabs.
6. In the **Device Group Privileges** tab, define the access you want the user to have at each device group.

   Note: Membership in a user group can affect a user's device and surveillance privileges, based on the user group's privileges: the settings that provide the least-restrictive privileges, whether in the user's or user group's **Device Group Privileges** tab, will be in affect at a device group.

Editing a remote user

Use the "User Configuration" display to edit a remote user.

Note: To add a remote user, use the **Authentication Servers** tab; to delete a remote user, select that user in the **Users** tab and click **Delete**.

1. In the **Users** tab for the **Users and User Groups** option, select a listed remote user and click **Edit User**, to access the "User Configuration" display.

   Note: For a remote user, the **User Information** tab is viewable, but disabled, and no **User Group Memberships** tab appears in the "User Configuration" display.
2. In the **User Roles** tab, select a role for the user, and click **Apply**.

   Note: If you select the **InfraStruXure Central Administrator** role, click **OK** to exit the "User Configuration" display: this role provides full access to all server, device, and surveillance functions; the **Device Group Privileges** tab settings will have no affect on the remote user's privileges.
3. In the **Device Group Privileges** tab, define the access you want the user to have at each device group.

   Note: Membership in a remote user group can affect a remote user's device and surveillance privileges, based on the user group's privileges: the settings that provide the least-restrictive privileges, whether in the user's or user group's **Device Group Privileges** tab, will be in affect at a device group.

"User Configuration" display

Use this display's tabs to add a local user, or to edit the settings for an existing local or remote user.

User Information tab

Use this tab to define the credentials for a local user.

Credential	Definition
Username	Identify the name used to log on to the server.

Credential	Definition
Password	Type in the password to be used to log on to the server.
Verify password	Retype the password.
Full name (optional)	Identify the user's full name.
E-mail address (optional for non-**InfraStruXure Central Administrators**)	Identify the user's email address. **Note:** This address is used to send e-mail to an **InfraStruXure Cental Administrator** for notifications related to the InfraStruXure Central server itself, and not for monitored devices.
Description (optional)	Identify a role, title, or other attribute that describes the user.

User Roles or User Group Roles tab

Use this tab to select the role you want to assign to a user or user group.

Role	Description
InfraStruXure Central Administrator	Full access to all server functions, and to all device and surveillance data for all device groups. **Note:** The **InfraStruXure Central Proxy** is included automatically when the **InfraStruXure Central Administrator** role is selected.
InfraStruXure Central Proxy	No access to server functions, and no access privileges to the device and surveillance, except as defined by settings in the following tabs: **Users**: **User Group Memberships** and **Device Group Privileges** tab settings **User groups**: **Device Group Privileges** tab settings **Note:** Not selecting a role has the same affect as selecting **InfraStruXure Central Proxy**.
Separately-licensed application roles	User roles will be listed for separately-licensed applications that require access to InfraStruXure Central server data. For example, two roles are available for the InfraStruXure Central Capacity Management and InfraStruXure Central Change Management applications: **Capacity/Change Manager Administrator** **Capacity/Change Manager Viewer** **Note:** An application's **Administrator** has full access to the data the InfraStruXure Central server provides to that application; an

Role	Description
	application's **Viewer** has access only to data provided for the device groups at which that viewer has access privileges at the InfraStruXure Central server.

User Group Memberships tab

Use this tab to select the user groups to which you want to assign a local user.

Note: Local users cannot be added to remote user groups; remote users cannot be added to any user group, local or remote.
This tab lists all local user groups, allowing you to select the groups to which a local user is assigned. Three of those user groups are provided, by default.

Note: Selecting a user in the **User Group Members** tab results in the user group being selected in that user's **User Group Memberships** tab, and vice versa.

- **Device Administrators**: by default, this user group provides **Administration Access** for device privileges, and **No Access** for surveillance privileges, at all device groups.
- **Device Viewers**: by default, this user group provides **View Access** for device privileges, and **No Access** for surveillance privileges, at all device groups.
- **Server Administrators**: by default, this user group provides the same server, device, and surveillance privileges as the **InfraStruXure Central Administrator** users role: full access to all server, device, and surveillance functions.
  Note: You can edit the default names and access privileges for any of these user groups.

Device Group Privileges tab

Use this tab to select the device and surveillance privileges you want a user or user group to have at each device group.

By default, **No Access** is selected for both the **Device Privileges** and **Surveillance Privileges** for all users and user groups, with the exception of the three user groups the InfraStruXure Central server provides by default (**Device Administrators**, **Device Viewers**, and **Server Administrators**), unless **InfraStruXure Central Administrator** is selected as the user or user group's role.

Note: Membership in a user group can affect a user's device and surveillance privileges, based on the user group's privileges: the settings that provide the least-restrictive privileges, whether in the user's or user group's **Device Group Privileges** tab, will be the privileges the user has at a device group: if a user that has no surveillance access (**No Access**) belongs to a user group that has **View and Tag Access** for its surveillance privileges at a device group, the user has **View and Tag Access** at that device group.

Element	Description
Device group list	Use to select the device group for which you want to add, modify, or remove the device or surveillance privileges. The check boxes beside each group provide the the following information: **Blank:** **No Access** is the current setting for device and surveillance privileges. **Check-marked**: a privilege setting other than **No Access** has been added to the device group.

	Solid green: a group is inheriting its privilege settings either from **All Devices**, or from a parent group. **Note:** The **All Devices** group privileges provide a baseline for all other device groups: other device groups will use at least the same privileges as **All Devices**, but any group can be set to use less-restrictive privileges.
Surveillance Privileges	Reports the current surveillance privileges for the group selected in the list.
Device Privileges	Reports the current device privileges for the group selected in the list.
Add	Click to add other than **No Access** as the device, or device and surveillance privileges, at a selected group. **Note:** Enabled only when a selected group's device and surveillance privileges are set to **No Access**.
Modify	Click to modify the device or surveillance privileges, or both, for a selected device group. **Note:** Enabled only when at least **View Access** is set as the device privileges at a selected group.
Remove	Click to delete any changes made to the device or surveillance privileges for a selected device group. **Note:** Enabled only when at least **View Access** is set as the device privileges at a selected group.

Managing device and surveillance privileges:

You can configure (add or modify) the device and surveillance privilege settings for any device group, or remove privilege settings for any device group.

Configuring privileges:

You can add access privileges when device and surveillance privileges are both set to **No Access** for a selected device group; you can modify privileges for a selected device group that has at least its device privileges set to other than **No Access**.

1. Select a listed device group and click **Add** or **Modify** (whichever is activated) to access the "Device Group Privileges" display.
2. Set the device and surveillance privileges for the device group, and click **OK**.

   Note: A device group must have at least **View Access** as its device privileges in order to configure surveillance privileges.

Removing privileges:

You can remove changes made to the device and surveillance privileges at any device group, by selecting that group in the list, and clicking **Remove**. The result of this action depends on the device group selected.

- For any device group other than **All Devices**, device and surveillance privileges settings are reset to match the settings for **All Devices**.

- For **All Devices**, device and surveillance privileges settings are reset to **No Access** for **All Devices**, and for any device groups that inherit their privilege settings from **All Devices**. **Note:** By default, a device group inherits its privilege settings from **All Devices** until you configure that group's privilege settings. At that point, deleting privilege changes made for **All Devices** will not reset that group to privileges that are more restrictive than those that were configured for that group.

Device privileges:

Four selections are available for a user or user group's device privileges.

Note: Users assigned the **InfraStruXure Central Administrator** role, or assigned to a user group that has this role, have full device and surveillance access, as well as access to all server functions.

In addition to the device functions identified in the following table, any user can configure **Client Preferences**, **Exit** the client, or log on at another server using **Change Server**.

Device Privilege	Description
No Access	No device access is provided.
View Access	A user with this privilege setting for a device group can perform the following functions for that group's devices: View information about active and historical alarms. View information about device sensors. Create a **Graph** view for a selected sensor type that is associated with the devices. View and export copies of saved reports in a table (as.csv or.txt file) or graph (as.bmp, jpg, or.png file) format. Create and export copies of device sensor reports in a table (as.csv or.txt file) or graph (as.bmp, jpg, or.png file) format. Launch to the web interfaces at the devices. Request that the InfraStruXure Central server scan a selected SNMP device, or set of SNMP devices, to update the available information.
View and Control Access	Users with this privilege setting for a device group can perform the same device functions as the **View Access** provides. **Note:** This privilege does not provide any additional capabilities in InfraStruXure Central server 5.0.
Administration Access	A user with this privilege setting at a device group can perform all functions allowed by the **View Access** privileges for that group's devices, as well as the following additional functions: Create a custom **Map View** for the device group. Configure **Alert Thresholds** for the group's device sensors. Configure **NetBotz Appliance Configuration** options at the group's monitored NetBotz Appliances. Configure the **Device Configuration** settings for the group's SNMP devices. Configure the **Device FTP Settings**. Apply SNMP device and NetBotz Appliance firmware updates that have been downloaded to the InfraStruXure Central server for the group's devices.

Device Privilege	Description
	Note: Only an **InfraStruXure Central Administrator** can download the updates to the server.

Surveillance privileges:

Four selections are available for a user or user group's surveillance privileges.

Note: Users assigned the **InfraStruXure Central Administrator** role, or assigned to a user group that has this role, have full device and surveillance access, as well as access to all server functions.

In addition to the surveillance functions identified in the following table, a user can perform all device functions for the device privilege associated with a device group: **Surveillance Privileges** for a device group requires at least **View Access** for that group's **Device Privileges**.

Surveillance Privilege	Description
No Access	No surveillance access is provided.
View Access	A user with this privilege setting for a device group can perform the following functions for that group's camera devices: View and export surveillance clips. Access the **Camera** view for a licensed camera in the **Thumbnails** view.
View and Tag Access	A user with this privilege setting at a device group can perform all functions allowed by the **View Access** provides, but with the added ability to tag surveillance clips.
Administration Access	A user with this privilege setting at a device group can perform all functions allowed by the **View and Tag Access** provides, but with the added ability to configure the **Surveillance Settings** for all camera devices.

"Device Group Privileges" display:

Use this display to define the **Device** and **Surveillance Privileges** you want a user or user group to have for the device group selected in the **Device Group Privileges** tab.

The privilege settings defined for one device group can affect the settings available to other device groups.

- All settings are available for **All Devices**, unless another device group has had privilege settings added (check-marked in the **Device Group Privileges** tab list): no setting above the highest setting selected at any other group is available for the **All Devices** group. For example:
  - If a device group has had a privilege set to **View Access**, and no device group has a higher setting selected, only the **View Access** and **No Access** privileges will be available for the **All Devices** group.
  - If any device group has had its **Device Privileges** set at **View and Control Access**, **Administration Access** will be unavailable for that privilege for the **All Devices** group. **Note:** If any group other than **Unassigned** has had a privilege set at **Administration Access**, all settings for that privilege will be available for the **All Devices** group.
- The privilege settings available at other groups depend on the settings defined at their parent group: privilege settings more restrictive than the parent group's settings (**All Devices**, or the group to which a subgroup is assigned) are unavailable. For example:

  When **All Devices** has **View Access** selected for its **Device Privileges**, and **View and Tag Access** selected for its **Surveillance Privileges**, **No Access** is unavailable for the **Device**

Privileges at all other groups, and **No Access** and **View Access** are unavailable for the **Surveillance Privileges** at all other groups.

Another factor affects the privileges set at device groups other than **All Devices**: you can select a privilege that is identical to the privilege a group is inheriting from **All Devices**, or a parent group. Although the selected group's privileges remain unchanged, those privileges are no longer inherited, and can no longer be affected by changes made to inherited settings. For example, if you select **View Access**, instead of **View Access (Inherited from All Devices)**, the access selection will not be affected by changes to the **All Devices** group access selection.

User Groups tab

Use this **Users and User Groups** option tab in the "Server Administration Settings" display to manage the local and remote user groups, and the access each group has to the server functions, and to the device and surveillance data available at each device group in the Device Groups view.

User groups are used to manage the access privileges for data and surveillance functions on a device group-by-device group basis for all users assigned to these groups.

- You can do the following in this tab:
  - Add or edit local user group settings.
    - The name used to identify a group.
    - The user group roles, if any, a group is assigned at the server.
    - The users assigned to a group.
    - The access privileges a group has to the device and surveillance data available at each device group.
      Note: A user group assigned the **InfraStruXure Central Administrator** role provides full access to server, device, and surveillance functions to users assigned to that group.
  - Edit remote user group settings.
    - The user group roles, if any, a group is assigned at the server.
    - The access privileges a group has to the device and surveillance data available at each device group.
  - Delete local and remote user groups.

Managing a local user group

Use the "User Group Configuration" display to add or edit a local user group.

Note: To delete a local user group, select that group in the **User Groups** tab, and click **Delete**.

1. In the **User Groups** tab for the **Users and User Groups** option, click **Add Group** to add a local user group, or select a listed local user group and click **Edit Group** to access the "User Group Configuration" display.
2. In the **User Group Information** tab, define a name for the group.
3. In the **User Group Roles** tab, select the role or roles for the group.

   Note: If you select a the **InfraStruXure Central Administrator** role, the **Device Group Privileges** tab settings will have no affect on any users assigned to the users group: this role provides full access to all server, device, and surveillance functions.
4. In the **User Group Members** tab, select the users you want assigned to the group.
5. If you made any change to a tab's settings, click **Apply**.

   Note: You cannot access the **Device Group Privileges** tab without first applying changes made in the other tabs.

6. In the **Device Group Privileges** tab, define the access you want the user group to have at each device group.

   Note: Membership in a user group can affect a user's device and surveillance privileges, based on the user group's privileges: the settings that provide the least-restrictive access privileges, whether in the user's or user group's **Device Group Privileges** tab, will be in affect at a device group.

Editing a remote user group

Use the "User Group Configuration" display to edit a remote user group.

Note: To add a remote user group, use the **Authentication Servers** tab; to delete a remote user group, select that group in the **User Groups** tab and click **Delete**.

1. In the **User Groups** tab for the **Users and User Groups** option, select a listed remote group and click **Edit Group**, to access the "User Group Configuration" display.

   Note: For a remote user user group, the **User Group Information** tab viewable, but disabled, and no **User Group Members** tab appears in the "User Group Configuration" display.
2. In the **User Group Roles** tab, select the role or roles for the group, and click Apply.

   Note: If you select a the **InfraStruXure Central Administrator** role, click **OK** to exit the "User Group Configuration" display: this role provides full access to all server, device, and surveillance functions; the **Device Group Privileges** tab settings will have no affect on any users assigned to the users group.
3. If you made any change to a tab's settings, click **Apply**.

   Note: You cannot access the **Device Group Privileges** tab without first applying changes made in the other tabs.
4. In the **Device Group Privileges** tab, define the access you want the user group to have at each device group.

   Note: Membership in a remote user group can affect a remote user's device and surveillance privileges, based on the user group's privileges: the settings that provide the least-restrictive access privileges, whether in the user's or user group's **Device Group Privileges** tab, will be in affect at a device group.

"User Group Configuration" display

Use this display's tabs to add a local user group, or to edit the settings for an existing local or remote user group.

User Group Information tab

Use this tab to define a name for a local user group.

User Group Members tab

Use this tab to select the local users you want to assign to a local user group.

Note: Local users cannot be added to remote groups; remote users cannot be added to any user group, local or remote.

Lists all local users, allowing you to select which of those users you want assigned to the user group.

Note: Selecting a user in the **User Group Members** tab results in the user group being selected in that user's **User Group Memberships** tab, and vice versa.

Authentication Servers tab

Use this **Users and User Groups** option tab to manage the authentication servers used to add remote users and user groups for the InfraStruXure Central server.

Each authentication server listed in this tab has users and user groups that can be assigned as remote users and user groups at the InfraStruXure Central server. These users and user groups can be selected when the authentication server is added to the tab, using the "Add Authentication Server" wizard, or after it has been added, using the "Edit Authentication Server" wizard.

Note: When a remote user identified in the **Users** tab, or a user that belongs to a remote user group identified in the **User Groups** tab, attempts to log on to the InfraStruXure Central server, the logon values (username and password) are sent to the authentication server associated with that user. It is that server, and not the InfraStruXure Central server, that authenticates the log on attempt.

Managing authentication servers, remote users, and remote user groups

You use the "Add Authentication Server" or "Edit Authentication Server" wizard to add remote users and user groups that will have access to the InfraStruXure Central console, depending on whether the authentication server that lists those users and user groups is included in the **Authentication Servers** tab.

Note: Use the **Users** tab to edit or delete remote users, and the **User Groups** tab to edit or delete remote user groups that have access to the InfraStruXure Central console.

1. In the **Authentication Servers** tab for the **Users and User Groups** option, click **Add Authentication Server** to access the "Add Authentication Server" wizard, or select a listed server and click **Edit Authentication Server** to access the "Edit Authentication Server" wizard.

   Note: To delete an authentication server, select that server in the **Authentication Servers** tab and click **Delete**.
2. In the "LDAP/Active Directory Server Settings" display, configure the settings, if necessary, and click **Next**.
3. In the "LDAP/Active Directory Bind Settings" display, configure the settings, if necessary, and click **Next**.
4. In the "Remote Users and User Groups Selection" display, select the users and user groups you want to add that will have access to the InfraStruXure Central console.
   - Select the remote users you want to add from the **Users** folder, at an Active Directory server, or **people** folder, at an OpenLDAP server.
   - Select the remote user groups you want to add from the **group** folder at either server type.

"Add Authentication Server" or "Edit Authentication Server" wizard

Use this wizard to add remote users and user groups, and to add or edit the authentication servers at which those users and user groups are defined.

"LDAP/Active Directory Server Settings" display

Use this display to configure the settings for the authentication server.

Element	Description
Server Label	Define a name to be used as a label that identifies the authentication server.
Server Address	Identify the hostname or IP Address of the authentication server.
Server Type	Select the type of authentication server: **Active Directory** or **OpenLDAP**.
Server Port	Identify the number of the port used for authentication server communication (**389** is the default).
Use SSL	Select to use the Secure Sockets Layer (SSL) protocol for communication between the InfraStruXure Central and the authentication server.

"LDAP/Active Directory Bind Settings" display

Use this display to configure the settings the InfraStruXure Central server uses to access the authentication server.

Element	Description
Bind User DN	Identify the user DN required to access the authentication server.
Bind Password	Identify the password required to access the authentication server.
Search Base	Identify a search base that can narrow the search scope and decrease directory lookup time at the authentication server.

"Remote Users and User Groups Selection" display

Use this display to select the remote users and remote user groups that will have logon access to the InfraStruXure Central server.

Note: Users are located in the **User** folder, at an Active Directory server, or **people** folder, at an OpenLDAP server; user groups are located in the **group** folder at either server type.

Client Preferences (Edit menu)

Use this option's display to define settings that apply to your InfraStruXure Central client only.

Audio Settings

Use this option to select whether your InfraStruXure Central client will play a sound when alerts occur.

Element	Description
Play Sound when an Alert Occurs	Select to enable your client to play the sound for the **Select Audio File** selection.
Select Audio FIle	Select the sound you want your client to play from the drop-down list.
Test Sound	Click to hear the sound for a **Select Audio File** selection.

Browser Settings

Use this option to select the web browser your InfraStruXure Central client will use to connect to the web interface at a monitored device.

Element	Description
Use the Default Web Browser to Launch to Device	Select to use your default web browser (the default selection), or deselect to use a different browser.
Path	Identify the location of the web browser executable file (*.exe).
Browse	Click to browse to the executable file (*.exe) for the web browser you want to use, if necessary to select that file's **Path**.
Test Browser	Click to verify that the selected browser can access the APC home page.

Device View Settings

Use this option to define the maximum number of devices that can be listed in the **Device View** at any one time (**500**, by default).

Note: The **Map View** is unaffected by this setting.

This setting does not limit the number of devices the InfraStruXure Central server can monitor, only how many it can display in the **Device View**. For example, the server monitors 1000 devices, with 600 devices evenly distributed in six different device groups:

- When **All Devices** is selected, only 500 devices will appear in the **Device View**. You can use the **Search** feature to narrow the list down to a specific set of devices.
- When **Unassigned** is selected, the 400 devices that are not yet assigned to any device group will be listed in the **Device View**.
- When any one of the six other device groups is selected, all the devices in that group will be listed in the **Device View**.

Settings menu

This menu provides options used to configure settings that affect how the InfraStruXure Central server, InfraStruXure Central client, monitored NetBotz Appliances, and monitored SNMP devices function.

Option	Description
Alert Settings	Provides options that define the **Alert Actions**, **Alert Profiles**, and **Alert Thresholds** associated with the alert notifications generated by the InfraStruXure Central server, or by its monitored NetBotz Appliances.
SNMP Device Settings	Provides options used to configure monitored SNMP devices.
NetBotz Appliance Configuration	Provides options used to configure monitored NetBotz Appliances.
Surveillance Settings	Accesses the surveillance settings on the InfraStruXure Central server.
Graphing and Reporting	Provides one option, **Scheduled Export Configuration**, used to managed the export configurations for the scheduled exporting of saved reports. **Note:** For information about this option, and about the right-click **Graphing and Reporting** options available in various views, see Graphing and reporting feature.
Server Administration Settings	Provides options used to configure InfraStruXure Central server settings.

Alert Settings (Settings menu)

Provides options used to configure how the InfraStruXure Central server and NetBotz Appliances report alarm conditions.

Alert Notifications overview

The InfraStruXure Central server can notify users when the InfraStruXure Central server's alert thresholds are triggered for its monitored SNMP devices. The monitored NetBotz Appliances each generate their own alert notifications in response to alert threshold violations that occur at the devices they monitor.

The **Alert Settings** options in the **Settings** menu define how notifications are performed.

- **Alert Actions**: Used to create, edit, or delete the alert actions which define how users will be notified of alarm conditions.
  Note: You must create at least one alert action before your InfraStruXure Central server can generate alert notifications.
- **Alert Profiles**: Used to create, edit, or delete alert profiles that define the notification sequences to occur when a threshold is triggered.
  Note: You must edit the default profiles, or add new profiles, to include one or more alert actions before your InfraStruXure Central server can generate alert notifications.
- **Alert Thresholds**: Used to define threshold settings that the InfraStruXure Central server and NetBotz Appliances will use to monitor sensor values.

Alert Actions option

This option accesses the "Alert Actions" wizard used to create and edit the actions that can be included in the alert profiles used with alert notifications.

The alert notifications can alert alert you, or other members of your organization, when the following events occur:

- A sensor threshold violation, or other alarm condition, occurs at a monitored NetBotz Appliance.
- A violation of an alert threshold for a device the InfraStruXure Central server monitors.
- An alarm occurs at a monitored SNMP device.
  Note: Default alert profiles exist, one for notifications associated with each NetBotz Appliance, and one for notifications associated with the InfraStruXure Central server's alert thresholds, and the alarms at the monitored SNMP devices.

You can create multiple versions of the alert actions, each with unique settings, such as which severities apply to the alert action.

Alert actions management

You use the "Alert Actions" wizard to create, modify, or delete the alert actions. These actions can be used in alert profiles as part of the alert notifications used by monitored NetBotz Appliances, or by the InfraStruXure Central server.

Creating an alert action

You must create at least one alert action before your InfraStruXure Central server can generate alert notifications.

All alert actions are created using the same basic procedure.

1. Select **Alert Actions** in the **Settings** menu.
2. In the "Select Alert Action Type" display, highlight the type of alert you want to create, and click **Next**.
3. In the "Select Next Action" display, select to create a new action, and click **Next**.
4. In the "Select Devices" display, select the parent device or devices you want associated with the alert action, and click **Next**.
    - Creating the alert action on the InfraStruXure Central server will make it available for use with all profiles on the server.
    - Creating an alert action on a NetBotz Appliance will make the alert action available to all profiles on the selected NetBotz Appliance.
5. In the "Alert Action" display for the selected action, define the settings you want the action to use, and click **Next**.

    Note: For information about the settings for the action you are creating, see the help section for that action's settings display.
6. In the "Test Action" display, click **Finish** without testing the action, or select the action you want to test, click **Test Action**, and then click **Finish**.

    Note: You will need to verify the test was successful. For example, for a **Send SNMPv1 Trap**, verify the trap was received at the trap receiver; for a **Send E-mail**, verify the e-mail was received.
7. In the "Choose Next Action" display, select whether you want to configure additional actions, add actions to alert profiles, or exit the "Alert Actions" wizard, and click **OK**, or click **Cancel**, to exit the wizard.

Modifying an alert action

You can use the same basic procedure to modify any type of alert action.

1. Select "Alert Actions" in the **Settings** menu.
2. In the "Select Alert Action Type" display, highlight the type of alert you want to modify, and click **Next**.
3. In the "Select Next Action" display, select to modify an action, and click **Next**.
4. In the "Select Devices" display, select the parent device or devices associated with the alert action you want to modify, and click **Next**.
5. In the "Select Alert Actions" display, select only the alert action you want to edit.

    CAUTION: If you select multiple alert actions, the changes you make will result in those alert actions using the same settings and name.
6. In the "Alert Action" display for the selected action, edit the settings, as needed, and click **Next**.
7. In the "Test Action" display, click **Finish** without testing the action, or select the action you want to test, click **Test Action**, and then click **Finish**.

    Note: You will need to verify the test was successful. For example, for a **Send SNMPv1 Trap**, verify the trap was received at the trap receiver; for a **Send E-mail**, verify the e-mail was received.
8. In the "Choose Next Action" display, select whether you want to configure additional actions, add actions to alert profiles, or exit the "Alert Actions" wizard, and click **OK**.

Deleting an alert action

You can use the same basic procedure to delete any type of alert action.

1. Select "Alert Actions" in the **Settings** menu.
2. In the "Select Alert Action Type" display, highlight the type of alert you want to delete, and click **Next**.
3. In the "Select Next Action" display, select to modify an action, and click **Next**.
4. In the "Select Devices" display, select the parent device or devices associated with the action you want to delete, and click **Next**.
5. In the "Select Alert Actions" display, select the action or actions you want to delete, and click **Delete**.
6. Click **Cancel**, to exit the "Alert Actions" wizard.

"Alert Actions" wizard

This wizard, accessed by **Alert Actions** in the **Settings** menu, is used to manage the alert actions.

The "Alert Actions" wizard uses some or all of the following displays when creating, modifying, or deleting any of the alert action types.

"Select Alert Action Type" display

Use this display to select the type of action you want to create, modify, or delete.

Alert Action	Description
Send E-mail	Sends a message that uses the standard e-mail format.
Activate Button Output	Activates a button output on a device managed by a NetBotz Appliance.
Send SNMPv3 Inform	Sends an SNMPv3 inform.
Send SNMPv1 Trap	Sends an SNMPv1 trap.
Send Short Message E-mail	Sends a message that uses the short-message e-mail format.
Send HTTP Post	Sends an HTTP post.
Send Data to FTP Server	Sends data to an FTP server.
Send Wireless SMS Message	Sends a wireless SMS message from a wireless modem connected to a NetBotz Appliance.
Set Switch Output State	Sets the state of an output switch on a device managed by a NetBotz Appliance.

"Select Next Action" display

Use this display to select whether you want to edit an existing action, or create a new one.

"Select Devices" display

Use this display to select an alert action's parent devices.

Note: The InfraStruXure Central server is the parent device for its monitored SNMP devices; each NetBotz Appliance is the parent device for its camera pods, sensor pods, and other devices it monitors.

Parent Device	Description
<server_name>(InfraStruXure Central)	Select the InfraStruXure Central server option to create, edit, or delete an alert action that can be used with the server's monitored devices.

NetBotz Appliance	Select one or more NetBotz Appliance options to create, edit, or delete an alert action that can be used with their monitored camera pods, sensor pods, and other devices.

"Select Alert Action" display

Use this display to select the alert action or actions you want to modify or delete, then click **Next**, to modify your selections, or **Delete**, to delete them.

Note: If you select to modify multiple actions, those actions will all use the same settings and name.

"Alert Action" displays

Each type of alert action has its own configuration display.

Common alert action settings:

All alert action types share a name field, severity selections, and an "Advanced Scheduling" display.

Alert action severity settings:

Every alert action type allows you to select up to five severities. The alert action will only trigger when used in an alert profile that is tied to an alert threshold with a matching severity.

In the following example, User1 will only receive an sms message if a critical severity threshold is violated.

- An alert action named "send_user1_sms” is created, and defined to send User1 an SMS e-mail for critical events only.
- The “send_user1_sms” alert action is added to an alert profile called “sms messaging.”
- The "sms messaging" alert profile is selected on various alert thresholds. The alert thresholds are of varying severity - some are set for critical, and some are set for warning. If an alarm occurs, User1 will only receive an SMS message for those alert thresholds defined as critical.

You must select at least one severity.

Severity	Description
Information	Typically used to set up an alert action to respond to events considered to be unimportant, but important enough to require alert notifications when they occur.
Warning	Typically used by SNMP devices to indicate a condition exists that may require attention to make sure it does not deteriorate into a critical state. For example, a UPS that is running on battery power during a power failure will shut down its load equipment if its battery power is depleted before power returns to normal.
Error	Typically used by NetBotz Appliances to indicate a sensor threshold violation requires immediate attention. For example, a high temperature violation that could lead to equipment damage.
Critical	Typically used by SNMP devices to indicate an operational failure requires immediate attention. For

	example, a battery that needs to be replaced can result in the loss of data at the UPS load equipment if a power failure occurs.
Failure	Typically used by NetBotz Appliances to indicate an operational failure requires immediate attention. For example, communication with a camera pod was lost which could lead to an undetected security violation.

"Advanced Scheduling" display:

Use this display to define the specific periods of time, for each day of the week, during which an associated activity will be disabled (by default, scheduling is enabled 24 hours a day, seven days a week).

Note: This display is used to schedule when an alert action will be enabled and disabled, using the action's settings display, or to schedule when a camera is enabled or disabled, using the "Surveillance Settings" display.

The table provides cells for 15-minute increments, and columns for every day of the week. You can do all of the following to schedule when an alert action, or camera, is enabled:

- Click a column title to enable or disable all of that day's cells.
- Drag your mouse from one cell to another cell in a column, to enable or disable a set of cells.
- Drag your mouse from a cell in one column to a cell in another column, to enable or disable an identical set of cells for each of the selected days.
- Click a single cell.
  Note: The NetBotz Appliance also can schedule a camera's surveillance activity. The camera will not capture data when either the InfraStruXure Cental server or the NetBotz Appliance has surveillance disabled; both must have surveillance enabled, to capture data.

"Send E-mail" display:

Use this display to define the settings for a **Send E-mail** alert action on the InfraStruXure Central server, or on a NetBotz Appliance.

A name field, severity selections, and the "Advanced Scheduling" display that all alert action types share, are also available.
Note: Make sure the InfraStruXure Central server's SMTP settings, and the separate SMTP settings for the monitored NetBotz Appliances, are all defined properly.

E-mail tab:

Element	Description
Add	Click to add an e-mail address to the address list.
Remove	Click to remove a selected e-mail address from the address list.
Include Threshold-specific Addresses	Select to send e-mails to e-mail addresses defined at InfraStruXure Central alert thresholds.

Threshold-specific addresses example:

- A “generic_send_email” alert action is created with no e-mail addresses included.
- **Include Threshold-specific Addresses** is selected for this "generic_send_email" action.
- The “generic_send_email” alert action is added to an alert profile called “alert_profile1.”
- The “alert_profile1” profile is specified for two thresholds, “temp_too_high” and “humidity_too_high.”
- The “temp_too_high” threshold has **Threshold-Specific Addresses** for User1 and User2, and the “humidity_too_high” threshold has **Threshold-Specific Addresses** for User3 and User4.
  - When “temp_too_high” triggers, only User1 and User2 will receive e-mails.
  - When “humidity_too_high” triggers, only User3 and User4 will receive e-mails.

Advanced tab:

Provides elements that further define what an e-mail can include, as well as an **Advanced Scheduling** button that allows you to select when an alert action is enabled (all time periods are enabled, by default).
Note: Three settings, **Maximum Camera Pictures**, **Include Related Maps with the Alert**, and **Picture Export Format** only apply to alert actions created on NetBotz Appliances.

Element	Description
Maximum Camera Pictures	Select the maximum number of pictures that can be included in e-mails.
Include a Graph with the Alert	Select to include graphs in e-mails.
Include Related Maps with the Alert	Select to include related maps in e-mails.
Include a Sound Clip with the Alert	Select to include related sound clips in e-mails, for NetBotz Appliances only. **Note:** Disabled for NetBotz Appliances that have no audio support.
Do Not Send Return-to-Normal Messages	Select if you do not want to receive an e-mail when the threshold violation returns to normal.
Minimize Header Usage	Select to minimize the size of the e-mail headers.
Picture Export Format	Select the format used for pictures sent with e-mails. **Note:** The export options will depend on how the NetBotz Appliance is configured.

"Activate Button Output" display:

Use this display to define the settings for an **Activate Button Output** alert action on a NetBotz Appliance.

A name field, severity selections, and the "Advanced Scheduling" display that all alert action types share, are also available.

Element	Description
Button Output Device	Select the button-output device that will be activated at the NetBotz Appliance. **Note:** When no devices that support a button output are monitored by the NetBotz Appliance, **N/A** is the only choice.

Activate on Return-to-Normal	Select to activate the button output when the threshold state returns to normal.

"Send SNMPv1 Trap" display:

Use this display to define the settings for a **Send SNMPv1 Trap** alert action on the InfraStruXure Central server, or on a NetBotz Appliance.

A name field, severity selections, and the "Advanced Scheduling" display that all alert action types share, are also available.

Element	Description
Target Host Address	Identify the hostname or IP address of the Network Management System (NMS) to which traps will be sent.
Community String	Identify the community string that will be used when sending traps to the target NMS.
Trap Port Number	Select the number of the port the target NMS uses to receive SNMP traps.

"Send SNMPv3 Inform" display:

Use this display to define the settings for a **Send SNMPv3 Inform** alert action on the InfraStruXure Central server, or on a NetBotz Appliance.

A name field, severity selections, and the "Advanced Scheduling" display that all alert action types share, are also available.

Primary tab:

Element	Description
Target Host Address	Identify the Hostname or IP address of the Network Management System (NMS) to which informs will be sent.
Authentication User ID	Identify the user identification to be used when sending SNMPv3 informs to the target NMS.
Authentication Password	Type in the password to be used when sending SNMPv3 informs to the target NMS.
Verify Password	Retype the password.
Authentication Protocol	Select **SHA-1** or **MD5** as the protocol used when sending SNMPv3 informs to the target NMS.

Advanced tab:

Provides elements that further define how SNMPv3 informs are sent, as well as an **Advanced Scheduling** button that allows you to select when an alert action is enabled (all time periods are enabled, by default).

Element	Description
Inform Port Number	Identify the number of the port that the target NMS identified in the **Primary** tab uses to receive SNMPv3 informs.
Encryption Protocol	Select whether encryption will be used with the SNMPv3, and if used, which protocol: **None**, **DES**, or **AES-128**.
Encryption Password	Identify the encryption password to be used to send SNMPv3 informs.
Verify Password	Type in the password, again.

"Send Short Message E-mail" display:

Use this display to define the settings for a **Send Short Message E-mail** alert action on the InfraStruXure Central server, or on a NetBotz Appliance.

A name field, severity selections, and the "Advanced Scheduling" display that all alert action types share, are also available.
Note: Make sure the InfraStruXure Central server's SMTP settings, and the separate SMTP settings for the monitored NetBotz Appliances, are all defined properly.

E-mail tab:

Element	Description
Add	Click to add an e-mail address to the address list.
Remove	Click to remove a selected e-mail address from the address list.
Include Threshold-specific Addresses	Select to send e-mails to e-mail addresses defined for InfraStruXure Central alert thresholds.
Subject	Enter a subject for the message; macros can be used.
Message	Enter a message; macros can be used.

Threshold-specific addresses example:

- A “generic_send_SMS_email” alert action is created with no e-mail addresses included.
- **Include Threshold-specific Addresses** is selected for this "generic_send_SMS_email" action.
- The “generic_send_SMS_email” alert action is added to an alert profile called “alert_profile1.”
- The “alert_profile1” profile is specified for two thresholds, “temp_too_high” and “humidity_too_high.”
- The “temp_too_high” threshold has **Threshold-Specific Addresses** for User1 and User2, and the “humidity_too_high” threshold has **Threshold-Specific Addresses** for User3 and User4.
  - When “temp_too_high” triggers, only User1 and User2 will receive short-message e-mails.
  - When “humidity_too_high” triggers, only User3 and User4 will receive short-message e-mails.

Advanced tab:

Provides elements that further define what an e-mail can include, as well as an **Advanced Scheduling** button that allows you to select when an alert action is enabled (all time periods are enabled, by default).

Element	Description
Do Not Send Return-to-Normal Messages	Select if you do not want to receive an e-mail when the threshold violation returns to normal.
Minimize Header Usage	Select to minimize the size of the e-mail headers.
Send both HTML and Plain Text Message	Select to include HTML formatted messages in addition to plain text messages.
Message Size Limit (bytes)	Identify the maximum number of bytes used for a message.

"Send HTTP Post" display:

Use this display to define the settings for a **Send HTTP Post** alert action on the InfraStruXure Central server, or on a NetBotz Appliance.

A name field, severity selections, and the "Advanced Scheduling" display that all alert action types share, are also available.

Primary and Backup tabs:

You must define at least the **Primary** tab elements.

Element	Description
Target URL	Identify the web address, port and parameters of the system to which HTTP post data will be posted.
Target User ID	Identify the user identification needed to post HTTP data to the server at the specified **Target URL**.
Target Password	Identify the password needed to to post HTTP data to the server at the specified **Target URL**.
Verify Password	Retype the password.

Advanced tab:

Provides elements that further define what an HTTP post can include, as well as an **Advanced Scheduling** button that allows you to select when an alert action is enabled (all time periods are enabled, by default).
Note: Two elements, **Maximum Camera Pictures** and **Include Related Maps with the Alert**, apply to alert actions created on NetBotz Appliances, only.

Setting	Description
Maximum Camera Pictures	Identify the maximum number of pictures that can be included in an HTTP post.
Include a Graph with the Alert	Select to include a graph with the HTTP post.
Include Related Maps with the Alert	Select to include a related maps with the HTTP post.
Include a Sound Clip with the Alert	Select to include related sound clips in the HTTP post, for NetBotz Appliances only. **Note:** Disabled for NetBotz Appliances that have no audio support.

SSL Verify Options	Select **No verification**, **Verify certificate**, or **Verify certificate and hostname** for HTTP posts.

"Send Data to FTP Server" display:

Use this display to define the settings for a **Send HTTP Post** alert action on the InfraStruXure Central server, or on a NetBotz Appliance.

A name field, severity selections, and the "Advanced Scheduling" display that all alert action types share, are also available.

Primary and Backup tabs:

You must define at least the **Primary** tab elements.

Note: The only difference between the two tabs is that the **Backup** tab includes backup settings.

Setting	Description
FTP Server Hostname	Identify the hostname or IP address of the FTP server that will receive the data.
User ID	Identify the user identification needed to log on to the FTP server.
Password	Identify the password needed to log on to the FTP server.
Verify Password	Retype the password.
Target Directory	Identify the relative directory path to be used to store the data at 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. **Note:** This **Target Directory** field accepts macros.
Base Filename	Identify the base filename to be used for storing the data at the FTP server. 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.). Alert data will be stored in a file with this name, followed by the *.nbalert file extension. Pictures include in the data 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:** This **Base Filename** field accepts macros.

Advanced tab:

Provides elements that further define what an e-mail can include, as well as an **Advanced Scheduling** button that allows you to select when an alert action is enabled (all time periods are enabled, by default).
Note: Three settings, **Maximum Camera Pictures**, **Include Related Maps with the Alert**, and **Picture Export Format** only apply to alert actions created on NetBotz Appliances.

Setting	Description
Maximum Camera Pictures	Identify the maximum number of pictures that can be included in the data sent to an FTP server.
Include a Graph with the Alert	Select to include graphs with data sent to an FTP server.
Include Related Maps with the Alert	Select to include related maps with data sent to an FTP server.
Include a Sound Clip with the Alert	Select to include related sound clips in the data sent to an FTP server, for NetBotz Appliances only. **Note:** Disabled for NetBotz Appliances that have no audio support.
Picture Export Format	Select the format used for pictures sent with the data sent to an FTP server. **Note:** The export options will depend on how the NetBotz Appliance is configured.

"Send Wireless SMS Message" display:

Use this display to define the settings for a **Send Wireless SMS Message** alert action on a NetBotz Appliance configured with a wireless modem.

Note: This alert action is available for a NetBotz Appliance with a modem that supports SMS messaging installed in, or connected to, that appliance, only.
A name field, severity selections, and the "Advanced Scheduling" display that all alert action types share, are also available.

Basic tab:

Element	Description
Add	Click to add a destination address of the recipients to whom the wireless SMS message alert notification will be sent, in the following format. sms:sms_device_address where sms: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
Remove	Click to remove a selected destination from the list.
Include Threshold-specific SMS Destinations	Select to send wireless SMS messages to the destination addresses added to the **E-mail** tab for NetBotz Appliance alert thresholds. **Note:** If the destination addresses list is empty, and **Include threshold-specific SMS destinations** is not

	selected, no wireless SMS messages can be sent; if the destination addresses list is empty, and **Include threshold-specific SMS destinations** is selected, wireless SMS messages can be sent only for thresholds that have an SMS destination address identified in their Threshold-specific address list.
Message	Enter a message for the alert; macros can be used.

Threshold-specific addresses example:

- A “generic_send_wireless_SMS” alert action is created and no SMS destinations are included.
- **Include threshold-specific SMS destinations** is selected for this "generic_send_wireless_SMS" action.
- The “generic_send_wireless_SMS” alert action is added to an alert profile called “alert_profile1.”
- The “alert_profile1” profile is specified for two NetBotz Appliance thresholds, “temp_too_high” and “humidity_too_high.”
- The “temp_too_high” threshold has **Threshold-Specific Addresses** for User1 and User2, and the “humidity_too_high” threshold has **Threshold-Specific Addresses** for User3 and User4.
    - When “temp_too_high” triggers, only User1 and User2 will receive SMS messages.
    - When “humidity_too_high” triggers, only User3 and User4 will receive SMS messages.

Advanced tab:

Provides elements that further define what a wireless SMS message can include, as well as an **Advanced Scheduling** button that allows you to select when an alert action is enabled (all time periods are enabled, by default).

Element	Description
Do Not Send Return-to-Normal Messages	Select if you do not want to send SMS messages when the threshold state returns to normal.
Message Character Size Limit (1 - 160)	Identify the number of characters that can be used in the messages.
Message Validity Period	Select how long a period of time the messages will be valid, from **5 Minutes** through **3 Days**.

"Set Switch Output State" display:

Use this display to define the settings for a **Set Switch Output State** alert action on a NetBotz Appliance.

A name field, severity selections, and the "Advanced Scheduling" display that all alert action types share, are also available.

Note: All time periods are enabled for an alert action, by default, in its "Advanced Scheduling" display.

Element	Description

Switch Output Device	Select the switch relay device that will be triggered by the alert action from the list of all switch relay devices defined for use with the selected NetBotz Appliance. **Note:** When no devices that support a switch output are monitored by the NetBotz Appliance, **N/A** is the only choice.
Switch State on Alert	Select the state (**On** or **Off**) to which the selected switch relay device will be set when an alert occurs.
Switch State on Clear	Select the state (**Unchanged**, **On**, or **Off**) to which the selected switch relay device will be set when the violated threshold returns to a normal state.

Macros for alert action settings:

Three basic types of macros can be used for **Send Short Message E-mail**, **Send Data to FTP Server**, and **Send Wireless SMS Message** alert action settings.

Identification macros:

All identification macros, except one, are available for use when defining alert action settings for NetBotz Appliances and InfraStruXure Central server's monitored SNMP devices: ${VER} identifies the version number for a NetBotz Appliance.

Macro	Definition	Example
${SERIAL}	The serial number of the device.	WA0450111525
${IP}	The dotted-decimal IP address of the device.	192.168.2.23
${HOSTNAME}	The hostname of the device.	isxc.apc.com
${MODEL}	The model of the device.	WallBotz 500
${TIMESTAMP}	The current UTC time (seconds since 1/1/1970).	998885130
${DATE}	The current date (year-month-day).	2008-03-27
${YEAR}	The current year.	2008
${MONTH}	The current month (2-digit number, January=01).	03
${DAY}	The current day of the month (2-digit number).	27
${TIME}	The current time (24-hour, hour-minute-second).	23-30-01
${HOUR}	The current hour of the day (2-digit, 24-hour time).	23
${MIN}	The current minute of the hour.	30
${SEC}	The current second of the minute.	01
${VER}	The current firmware version of the NetBotz Appliance.	2_6_2-20071031_1658

Location macros:

All location macros are available for use when defining alert action settings for NetBotz Appliances; only one macro, ${LOCATION}, is typically used in alert action settings for the InfraStruXure Central server's monitored SNMP devices.

Macro	Definition	Example
${LOCATION}	The location for an InfraStruXure Central SNMP device, or the Location setting at a NetBotz device.	Test Lab
${ENCLOSURE}	Enclosure ID	RACK1234
${SLOT}	Slot in Enclosure	A23
${ENCRELLOC}	Position in Enclosure	ATUPS
${ROOM}	Room Number	C-100
${ROOMROW}	Row in Room	AA
${ROOMCOL}	Column in Room	25
${HEIGHT}	Height above Floor	60
${BLDG}	Building	205
${FLOOR}	Floor Number	3
${COMPANY}	Company Name	APC
${ADDRESS1}	Address 1	132 Fairgrounds Road
${ADDRESS2}	Address 2	Building 1
${CITY}	City	W. Kingston
${STATE}	State/Province	RI
${COUNTRY}	Country	USA
${CONTACT}	Primary Contact	J. Smith
${SITE}	Site Name	West Campus
${NOTES}	Notes	IT Closet, Server Room
${LATITUDE}	Latitude (for units to which a GPS pod is connected)	30° 18’ N
${LONGITUDE}	Longitude (for units to which a GPS pod is connected)	97° 42’ W
${GPSLOC}	The current longitude and latitude data when the alert occurred (for units to which a GPS pod is connected)	30° 18’ N / 97° 42’ W

Alert macros:

Alert macros are available for use when defining alert action settings on the InfraStruXure Central as well as NetBotz Appliances.

Macro	Definition	Example
${ALERTTYPE}	The type of alert.	HIGHERR

${SENSORTYPE}	The type of sensor generating the alert.	TEMP
${SENSORVAL}	The value reported by the sensor that is generating the alert.	60
${ALERTTIME}	The date and time at which the alert notification was generated.	Apr 2, 2002 13:01:45
${ALERTSEV}	The severity value reported by the sensor that is generating the alert (such as ERR, WARN, INFO). If the alert state has returned to normal, the severity value will be followed by "-RTN" (for example WARN-RTN).	ERR, WARN-RTN
${SENSORNAME}	The name of the sensor associated with the alert.	Bldg. 3 Door
${ALERT_PROFILE}	The name of the alert profile that was used to generate the alert.	Default, Profile #1
${ALERT_LEVEL}	The name of the specific alert sequence that caused the alert to be generated. Corresponds with the Label value of the alert sequence.	First Alert Level, Second Alert Level
${ISACTIVE?yes?no}	Specifies custom active vs. return to normal text. The strings “yes” and “no” can be replaced with user-specified strings. For example, if you specify “active” and “cleared” for the “yes” and “no” values and the macro is translated, if the alert is still active the word "active" would appear and when it has returned to normal, the word "cleared" would appear.	“active” and “cleared”
${USERURL}	The user-specified URL that can be defined within the threshold configuration.	http://www.mysite.com
${USERDESC}	The user-specified description value which can be defined within the threshold configuration.	“Too high”
${START_TIME}	The time at which the alert condition was initially detected.	13:01:45
${RESOLVE_TIME}	The time at which the alert condition returned to normal.	13:07:13
${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
${EVENTID}	The unique 16 character identifier shared by all messages generated as a result of a single alert notification event. For example, if an appliance generates an alert notification when the internal temperature sensor threshold is exceeded, and then generates a "return to normal" message when the temperature	3E4512C0FE03440F

	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.	
${ALERTPOD}	The label of value of the pod that either contains the sensor that reported the alert or to which the sensor is connected.	My Pod
${ALERTPODSERIAL}	The serial number of the pod that either contains the sensor that reported the alert or to which the sensor is connected.	NB007100730114
${ALERTPORT}	The label value for the external sensor port to which the external sensor that reported the alert is connected.	Ext1
${CURRENT_ALERT_NUM}	The number of times the alert sequence has been repeated, from 0 up to the Repeats value for the alert sequence.	0, 1, 2
${RESOLVEUSERID}	The user ID that is responsible for manually resolving an alert (when this option applies).	joeuser
${RESOLVECOMMENT}	The text entered into the user-specified description field whenever an alert needs to be manually returned to normal (an option which can be selected whenever a threshold is configured).	“Turned on the A/C”; “Fixed the leak”

"Test Action" display

Use this display to test an alert action after it is created or modified.

Note: You need to verify the test was successful: the display does not report test failures. For example, for **Send SNMPv1 Trap**, verity the trap was received at the trap receiver, or for **Send E-mail**, verify the e-mail was received.

"Choose Next Action" display

Use this display to choose whether you want to use the "Alert Actions" wizard to create, modify, or delete another alert action, access the "Alert Profiles" wizard to manage alert profiles, or exit the wizard.

Alert Profiles option

This option accesses the "Alert Profiles" wizard used to create and edit the profiles the InfraStruXure Central and NetBotz Appliances use to generate alert notifications.

A default alert profile exists for the InfraStruXure Central server, as well as at each NetBotz Appliance. This default profile cannot be deleted, but it can be edited and renamed. In addition to the default profile, you can create your own custom alert profiles at the InfraStruXure Central or at each NetBotz Appliance.

Note: Alert actions, alert profiles, and alert thresholds set on a NetBotz Appliance are actually stored on, and triggered from, the NetBotz Appliance; alert actions, alert profiles, and alert thresholds set on InfraStruXure Central server devices (excluding NetBotz Appliances) are stored on, and triggered from, the InfraStruXure Central server.

The following table identifies which alert profiles can be used for which alarms.

Alarm type	Profile
Alert thresholds defined in InfraStruXure Central for monitored SNMP device sensors	Any profile defined on the InfraStruXure Central server that is associated with an SNMP device sensor's threshold settings using an **Alert Thresholds** option.
InfraStruXure Central alarms that are reported automatically from monitored APC SNMP devices	Any profile defined on the InfraStruXure Central server that is associated with an SNMP device using **Device Settings**, an **SNMP Device Settings** option in the **Settings** menu.
Alert threshold violations from NetBotz Appliances	Any profile defined on the NetBotz Appliance. Each appliance has its own set of profiles.
Note: An alert profile must include at least one alert action before it can be used to generate alert notifications.	

Alert profile sequences

An alert profile must have at least one sequence that includes one or more alert actions defined. When that profile is associated with an alert threshold or other alarm condition, it is the alert profile sequences, and their associated alert actions, that control what alert notifications are generated in response to alarm conditions.

These sequences identify what will happen in response to an alarm condition, and when it will happen. For example, for a sequence that will send an e-mail to user 1, you can do the following:

- Define how many minutes to wait after the alarm occurs before an e-mail is sent to user 1.
- Select to have e-mails continuously sent to user 1 while the alarm remains active, or limit the e-mails to a specific number, as well as how much time will elapse between e-mails.
- Select capture settings for **Graphs**, **Pictures**, and **Maps** that may be included in an e-mail sent by a NetBotz Appliance, or for **Graphs** that may be included in e-mails sent by the InfraStruXure Central server.
- Select the alert action that has been defined to send an e-mail to user 1.

An alert profile can include multiple alert sequences which allow you to customize which alert actions are triggered, and when. For example, if sending e-mails to user 1 has not resulted in an alarm returning to its normal condition within 20 minutes, you can start sending e-mails to user 2, and start sending data to an FTP server.

How many alert profile sequences you use, and what actions they use, will depend on exactly what you want to happen, and when, for alarm conditions, including alert threshold violations, associated with the alert profile.

Managing alert profiles

Use the "Alert Profiles" wizard to add, modify, or delete one profile at a time.

1. Select "Alert Profiles" in the **Settings** menu.
2. In the "Select Parent Device" display, highlight the parent device (InfraStruXure Central server or individual NetBotz Appliance) associated with the profile you want to configure, and click **Next**.

   Note: Only one parent device can be selected: the InfraStruXure Central server is the parent device for the SNMP devices it monitors; each NetBotz Appliance is the parent device for the sensor, camera, and other serial devices, as well as the SNMP devices it monitors.
3. In the "Select Alert Profile" display, do one of the following.
   - Select the existing profile, and click **Next**, to modify that profile's settings.
   - Click **Add Profile**, and then click **Next**, to configure a new profile.
   - Select a profile, and click **Remove Profile**.
     Note: If you delete a profile that is associated with an alert threshold, or with an InfraStruXure Central SNMP device, the alert threshold, or SNMP device, will then use the default profile.
4. In the "Configure Alert Profile" display, do any of the following, and click **Finish**.
   - Edit the profile's name.
   - Edit the **Suppress Alert Notifications until** settings.
   - Use the **Remove Sequence** button to delete any sequences you no longer want a profile to use.
   - Use the **Add** and **Edit Sequence** buttons to access the "Edit Alert Profile Sequence" display to configure the sequences you want the profile to use.

"Alert Profiles" wizard

This wizard uses a set of displays that step you through the process of adding, editing, or deleting alert profiles.

"Select Parent Device" display

Use this display to select the parent device that can use the alert profile.

Note: Only one parent device can be selected: the InfraStruXure Central server is the parent device for the SNMP devices it monitors; each NetBotz Appliance is the parent device for the sensor, camera, and other serial devices, as well as for the SNMP devices it monitors.

Parent	Description
<server_name>(InfraStruXure Central)	Associates the alert profile with the InfraStruXure Central server for use with alert thresholds or other alarm conditions for its managed SNMP devices.
NetBotz Appliance	Associates the alert profile with the selected NetBotz Appliance for use with its alert thresholds.

"Select Alert Profile" display

Use this display to select the profile you want to manage.

Element	Description
List	Lists the existing alert profiles on the selected parent device.

Add profile	Click to add a new profile.
Remove profile	Click to delete a profile. The default profile, indicated by an asterisk, can never be deleted. **Note:** If you delete a profile that is associated with an alert threshold, or with an InfraStruXure Central SNMP device, the alert threshold, or SNMP device, will then use the default profile.

"Configure Alert Profile" display

Use this display to manage the alert sequences.

Each alert sequence allows you to add a new set of alert actions. Alert sequences allow you to stagger notifications based on the duration of an alarm condition.

Note: The alert profile must be associated with an alert threshold, or with an SNMP device monitored by the InfraStruXure Central server, in order for it to operate.

Element	Description
Profile name	Identify a name for the profile.
List	Identifies the alert sequences associated with the profile, by **Sequence Name**, and their **Delay (minutes)**, **Repeats**, and **Interval (minutes)** values.
Add sequence	Click to add a new alert sequence.
Edit sequence	Click to edit a selected alert sequence.
Remove sequence	Click to remove a selected alert sequence.
Suppress alert notifications	Select to suppress notifications for a defined period of time for the alert thresholds, and monitored SNMP devices, that use the profile.

"Add or Edit Alert Profile Sequence" display

Use this display to add or edit the alert sequences you want a profile to use.

Note: Alert notifications will cease as soon as the triggering event clears; a cleared notification is sent for each alert action, unless the alert action has **Do Not Send Return-to-Normal Messages** selected in the **Advanced** tab of the alert action's configuration display.

Element	Description
Label	Identify a name for the sequence.
Delay (minutes)	Define how long InfraStruXure Central will wait after it becomes aware of a threshold violation, or other alarm, associated with the alert profile, before it generates an alert notification.
Interval (minutes)	Define how long the sequence will wait before it repeats the alert notification.
Repeat (number of times)	Identify how many times the sequence will repeat itself.
Repeat until Alert Cleared	Select to have the sequence repeat itself continuously.
Capture Settings	Select the capture settings for **Graphs**, **Pictures**, and **Maps** that may be included with the sequence's

	alert notifications: **Capture if Requested**, **Always Capture**, or **Never Capture**. **Note:** All capture settings can be used for NetBotz Appliances; for SNMP devices, only graphs can be included in alert notifications.
Actions	**Add Action**: click to add an available alert action to the actions list for the alert sequence. **Note:** Only alert actions available for the parent device selected for the alert profile will be shown. **Remove Action**: click to permanently remove a selected alert action from the alert sequence. **View Action**: click to review or modify a selected alert action's configuration. **Test Action**: click to test a selected alert action.

Alert Thresholds options

The InfraStruXure Central allows you to create alert threshold settings for any sensor value reported for any device.

Two basic types of alert thresholds are available: those that use numeric settings, and those that use state settings.

- Numeric thresholds:
  - **Air Flow**
  - **Amp Detector**
  - **Audio**
  - **Dew Point**
  - **Humidity**
  - **Other Numeric Sensors**
  - **Power (VA)**
  - **Power (Watts)**
  - **Temperature**
  - **Voltage**
- State thresholds:
  - **Door**
  - **Dry Contact**
  - **Motion Sensor**
  - **Other State Sensors**

Both types of thresholds allow you to do the following:

- Create alert thresholds at one time for multiple sensors that monitor the same value (for example, all are **Humidity** sensors, or all are **Door** sensors) at the NetBotz Appliances and SNMP devices monitored by the InfraStruXure Central server.
- Assign any InfraStruXure Central alert profile to a single SNMP device sensor, or to any number of those device sensors at the same time.
- Assign a NetBotz Appliance alert profile to the specific sensor at the NetBotz Appliance the profile was created on, and to all the sensors on the devices it monitors.
- Specify the severity for any defined threshold.

Two menus provide access to the alert thresholds:

- **Alert Settings** in the **Settings** menu: each **Alert Threshold** option allows you to search some or all of the NetBotz Appliances and SNMP devices monitored by the InfraStruXure Central server for sensors that match the selected option. You can then edit or add thresholds for one of those sensors, or configure the same threshold for any number of those sensors, simultaneously.

- Right-click menu in the **Device View** or **Map View**: each **Alert Threshold** option allows you to add or edit alert thresholds for the device, or devices, selected when you right-click to select an option. This allows you to focus the threshold management to the sensors that match the selected option at a single device, or at a limited set of devices.

Alert thresholds and supported devices

Which alert thresholds can be used for sensors at the monitored devices depends on the type of device.

- For a NetBotz Appliance, all alert threshold options, except **Power(VA)** and **Power (Watts)**, can be used to define alert thresholds on camera pods, sensor pods, and other devices managed by the NetBotz Appliance..
- For a full SNMP support device monitored by the InfraStruXure Central server, all threshold options except **Audio**, **Dew Point**, **Door**, **Dry Contact**, and **Motion Sensor** can be used to define threshold settings the InfraStruXure Central server will monitor for that SNMP device.

NetBotz Appliances

When you create alert thresholds for a NetBotz Appliance, its sensor pods, camera pods, and monitored SNMP devices, the threshold settings are set at the NetBotz Appliance. It is the NetBotz appliance that stores the settings and sends the alerts to the InfraStruXure Central server.

Note: Because NetBotz Appliance alert profiles are device-specific, you will not be able to configure the profile for a threshold setting when configuring that setting for multiple appliances.

Full SNMP support devices

When you create alert thresholds for full SNMP support devices, the threshold settings you define are set at the InfraStruXure Central server, and used to monitor the associated sensors at those devices.
Note: This can result in two alarms when an alert threshold you define at the InfraStruXure Central server is violated: one from the SNMP device, and one for the alert threshold violation at the InfraStruXure Central server.

You can define alert thresholds for SNMP devices to do the following:

- Set the threshold settings that the InfraStruXure Central server will monitor for these SNMP devices.
- Select the alert profiles the InfraStruXure Central server will use for alert notifications related to these SNMP devices.

Basic and model ID SNMP support devices

The InfraStruXure Central server can generate alert notifications when it senses that it has lost communication with a Basic or model ID SNMP support device.

For devices without full SNMP support, you can define supplemental OIDs for sensors at those devices using **Supplemental OIDs**, an **SNMP Device Settings** option in the **Settings** menu. Once the supplemental OIDs are defined, you can create alert thresholds on the sensors.

Numeric alert thresholds

Numeric alert thresholds are thresholds defined for sensors that report numeric values.

There are nine specific types of numeric thresholds that can be set on numeric sensors.

Numerical threshold options

- All alert threshold options, except **Power (VA)** and **Power (Watts)**, can be used to set threshold settings at a NetBotz Appliance for itself, its sensor and camera pods, and other devices it manages.
- The **Other Numerical Sensors** and **Other State Settings** options, and for some third-party devices, **Voltage**, can be used to set threshold settings at a NetBotz device for the full SNMP support devices it monitors.
- All threshold options except **Audio**, **Dew Point**, **Door**, **Dry Contacts**, and **Motion Sensor** can be used to define threshold settings the InfraStruXure Central server will use to monitor its full SNMP support devices.

Threshold	Value	Description
Air Flow	**<n> ft/min**	Settings for sensors that measure air movement as feet per minute. **Note:** Sensors that use a different measurement, such as cubic feet per minute (CFM) will be displayed under the **Other Numeric Sensors** option.
Amp Detector	**Amps (0.0 - 100.0)**	Settings for sensors that measure current as total amperage (amps).
Audio	**Relative number (1 - 100)**	Settings for sensors that measure the volume of sound.
Dew Point	**°F (-40.0 - 122.0)/ °C (4.5 - 50.0)**	Settings for sensors that measure dew point as degrees Fahrenheit (°F) or Celsius (°C).
Humidity	**% (0 - 95)**	Settings for sensors that measure relative humidity as a percentage (%).
Other Numeric Settings	**Varied**	Settings for sensors that measure numeric settings not reported for other **Alert Thresholds** options.
Power (VA)	**VA**	Settings for sensors that measure power as total Volt-amperes (VA). **Note:** Sensors that measure power as a percentage of VA will be displayed under the **Other Numeric Sensors** option.
Power (Watts)	**W**	Settings for sensors that measure power as total watts (W).
Temperature	**°F (-40.0 - 122.0)/ °C (4.5 - 50.0)**	Settings for sensors that measure temperature as degrees Fahrenheit (°F) or Celsius (°C).
Voltage	**V**	Settings for sensors that measure either AC or DC voltage as total volts (V).

Numerical threshold types

Setting	Description
Minimum Value Threshold	An alarm occurs when the sensor's value is below the **Minimum** setting.

Maximum Value Threshold	An alarm occurs when the sensor's value is above the **Maximum** setting.
Range Threshold	An alarm occurs when the sensor's value is outside the range defined by the **Minimum** and **Maximum** settings.
Below Value for Time Threshold	An alarm occurs if the sensor's value is below the **Minimum** setting for longer than the **Time Allowed Below Minimum** setting's delay.
Above Value for Time Threshold	An alarm occurs if the sensor's value is above the **Maximum** setting for longer than the **Time Allowed Above Maximum** setting's delay.
Rate of Increase Threshold	An alarm occurs if the sensor value increases by more than the **Maximum Increase** setting since the last time the sensor's value was sampled. For example, at a sensor that measures amps, **1** would result in an alarm when the amps measured by the sensor increases by one amp.
Rate of Decrease Threshold	An alarm occurs if the sensor value decreases by more than the **Maximum Decrease** setting since the last time the sensor's value was sampled. For example, at a sensor that measures total watts (W), **100** would result in an alarm when the watts measured by that sensor goes down 100 watts.

Other numeric thresholds

The **Other Numeric Sensors** option allows you to set thresholds for numeric sensors that monitor values not covered by the nine threshold-specific numeric options.

The following lists identify some common examples of numeric sensors you can configure using the **Other Numeric Sensors** option. The actual sensors will depend on the device types managed by the InfraStruXure Central server.

UPS Battery Sensors:	**Other UPS Sensors**:	**Other Sensors**:
• Battery Age • Battery Runtime Remaining • Battery Capacity Remaining • Time Running on Battery	• UPS Age • Input Frequency • Output Frequency • Output Load • Output Power Percent VA	• Max Number of Output Relays • Max Number of Input Contacts • Runhours of Fan • Air Flowrate of Fan (in cfm) • Total Air Flow (in cfm) • RPM Speed of Fan

State alert thresholds

State thresholds are thresholds defined for sensors that report state values.

There are three specific types of state thresholds that can be set for state sensors.

State threshold options

Threshold	Value	Description
Door	**Open** or **Closed**	Settings for sensors that determine whether a door is open or closed.
Dry Contact	**Unknown**, **No Fault**, or **Fault**	Settings for sensors that determine the fault status of dry contacts.
Motion Sensor	**No Motion** or **Motion Detected**	Settings for sensors that detect motion.
Other State Sensors	**Varied**	Settings for sensors that measure state settings not reported for other **Alert Thresholds** options.

State threshold types

Setting	Description
Alert State Threshold	An alarm occurs when the sensor's state matches the **Alert State** setting.
State Mismatch Threshold	An alarm occurs when the sensor's state does not match the **Normal State** setting. **Note:** This threshold setting is useful for sensors that can report more than two states.
Alert State for Time Threshold	An alarm occurs when the sensor's state matches the **Alert State** setting for longer than the **Time Allowed in Alert State** setting's delay.
State Mismatch for Time Threshold	An alarm occurs when the sensor's state does not match the **Normal State** setting for longer than the time defined by the **Time Allowed in Abnormal State** setting. **Note:** This threshold setting is useful for sensors that can report more than two states.

Other state thresholds

The **Other State Sensors** option allows you to set thresholds for state sensors that monitor operational states not covered by the three threshold-specific, state options.

The following lists identify some common examples of state sensors you can configure using the **Other State Sensors** option. The actual sensors will depend on the device types managed by the InfraStruXure Central server.

These options use the same set of four threshold settings as the other state threshold options.

Note: Although this option typically discovers and lists multiple versions of the same types of sensors, you can configure one sensor at a time, only.

Active/Inactive: • Button	**Fault/No Fault**: • Contact • Input State	**Multiple Statuses:**: • Online • Device Status

• Temperature Override Status **Open/Closed**: • Input Contact • Output Relay • Bypass **On/Off**: • Switch • Outlet • Alarm Device • Test Relay **Other Settings**: • Ethernet Link • UPS Input Voltage (line neutral) • Current Output Phase	**Connected/Disconnected**: • Speakers • External Microphone **Yes/No**: • UPS on Bypass • UPS on Battery • Audio Alarm • Battery Low • Overload • Inverter Off • UPS Over Temperature • Utility Power Failure • Battery Needs Replacement • Battery Fault	• Battery Status • UPS Status • Communication Status • Alarm State • Self-Test • Runtime Calibration • Reason for Last Transfer to Battery • Battery Charge Fault • Rack ARU Operating Status of Fan • ARU Primary Power Present

Managing numerical and state alert thresholds

All numeric and state thresholds use the same basic procedure and displays to add, edit, or delete threshold settings.

Note: The same displays are used to manage the alert threshold settings regardless of whether you select the option in the **Settings** menu, the **Device View** right-click menu, or **Map View** right-click menu, except for the "Select Devices" display that appears only when you use the **Settings** menu options.

1. Select the sensor type you want to manage from the **Settings** menu or **Device View** right-click menu.
    - For a **Settings** menu option, go to step 2.
    - For a right-click menu option, go to step 3.
2. In the "Select Devices" display, select the devices you want to search for threshold settings that match the selected sensor type, and click **OK**.
3. In the "Select Thresholds" display, select the threshold type you want to manage from the **Thresholds** drop-down menu; the display will list alert thresholds that have already been defined for the threshold you select in that menu.
    - Click **Add**, and go to step 4 to define new threshold settings.
    - Select one or more of the listed settings, click **Edit**, and go to step 5 to edit those settings.
    - Select one or more of the existing thresholds, and click **Remove Selected**, to delete those threshold settings.
      Note: If you selected **Other Numeric Sensors** or **Other State Sensors** as the **Alert Thresholds** option, you will only be able to edit or delete one threshold at a time.
4. In the "Select Sensors" display, select the sensor or sensors you want to add alert thresholds for, and click **OK**.

    Note: If the no sensors are available for the selected sensor type, a "No Sensors Found" display will appear.
5. In the "Configure Settings" display, define the **Basic**, **Advanced**, and **E-Mail** tab settings, and click **OK**.
6. In the "Select Thresholds" display, repeat steps 3 through 5, as needed, to edit or add the settings for another **Thresholds** drop-down menu selection, or click **OK**, to exit the wizard.

"Select Devices" display

Use this display, which appears when you select the **Alert Thresholds** option in the **Settings** menu, to select the devices on which you want to create, edit, or remove an alert threshold.

The display lists all the devices monitored by the InfraStruXure Central server or by the discovered NetBotz Appliances. You can click the column headers to sort the list in ascending or descending order.

Column	Description
Parent Device	The IP address or hostname for a NetBotz Appliance, or **<server_name>(InfraStruXure Central)**, for SNMP devices monitored by the InfraStruXure Central server.
Hostname	Identifies a device by its hostname or IP address, when no hostname is defined.
Type	Identifies a device by its type, or by **SNMP Device**, if the InfraStruXure Central server cannot determine the device type.
Model	Identifies a device by its model number, when known.
Location	Identifies the location of a device, when known.

"Select Thresholds" display

Use this display to edit or delete existing alert thresholds, or to add a new alert threshold.

The display lists all the settings currently defined for the **Thresholds** selection.

Element	Description
Thresholds	Select the alert threshold you want to view in the display.
Filter	Filter the list based on text you enter in this box: only existing thresholds that contain the text you type are listed.
List	Select the previously defined threshold settings that you want to edit or delete. The following information is provided for the listed threshold setting. **Threshold Name**: the name of the threshold setting. **Parent Device**: either **<server_name>(InfraStruXure Central**) for a monitored SNMP device, or the IP address of hostname of the NetBotz Appliance that monitors a camera pod, sensor pod, or other device. **Monitored Device**: the device for which the alert thresholds are displayed. **Sensor**: the sensor with the defined setting.
Edit	Click to edit a selected alert threshold.
Remove Selected	Click to delete a selected alert threshold from the list.

Add	Click to add an alert threshold for the selected sensor.

"Select Sensors" display

Use this display to select the sensor or sensors on which you want to configure the alert threshold.

Element	Description
Filter	Filter the list based on text you enter in this box: only sensors that contain the text you type are listed.
List	Select the sensors at which you want to define the alert threshold. The following information is provided for the listed sensors. **Parent Device**: indicates whether the device is monitored by the InfraStruXure Central server or by a NetBotz Appliance. **Monitored Device**: the device that reports the sensor values. **Current Reading**: the current sensor value. **Sensor**: the name of the sensor.

"No Sensors Found" display

This display appears when there are no sensors that use the selected alert threshold setting. Click **Cancel**, to return to the "Select Thresholds" display.

"Configure Settings" display

Use this display to configure the **Basic** tab settings for the identified threshold. The **Advanced**, and **E-mail** tab settings are optional.

In addition to the settings provided by the three tabs, the display also identifies the name of the sensor (**Sensor Type**) and value currently read by the sensor (**Current Reading**), and allows you to define a name for the threshold setting (**Threshold Name**).

Basic threshold settings tab:

Element	Description
Threshold value	Define the criteria for the alert threshold. **Note:** The available value fields will depend on the type of numerical or state threshold selected.
Enabled	Select to enable the alert threshold, if it is disabled. **Note:** Thresholds are enabled by default.
Severity	Select the severity you want associated with the alert threshold: **Information**, **Warning**, **Error**, **Critical**, or **Failure**.
Profile	Select the **Alert Profile** you want to use for notifications generated in response to violations of the alert threshold.

View Profile	Click to view or edit the selected **Alert Profile**. **Note:** Any edits you make to an **Alert Profile** will take affect everywhere that profile is used.

Advanced threshold settings tab:

Element	Description
Return-to-Normal Delay	Define a delay, in seconds, that will occur after a threshold setting is no longer violated before the alarm condition clears. This delay helps prevent multiple alarms for values that may rapidly switch between alarm and non-alarm conditions before a problem finally clears.
Return-to-Normal Requires User Input	Select to clear a threshold violation only when a user with **Administrator** privileges marks the alert condition as resolved.
Cameras to Trigger	Select the camera pod or pods you want to have capture images that a NetBotz Appliance can include in alert notifications. **Note:** This only applies to alert thresholds created on NetBotz Appliance pods and devices.
User-specified URL	Identify an Internet address you want included in an alert notification for the alert threshold.
User-specified Description	Provide a description you want included in a threshold's alert notifications.

E-mail threshold settings tab:

Element	Description
Threshold-specific Addresses	Manage a list of e-mail or wireless SMS destination addresses you want to associate with the alert threshold. All e-mail addresses use the standard e-mail format: user@mycorp.com The wireless SMS destinations can be used by any NetBotz Appliance that has an SMS-capable modem installed in, or connect to, that appliance, to send messages to SMS-enabled devices. The addresses used for wireless SMS must use 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: The e-mail and SMS destination addresses can be used only by **Send E-mail**, **Send Short-message E-mail**, and **Send Wireless SMS Message** alert actions that are enabled to use threshold-specific addresses: the alert action has **Include Threshold-specific Addresses** selected. For example: • A “generic_send_email” alert action is created with no e-mail addresses included. • **Include Threshold-specific Addresses** is selected for this "generic_send_email" action. • The “generic_send_email” alert action is added to an alert profile called “alert_profile1.” • The “alert_profile1” profile is specified for two thresholds, “temp_too_high” and “humidity_too_high.” • The “temp_too_high” threshold has **Threshold-specific Addresses** for User1 and User2, and the “humidity_too_high” threshold has **Threshold-specific Addresses** for User3 and User4. • When “temp_too_high” triggers, only User1 and User2 will receive e-mails. • When “humidity_too_high” triggers, only User3 and User4 will receive e-mails.
Add	Click to add a new e-mail or SMS address to the list.
Remove	Click to delete a selected address from the list.

SNMP Device Settings (Settings menu)

Provides options used to configure the settings the InfraStruXure Central server uses for FTP and SNMP communication with its monitored SNMP devices.

Device FTP Settings option

Use this option's "Device FTP Settings" display to manage the FTP access values for APC SNMPv1 and SNMPv3 devices.

The server uses FTP communication for two purposes.

- To upload firmware updates to APC SNMP devices.
- To download device definition files (DDFs) from APC SNMP devices that have these files, at discovery.

Note: This display can be accessed by "Device FTP Settings" displays in the "Apply Firmware Updates" wizard, and in the SNMPv1 and SNMPv3 "Device Discovery" wizards, and by **Device FTP Settings**, an **SNMP Device Settings** option in the **Settings** menu.

Element	Description
List	Lists the sets of access settings the InfraStruXure Central server can use for FTP access to APC SNMPv1 and SNMPv3 devices. **Username**: The username used for FTP access to an APC SNMP device. **Port**: The port used for FTP access to an APC device. **Timeout**: How long the server will wait before it considers that an attempt to access an APC device has failed. **Retry Limit**: How many times the server will attempt to access an APC device before it stops trying to access a device.
Add	Click to add an access settings set to the list.
Edit	Click to edit a selected access settings set.
Remove	Click to delete a selected access settings set.

"Edit Device FTP Settings" display

Use this display to add or edit access settings the InfraStruXure Central server can use for FTP access to APC SNMPv1 and SNMPv3 devices.

Note: This display can be accessed by "Device FTP Settings" displays in the "Update Device Firmware" wizard, and in the SNMPv1 and SNMPv3 "Device Discovery" wizards, and by **Device FTP Settings**, an **SNMP Device Settings** option in the **Settings** menu.

Element	Description
Username	Identify the username used for FTP access to an APC device.
Password	Identify the password used for FTP access to an APC device.
Verify Password	Retype the password.
Port	Select the port the server will use for FTP communication with APC devices.
Timeout	Identify how long the server will wait before it considers that an attempt to access an APC device has failed. Click to edit a selected access setting.
Retry Limit	Select the number of times the server will attempt to access a device before it stops trying to access an APC device.

Device Configuration option

Use this option to manage the settings the InfraStruXure Central server uses for SNMPv1 and SNMPv3 communication with its monitored SNMP devices, as well as alert settings the server associates with those devices.

The monitored SNMP devices are listed by **Hostname** (or IP address), and the following information is provided for each:

- **Device Type**
- **Alert Profile** (the profile the InfraStruXure Central server associates with alarms at an APC SNMP device)
- **Protocol** (**SNMPv1** or **SNMPv3**)
- **Port**, **Timeout**, and **Retries** (SNMP communication settings)
- **Last Scan Time** (date and time when the InfraStruXure Central server last scanned a device for status information)

You can edit the **Alert Profile**, **Port**, **Timeout**, and **Retries** settings, as well as settings not identified in the list, by selecting one or more of the listed devices and clicking **Edit Device Configuration**. The following editable settings are not identified in the list.

- **Scan Interval (minutes)**
- **Offline Alert Severity**
- **Priority Scanning**
- **SNMPv1**: **Read** and **Write Community** names
- **SNMPv3**: **User**, **Authentication Protocol, Encryption Algorithm**, and **Authentication** and **Encryption Passwords**

Note: If you select to edit SNMPv1 and SNMPv3 devices at the same time, no **Priority Scanning**, SNMPv1-specific, or SNMPv3-specific settings will appear in the "Edit Device Configuration" display.

"Edit Device Configuration" display

Use this display to edit alert profile, severity, and SNMP communication settings the InfraStruXure Central server uses with its APC SNMP devices.

The display includes elements that are shared by APC SNMPv1 and SNMPv3 devices, as well as **SNMP Settings** elements that are specific to each protocol.

Note: If both SNMPv1 and SNMPv3 devices are selected, the **SNMP Settings** section will not appear in this display.

Shared Element	Description
Hostname	When only one device is selected, identifies the hostname or IP address of that device. **Note:** No **Hostname** is provided when multiple devices are selected.
Offline Alert Severity	Select the severity you want associated with alarms that occur when a selected device goes offline: **Informational**, **Warning**, **Error**, **Critical**, or **Failure**.
Alert Profile	Select the alert profile you want to associate with alarms that are sent from a selected APC SNMP device. **Note:** This profile selected does not change the alert profile specified on any alert thresholds defined for a selected device.
Scan Interval (minutes)	Select how much time will pass between InfraStruXure Central server scans of a selected device for status information: from **1** through **60** minutes, and **Default**, the minutes for which is defined by the **Global SNMP Settings** option's **Scan Interval** setting. **Note:** The more devices the server monitors, the higher the interval should be; if set too low, performance can be affected adversely.
Port	The number of the port used for SNMP communications with a selected APC SNMP device.
Timeout (seconds)	Select how long the InfraStruXure Central server will wait for a response before it considers an attempt to communicate with a selected APC SNMP device has failed.
Retries	Define how many times the InfraStruXure Central server will attempt to communicate with a selected APC device, after the initial attempt failed, before it stops trying to access that device during the current scanning process.

SNMPv1-specific SNMP Settings

Element	Description
Priority Scanning	Select this option to register the InfraStruXure Central server as a trap receiver at a selected device. This allows for faster reporting of errors at that device by the server. As a trap receiver, the server will poll the device as soon as it receives an SNMP trap from that device. As a non-trap receiver, the server reports device alarms during normal scan intervals only.
Read Community	Edit the community name that the server uses to read information from the SNMPv1 device.
Write Community	Edit the community name that the server uses to define itself as a trap receiver at a selected SNMPv1 device.

SNMPv3-specific SNMP Settings

Element	Description
Priority Scanning	Select this option to register the InfraStruXure Central server as a trap receiver at a selected device. This allows for faster reporting of errors at that device by the server. As a trap receiver, the server will poll the device as soon as it receives an SNMP trap from that device. As a non-trap receiver, the server reports device alarms during normal scan intervals only.
User	Identify the username the server uses for secure communication with a selected SNMPv3 device.
Authentication Protocol	Change the protocol (**MD5** or **SHA**), if necessary, selected for the server to use for communication with a selected SNMPv3 device.
Authentication Password/Verify	Type in and verify a new password, if necessary, for the selected **Authentication Protocol**.
Encryption Algorithm	Change the encryption method (**None**, **DES**, or **AES128**), if necessary, selected for the server to use for communication with a selected SNMPv3 device.
Encryption Password/Verify	Type in and verify a new password, if necessary, for the selected **Encryption Algorithm**.

Device Definition Files option

Use this option to manage the Device Definition Files (DDFs) that the InfraStruXure Central server uses to access information about the environmental, power, and cooling sensors at supported SNMP devices.

Each DDF file is designed to provide information about sensors for a particular product set from a specific manufacturer, and contains only the OIDs directly related to that product's capabilities.

Element	Description
Device Definition Files	Lists the DDFs already installed at the InfraStruXure Central server.
Remove	Click to delete a selected DDF from the list. **Note:** Deleting a DDF will affect what sensors the SNMP devices related to that DDF will report.
Add/Update Definitions	Click to access the wizard used to add or update DDF files, when available from APC.

Adding or updating device definition files (DDFs)

Use the "Add/Update Definitions" wizard to add or update the DDFs available for the InfraStruXure Central server's supported SNMP devices. The new or updated DDFs can be uploaded to the InfraStruXure Central server from a local file, or from the APC website.

1. Select **Device Settings**, an **SNMP Device Settings** option in the **Settings** menu.
2. Select the **Device Settings** option in the "SNMP Device Settings" display.
3. Click **Add/Update Definitions** in the **Device Definition Files** tab.
4. In the "Select Update Method" display, select the option you want to use to add or update DDFs, and follow the appropriate instructions.
   - To use files from APC, see step 5.
   - To use file previously downloaded to a local computer, see step 6.
5. To download files from APC, do the following.
   a. Select **Check APC Website** and click **Next**.
   b. In the "Select DDF Files" display, select the files you want to download, click **Next**, and go to step 7.
6. To use a local file, do the following.
   a. Select **Local File** and click **Browse**.
   b. In the "Open" display, navigate to the file you want to use, and double-click that file (or click it once, and then click **Open**).
   c. In the "Select Update Method" display, verify the correct file is identified, click **Next**, and go to step 7.
7. In the "Installed/Updated DDF Files" display, verify the files you selected are listed, and click **Finish**, to exit the wizard, or **Back**, to return to the "Select Update Method" display.

"Add/Update Definitions" wizard

This wizard steps you through the process of adding new Device Definition Files (DDFs), or updating existing files.

"Select Update Method" display

Use this display to select the source of new or updated DDF files.

Element	Description
Check APC Website	Click to see if any new or updated DDF files are available from APC.
Local File	Click to download a DDF file stored on a local computer.
Browse	Click to browse to the DDF file on the local computer.

"Select DDF Files" display

Use this display to select the DDF files you want to download from APC.

Element	Description
List	Select the DDF files that you want to download from APC from the list of available DDFs. Each listing shows the currently installed version and whether a new or updated version is available. **Installed**: The DDF version matches the server's file. **Updated**: The DDF is an updated version of the server's file. **New**: The DDF file is not installed at the server.
Next	Click to download the selected DDF files.

"Installed/Updated DDF Files" display

Use this display to verify that all DDF files were downloaded successfully.

Global SNMP Settings option

Use this option to define the global SNMP settings that the InfraStruXure Central server will use for its communication with its monitored SNMP devices.

Element	Description
Scan Interval	Select how much time will pass between InfraStruXure Central server scans for status

	information at a monitored SNMP device, when the **Device Settings** option in the "SNMP Device Settings display" has **Default** selected for that device's **Scan Interval (minutes)** setting. **Note:** The more devices the server monitors, the higher the default interval should be; if set too low, performance can be affected adversely.
Maximum Route Hops	Identify the maximum number of hops that will be recorded and saved by the route tracing support for the server's SNMP communications.
Include route trace in alerts	Select to enable alert notifications to include route tracing data.

Supplemental OIDs option

Use this option to add supplemental OIDs that define sensors for monitored SNMP devices.

Once a supplemental OID has been added, the InfraStruXure Central server will request it for every SNMP device, with the supplemental OID value reported only by SNMP devices that can report the sensor associated with that OID. This allows the server to monitor and provide alert notifications for the supplemental OID the same way it does for any other sensor for SNMP devices.

You use either the **Other Numeric Sensors** or **Other State Sensors** threshold option, depending on the nature of the data provided by the supplemental OID, to configure alert threshold settings for an SNMP device that has the type of sensor associated with the supplemental OID.

Note: To add a supplemental OID, you need access to the Management Information Base (MIB) that defines the OIDs available to the SNMP device.

Elements	Description
OIDs	Identifies the existing supplemental OIDs. **Sensor Type**: The type of sensor (temperature, humidity, air flow, etc.) that best matches the data reported by the OID. **Unit of Measure** (only available when **Generic** is the **Sensor Type**): The appropriate unit or measurement (degrees, seconds, volts, etc.) used when reporting the sensor data. **OID**: The definition of the OID to be monitored for an SNMP device (for example,. 1.3.6.1.4.1.318.1.1.1.2.2.2). **Description**: A description of the OID (for example, UPS Temperature).
Add	Click to add a new supplemental OID.
Remove	Click to delete a selected supplemental OID.

"Add" Supplemental OID display

Use this display to add a supplemental OID for an SNMP device.

Note: To add a supplemental OID, access to the Management Information Base (MIB) that defines the OIDs available to the SNMP device.

Element	Description
Sensor Type	Select the sensor type.
Unit of Measure	Select the unit of measure, when **Generic** is the **Sensor Type**.
OID	Identify the OID. For example: .1.3.6.1.4.1.318.1.1.1.2.2.2 **Note:** An OID must begin with.1.3.6.1 to be considered valid.
Description	Identify the description for the OID that will appear in the display for the **View Device Sensors** right-click option in the **Device View** and **Map View**. For example, **UPS Temperature**.

NetBotz Appliance Configuration (Settings menu)

The configuration settings at the monitored NetBotz Appliances can be defined using the **NetBotz Appliance Configuration** options, or by using the **NetBotz Advanced View** at each appliance. **NetBotz Appliance Configuration** options allow you to modify those configuration settings, as needed.

Note: Only model 5xx NetBotz Appliances support all the **NetBotz Appliance Configuration** options without any additional software modules. For information about whether a specific model 3xx or 4xx appliance can be configured using a **NetBotz Appliance Configuration** option, access the **NetBotz Advanced View** for that appliance.

With the exception of the **Camera Settings**, **Serial Device Settings**, **SMS Settings**, and **Pod Sharing Settings** options, the **NetBotz Appliance Configuration** options can be used to configure the settings at multiple appliances at the same time, using the same settings at each.

Note: Any of these configuration options can be accessed using right-click **NetBotz Appliance Configuration** options in the **Device View**, **Map View**, and **Device Groups** view; a single right-click option, **NetBotz Appliance Camera Settings**, is available in the **Thumbnails** view to access the **Camera Settings**.

Using the NetBotz Appliance Configuration options

The **NetBotz Appliance Configuration** options all use the same basic configuration procedure, with the exception of **Backup/Restore** and **Camera Settings**.

1. In the **Settings** menu, select a **NetBotz Appliance Configuration** option other than **Backup/Restore** or **Camera Settings**.

   Note: For information about the **Backup/Restore** and **Camera Settings** options, use the related links to the help for these options.
2. In the "Select NetBotz Appliance" display, select the NetBotz Appliance or Appliances you want to configure, and click **Next**.

   Note: The **Serial Device Settings**, **SMS Settings**, and **Pod Sharing Settings** options allow you to configure only one appliance at a time.
3. In the option's settings display, configure the settings you want the selected NetBotz Appliance or Appliances to use, and click **Next**.
4. In the "Results" display, review the configuration results, and click **Finish** when no NetBotz Appliance is reporting that its configuration is still **In Progress**.

   Note: For information about the possible status results, see the "Results" display description.

"Select NetBotz Appliance" display

Use this display to select the NetBotz Appliance, or appliances, you want to configure for the selected **NetBotz Appliance Configuration** option.

Note: The Camera Settings option uses a "Select Camera" display instead of this "Select NetBotz Appliance" display.
This display lists all NetBotz Appliances the InfraStruXure Central server is monitoring.

"Results" display

Use this display to review the result of a configuration activity for the selected **NetBotz Appliance Configuration** option.

Four results can be reported for each NetBotz Appliance you configured.

Note: **Unauthorized** can be reported only when attempting to restore the configuration at an appliance.

Result	Description
In Progress	The configuration is being performed.
Completed	The configuration was successful.
Unknown	Unable to provide a known result. **Recommended Action**: Try configuring the NetBotz Appliance, again. If the problem persists, log on to the **NetBotz Advanced View** at the appliance to see if the settings were applied successfully, and to configure the settings, if needed.
Unauthorized	An incorrect password was provided for the restore activity.

Backup/Restore option

Use this option to store a configuration backup file in the InfraStruXure Central server database for a selected NetBotz Appliance or Appliances, or to use those backup files to restore selected NetBotz Appliance configurations.

The "Backup/Restore" wizard has three displays, two of which are shared with other **NetBotz Appliance Configuration** options, and a password pop-up display.

1. Use the "Select Backup or Restore" display to select whether you want to backup or restore NetBotz Appliances.
2. Use the "Select NetBotz Appliance" display, which is shared with every **NetBotz Appliance Configuration** option except **Camera Settings**, to select the appliances you want to backup or restore.
3. Use the "Backup/Restore Password" pop-up display to define a password used to encrypt backup configurations, or to access the backup files used to restore configurations.
4. Use the shared "Results" display to view the results of the backup or restore activity.

"Select Backup or Restore" display

Use this display to select whether you want to **Backup** or **Restore** the configurations at one or more NetBotz Appliances.

Camera Settings option

Use this option to access the "Camera Settings" wizard used to configure the settings for the cameras at all monitored NetBotz Appliances.

Note: The "Camera Settings" wizard also can be accessed using right-click menu options in the **Device Groups** view and **Device View** (**Camera Settings** in the **NetBotz Appliance Configuration** menu), and **Thumbnails** view (**NetBotz Appliance Camera Settings** option).

The "Camera Settings" wizard has two displays:
Note: You can configure the settings for all listed cameras, one at a time: when done configuring one camera, select another camera in this "Select Camera" display.

"Select Camera" display

Use this display to select the camera for which you want to configure its associated NetBotz Appliance.

What cameras are listed depends the **Camera Settings** option used.
Note: You can configure the settings for all listed cameras, one at a time: when done configuring one camera, select another camera in this "Select Camera" display.

- **Camera Settings**, a **NetBotz Appliance Configuration** option in the **Settings** menu: all cameras at all monitored NetBotz Appliances.
- **Camera Settings**, a right-click **NetBotz Appliance Configuration** menu option in the **Device Groups** view: all cameras at all monitored NetBotz Appliances assigned to the selected device group.
- **Camera Settings**, a right-click **NetBotz Appliance Configuration** menu option in the **Device View**: all selected cameras, or all cameras for the selected NetBotz Appliances.
  Note: When a single camera device is selected, the "Camera Settings" display is accessed directly; when no selected NetBotz Appliance has an associated camera, the **Camera Settings** option is not available.
- **NetBotz Appliance Camera Settings**, a right-click option in the **Thumbnails** view: all cameras for the selected thumbnails.
  Note: When the thumbnail for only one camera is selected, the "Camera Settings" display is accessed directly.

"Camera Settings" display

Use this display to configure the settings at the NetBotz Appliance associated with a selected camera.

Alarm Capture Data

Use this option to define when the selected camera will begin to capture data during an alarm, as well as the quality of the clip generated by the camera for alarms.

Note: The **Alarm Capture Data** settings have nothing to do with how clips are generated for normal surveillance activities. For information about the settings that affect surveillance clips, see Surveillance Settings options under Surveillance feature.

Element	Description
Camera Resolution	Sets the resolution of the images captured by the camera. The available sizes depend on the capabilities of the selected camera. Larger image resolutions will require increased amounts of disk space.
Maximum Rate	Sets the maximum number of frames per second recorded to the disk when a clip is captured. This setting defaults to 1 frame per second.
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 are: **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. A maximum frame rate of 30 frames per second is available only at Normal Quality or lower and only at resolutions up to 640x480. The 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 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.
Post Alert Capture Time (seconds)	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. **Note:** Three alert actions have the **Maximum Camera Pictures** setting: **Send E-mail**, **Send HTTP Post**, and **Send Data to FTP Server**.
Pre-alert Capture Time (seconds)	Specifies the total number of seconds prior to the alert triggering event for which images will be included in alert notifications. The number of pre-alert images that are captured is equal to the **Pre-Alert Capture Time** multiplied by the the **Maximum 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. **Note:** Three alert actions have the **Maximum Camera Pictures** setting: **Send E-mail**, **Send HTTP Post**, and **Send Data to FTP Server**.
Time delay before capturing (seconds)	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 NetBotz Appliances that are capable of capturing audio.
Audio Volume	Specifies the volume at which audio will be captured.
Summary of Alarm Capture Data	Shows a variety of information about the files that will be generated by the camera using the currently selected **Capture Settings**. The information in this field will update automatically as new settings are specified or selected.

Image Settings

Use this option to configure the image quality and other settings (such as **Timestamp Location**) used for the selected camera during alarm and surveillance activities.

Element	Description

Brightness (0-255)	Sets the brightness of the captured image. The value can be set from **0** to **255**.
Gamma Correction	Use this 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 bleached out or too dark.
Video Format	Use to specify the format for transmitted clips. 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	Select 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 NetBotz 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	Select 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. 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). **Note:** This option is not available for use when configuring **Capture Settings** for CCTV Adapter Pods.
Type of Lighting	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.

	Custom: use the **Red balance** and **Blue balance** controls to fine tune the image to your specifications.
Red Balance (1 - 254)	Adjusts the color balance of the image to counteract the effect of the lighting in the clip.
Blue Balance (1 - 254)	Adjusts the color balance of the image to counteract the effect of the lighting in the clip.
Timestamp Location	Use this control to specify the location of the timestamp within the image capture: **None**, **Bottom right**, **Bottom center**, **Bottom left**, **Top right**, **Top center**, and **Top left**.

Masking

Use this option to create masks that will cause motion in user-sepecified image areas to be ignored (**Motion Mask**), or prevent user-specified regions of the image from being seen (**Blockout Mask**) for the selected camera during alarm and surveillance activities.

Note: When switching between the **Motion Mask** and **Blockout Mask** tabs, you may notice a difference in the size or resolution of the displayed **Camera** view. The **Blockout Mask** shows the entire field of view of the camera, while the **Motion Mask** shows the current cropped area of the **Camera** view. If you have limited the view of the camera by zooming in on the displayed image (through the device web interface or the NetBotz Advanced View application), the **Motion Mask** tab will show only the cropped area.

Motion Mask:

Use this tab to configure the camera's motion sensor to ignore movement that is detected in specified regions of the image capture.

Note: A motion mask causes the camera to ignore any detected motion in the masked area. If detected motion would normally cause a clip to be generated, the motion mask prevents any action from being taken. These masks are useful if you want to restrict the camera to movement only in a certain area: for example, monitoring an entryway next to a busy corridor. Using a motion mask, you can block off the corridor, so that only motion through the entryway causes a clip to be generated.

Element	Description
Drawing Mode	Select the **Drawing Mode**. **Mask**: dragging the mouse across the displayed **Camera** view draws a green masking rectangle. After you release the mouse button, the masking rectangle turns light blue. Any motion that takes place behind the blue rectangle will not trigger a clip. **Unmask**: dragging the mouse across the displayed **Camera** view draws a purple rectangle. After you release the mouse button, the rectangle disappears, along with any portion of a masking rectangle that intersects the purple rectangle.

	You can flip back and forth between modes as many times as you like until the motion mask is defined to your liking. Once you are finished, click **Apply** to save your changes. If you want to remove the current mask, click **Revert Masks**. This does not affect masks that you have already saved with the **Apply** button. If you want to remove an applied mask, use the **Unmask** mode.
Area of Motion	Use this setting to specify how large an area of the image capture must change (as determined by the **Sensitivity** value) before the changed image data is considered movement. A lower **Area of Motion** value indicates a smaller area and therefore higher sensitivity.
Sensitivity	Use this setting to specify how much change in a portion of the image capture will be tolerated before the changed image data is considered movement. A lower value indicates less tolerance for change between images and therefore higher sensitivity.
Enable Camera Motion	Select to enable the camera motion sensor.
Show Motion Outline	Select to have a dotted-line outline surround any region of a captured image that is determined to be indicative of motion.

Blockout Mask:

Use this tab to configure a selected camera so that specified areas of the image cannot be seen, when that camera is monitored by a NetBotz Appliance that has the Premium Software Module.

Element	Description
Drawing Mode	Select the **Drawing Mode**. **Mask**: drag the mouse across the displayed **Camera** view to draw a green masking rectangle. After you release the mouse button, the masking rectangle turns light blue. When the surveillance feed is viewed, the masked area will be covered with a light grey rectangle. Any motion that takes place behind the gray rectangle will not trigger a clip. **Unmask**: drag the mouse across the displayed **Camera** view to draw a purple rectangle. After you release the mouse button, the rectangle disappears, along with any portion of a masking rectangle that intersects the purple rectangle. You can flip back and forth between modes as many times as you like until the motion mask is

	defined to your liking. Once you are finished, click **Apply** to save your changes. If you want to remove the current mask, click **Revert Masks**. This does not affect masks that you have already saved with the **Apply** button. If you want to remove an applied mask, use the **Unmask** mode.

Clock Settings option

Use this option's configuration display to edit the date and time settings at the selected NetBotz Appliance or Appliances, or to synchronize the settings with the date and time at an NTP server.

Element	Description
Enable NTP Server	When selected, a Network Time Protocol (NTP) server provides the date and time values at a selected appliance; otherwise, these values are defined by the other **Date** and **Time** elements.
NTP Server 1 - 3	Identify the IP address or hostname of at least one NTP server, when **Enable NTP Server** is selected.
Use Server Time	Click to use the InfraStruXure Central server's time and date settings at a selected appliance, when **Enable NTP Server** is not selected.
Date	Define the date a selected appliance will use, when **Enable NTP Server** is not selected.
Time	Define the time a selected appliance will use, when **Enable NTP Server** is not selected.
Calendar	Displays the date currently defined at a selected appliance, and can be used to define that date, when **Enable NTP Server** is not selected.

DNS Settings option

Use this option's configuration display to identify the name of the domain on which the selected NetBotz Appliance or Appliances reside, as well as the hostname or IP address of the **Primary DNS**, and of the **Secondary** or **Tertiary DNS Servers**, or both, that are available on that domain.

E-mail Settings option

Use this option's configuration display to configure the settings the selected NetBotz Appliance or Appliances can use to send e-mail notifications.

Note: This option's display elements are identical to those used by the **E-mail Settings** option in the "Server Administration Settings" display.

Location Settings option

Use this option's configuration display to edit the location settings at the selected NetBotz Appliance or Appliances.

Elements	Description
Pod/Sensors	Allows you to select a listed device or sensor for which you want to edit the **Location Data**. When a single appliance is selected, the list has the following entries: • NetBotz Appliance • Sensor pods • Output relay pods • Camera pods, with individual sensors • Ethernet link status When multiple appliances are selected, this list provides the following entries, only: • NetBotz Appliances • Sensor pods • Camera pods, without individual sensors **Note:** No listing is provided for output relay pods, or Ethernet link status.
Location Data	Allows you to select the value you want to edit from a wide-variety of standard, location-based values. **Note:** By default, pods, and the Ethernet link status, inherit their NetBotz Appliance settings, and sensors inherit their pod's settings.
Edit	Click to edit a selected location value.

Pod Sharing Settings option

Use this option's configuration display to configure a selected NetBotz 500 or 550 Appliance to host virtual pods for remote NetBotz Appliances, and AP9361 APC NetBotz Rack Access PX - HID devices.

Element	Description
Remote Devices	Identify the remote devices you want to have share their pods with a selected NetBotz 500 or 550 Appliance by using the "Update Remote Device" display to add a new remote device, or edit or delete an existing one.
Shared Pods	With a remote device selected in the **Remote Devices** list, highlight one or more of its pods in this **Shared Pods** list. Then click **Share Remote Pod**, to share the selected pods with the NetBotz 500 or 550 host, or **Stop Sharing Pod**, to stop sharing those pods.

	Note: The NetBotz Appliance entry allows you to select whether you want to share the integrated pods at that appliance.

Pod sharing overview

Pod Sharing enables your NetBotz 500 or 550 Appliance to connect with, and receive data directly from, pod devices integrated with or connected to NetBotz Appliances and AP9361 APC NetBotz Rack Access devices. These shared pods can be an integrated camera or sensor pod, or externally connected pods.

With pod Sharing, a single NetBotz 500 or 550 Appliance acts as a facility host to manage alerts from many other NetBotz Appliances, and AP9361 APC NetBotz Rack Access devices, distributed throughout your network. Once a pod is shared with the host NetBotz 500 or 550 Appliance, it functions as though it were connected directly to that NetBotz appliance. 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 devices.

A NetBotz 500 or 550 host can share pods with RackBotz and WallBotz 320, 350, 420, 450, 500, and 550 NetBotz Appliances, as well as with legacy NetBotz devices that run 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.

It is important to note the following concerning pod sharing.

- The Pod Sharing task can be run only on one device at a time.
- A NetBotz 500 v2.6 or later, or a NetBotz 550, can host remote pods without using the optional Premium Software Module that must be used with earlier NetBotz 500 versions for pod sharing.
- Pods that are not physically connected to a device do not count against the total number of USB-connected devices allowed for the NetBotz Appliance model.
  - A NetBotz 420 supports an additional camera pod and up to four additional non-camera pods.
  - A NetBotz 500 or 550 supports up to four camera pods and up to 17 non-camera pods.
- Frame rate 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, for a Camera Pod 120 connected to a NetBotz 500, the maximum resolution is 1280x1024. However, if the Camera Pod 120 is connected to a NetBotz 420, the maximum is 640x480.

"Update Remote Device" display

Use this display to configure the settings used for HTTP or HTTPS communication between the pod-sharing host and the remote devices.

Element	Description
Host/IP Address	Identify the hostname or IP address of the remote device that has pods you want it to share with the host NetBotz Appliance.

Port	Identify the port used for the communication: default is 80 for HTTP, and 443 for HTTPS.
SSL Options	Select how the Secure Sockets Layer (SSL) protocol will be used for the communication with the remote device: **None**, **Require SSL - No verification**, **Require SSL - Verify certificate**, or **Require SSL - Verify certificate and hostname**.
User ID	Type in the User ID to be used to access the remote device. **Note:** Some remote pod functionality may be unavailable if the user ID is for a user account that does not have **Administrator** privileges.
Password	Type in the password to be used with the User ID to access the remote device.
Confirm Password	Retype the password.
Timeout (seconds)	Define how long, in seconds, the host NetBotz Appliance will wait for a response before it considers an attempt to communicate with a remote device has failed.

Post Alert Data Settings option

Use this option's configuration display to identify the IP or address you want the NetBotz Appliances monitored by your InfraStruXure Central server to send their alert data.

When a NetBotz Appliance is discovered by InfraStruXure Central, the hostname of the InfraStruXure Central is added to the NetBotz Appliance. This enabled the InfraStruXure Central to receive alert postings from the NetBotz Appliance. If your server does not use DNS, you will need to change the alert post entry on the NetBotz Appliance to the IP Address of the InfraStruXure Central server.

Note: This display also can be accessed when using **Network Settings**, a **Server Administration Settings** option in the **Settings** menu, to change the **Public (LAN1)** tab's **Hostname** or **IP Address** settings: when asked if you want to update the NetBotz Appliance post settings, click **Yes**.

Element	Description
Current InfraStruXure Central Hostname	The **Hostname** defined in the **Network Settings** option's **Public (LAN1)** tab.
Current InfraStruXure Central IP Address	The **IP Address** defined in the **Network Settings** option's **Public (LAN1)** tab.
Select the Address to Use for Sending Alert Data	Select an IP address or hostname from the drop-down list, or type in the hostname or IP address you want the monitored NetBotz Appliances to use to post alert data.

Region Settings option

Use this option's configuration display to edit the regional settings at the selected NetBotz Appliance or Appliances.

Element	Description
Locale	Select the locale that best identifies where a selected appliance is physically located, to match a selected NetBotz Appliance's measurements (metric or US standard) and date/time formats to the formats commonly used at that location.
Use 24-hour Time	Select to have a selected appliance use a 24-hour clock.
Time Zone	Select the time zone in which a selected appliance is located.

Serial Device Settings option

Use this option's configuration display to identify the **Port Label** for each serial port at the selected NetBotz Appliance, and the devices that connect to those ports.

You can select **Remove** to delete a port's device reference when the device is disconnected from the NetBotz Appliance.

SMS Settings option

Use this option's configuration display to configure the settings the selected NetBotz Appliance can use for Short-Message Service (SMS) communication.

Basic tab

Element	Description
SIM PIN	For modems that use a SIM (subscriber identification module), identify the PIN (personal identification number) used to unlock that SIM. **Note:** For modems that do not have a SIM, this field must be blank.
Confirm SIM PIN	Identify the SIM PIN, again.
Service Center (SMSC)	Identify the address of the Short Message Service Center (SMSC) 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. **Note:** Entering a value in this field will override automatic SMSC selection.
Destination	Identify the address used to send an SMS to an e-mail destination. When an SMS message needs to be sent to an e-mail destination address, the NetBotz Appliance 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 that address. **Note:** The default value for this field is **0000000000**, the value that works with AT&T Wireless.
Interrupt PPP When an SMS Alert Occurs	Select this option if your modem supports both SMS and Point-to-Point Protocol (PPP) communications, to allow SMS communication to override PPP communication when necessary. If PPP dial-out is active when the NetBotz Appliance 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.

Advanced tab

Element	Description
Send Debug Messages to Syslog	Select to have debug messages forwarded to the syslog host.
Use Default SMS Settings	Select to use the default SMS values for your SMS-capable modem. **Note:** To use custom settings, disable this option and use **Use Protocol Descriptor Unit (PDU)**, **Character Set**, and **Initialization Commands** to specify those customs settings.
Use Protocol Descriptor Unit (PDU)	Select to use the PDU mode when communicating with the modem to send an SMS message. **Note:** PDU mode is more versatile than the default SMS text settings mode, and some modems do not support both modes.
Character Set	Identify the character set to be used when communicating with the modem to send an SMS message.
Initialization Commands	Identify he initialization string to be used for the modem that will send SMS messages.

SNMP Settings option

Use this option's configuration display to configure the Simple Network Management Protocol (SNMP) settings the selected NetBotz Appliance or Appliances can use to communicate with with an SNMP-based Network Management Server (NMS).

Note: Enable SNMP Agent must be selected to configure the settings.

Version 1/Version 2c tab

Use this tab to define the settings an NMS can use for SNMPv1 or SNMPv2c communication with a NetBotz Appliance.

Element	Description
Enable SNMP Agent	Select to enable the SNMP agent settings.
Read-only Community Name	Define the community name used for read-only SNMP requests.
Confirm Name	Confirm a new or edited **Read-only Community Name** definition.
Read/Write Community Name	Define the community name used for read and write SNMP requests.
Confirm Name	Confirm a new or changed **Read/Write Community Name** definition.
Port	Identify the number of the port used for SNMP agent communication.

Version 3 tab

Use this tab to identify the settings that an NMS can use for SNMPv3 communication with a NetBotz Appliance.

Element	Description
Users	Select the user accounts an NMS can use to connect to the SNMPV3 Agent on a selected NetBotz Appliance.
Authentication Protocol	Select **SHA-1** or **MD5** as the protocol used when sending SNMPv3 informs to the target device.
Encryption Algorithm	Select whether encryption will be used with the SNMPv3, and if used, which protocol: **None**, **DES**, or **AES-128**.

User Settings option

Use this option's configuration display to manage the users at the selected NetBotz Appliance or Appliances, as well as to select the severity of logon failures, and the alert profile used for the alert notifications for those failures.

Users

A **Users** list identifies the users by **Name**, **Username**, and **Privilege Set**., and **Add**, **Edit**, and **Delete** buttons allow you to manage that list.

The "Add User" and "Edit User" displays have standard account **Name** and logon values (**Username**, **Password**, and **Verify Password**). They also have a **Privilege Set** drop-down menu used to select the access a user will have at the selected NetBotz Appliances.

Note: You cannot delete the **Guest Account**, and can only edit its **Privilege Set**; you can edit the **Name**, **Username**, and **Password** values for the default administrator, but you cannot delete it, or change its **Privilege Set**.

Privilege	Description
None	Allows no access to any features.
Administrator	Allows access to all information and configuration tasks at a selected appliance.
Sensor (No camera)	Allows access to the **Navigation** pane, **Sensor Data** pane, **Map View** (if enabled), and selected portions of the **NetBotz Advanced View** information and action views, as well as the ability to view the **Graphs View** and **About** view. This **Privilege Set** does not allow access to the **Cameras View**, **Alerts View**, or **Configuration** view.
Sensor	In addition to **Sensor** (**No Camera**) access, allows access to the **Cameras View**. This Privilege Set does not permit access to the **Alerts View** or **Configuration** view.
Application	Allows access to the **Navigation** pane, **Sensor Data** pane, **Map View** (if enabled), and selected portions of the **NetBotz Advanced View** information and action views. Also allows viewing the **Camera View**, **Graphs View**, **Alerts View**, and **About** view. This **Privilege Set** does not permit access to the **Configuration** view, or the ability to resolve alert conditions for thresholds configured with the **Return-To-Normal Requires User Input** setting selected for their **Advanced Settings**.
Application (with Alert Update)	In addition to **Application** access, allows the ability to resolve alert conditions for thresholds configured with the **Return-To-Normal Requires User Input** setting selected for their **Advanced Settings**. This **Privilege Set** does not permit access to the **Configuration** view.

Logon alerting

Provides two drop-down menus, one which selects the alert profile you want a selected NetBotz Appliance (greyed out when multiple appliances are selected) to use for alert notifications for logon failures, and one which selects the severity you want assigned to logon failures at the selected appliance or appliances: **Informational**, **Warning**, **Error**, **Critical**, and **Failure**.

Note: **Default**, for **Logon Failure Alert Profile**, and **Failure**, for **Logon Failure Alert Severity**, are the default settings.

Web Server Settings option

Use this option's configuration display to select the **HTTP** protocol, **HTTPS** protocol, or both, and define the **Port** number for each, that the selected NetBotz Appliance or Appliances can use for web-based communication.

Surveillance Settings (Settings menu)

Use this option's "Surveillance Settings" wizard configure how the InfraStruXure Central server affects, and responds to, its monitored NetBotz Appliance cameras.

The wizard has four displays:

- "Select Camera Type" display: select the type of camera you want to configure.
- "Select Surveillance Devices" display: select the camera or cameras you want to configure.
- "Camera Settings" display: configure the settings the InfraStruXure Central server uses to affect, and respond to, its monitored NetBotz Appliance cameras.
- "Configured Surveillance Device" display: view a list of the cameras that were configured successfully.

  Note: For more information about the "Surveillance settings" wizard displays, and the **Surveillance Settings** options available in the **Thumbnails** and **Device Groups** view (when viewed in the **Surveillance** perspective), see Surveillance Settings options under Surveillance feature.

Graphing and Reporting (Settings menu)

Use the **Scheduled Export Configuration** option to manage the export configurations that are used to export reports on a scheduled basis.

Note: A **Scheduled Export Configuration** button icon in the **Saved Reports** view also accesses the "Scheduled Export Configuration" display. For more information about the **Scheduled Export Configuration** option and icon, and about the right-click **Graphing and Reporting** options available in various views, see Graphing and reporting feature.

Server Administration Settings (Settings menu)

This menu option accesses "Server Administration Settings" display options used to access settings that directly affect the operation of your InfraStruXure Central server.

Note: For information about the **Users and User Groups** option, see Users and user groups.

E-mail Settings option

Use this option's elements to enable your InfraStruXure Central server to send e-mail notifications.

This option has two tabs (one for the **Primary** SMTP server, one for the **Backup**), each with the same elements, as well as the **From address** field definition used for InfraStruXure Central server e-mail notifications.
Note: These settings are used by the InfraStruXure Central server to send e-mail alert notifications for monitored SNMP devices, and for e-mail messages related to InfraStruXure Central server functions, such as storage disk status and repository purge messages.

Element	Description
"From" address	Define the address that will identify that the e-mails are sent by the InfraStruXure Central server.
SMTP Server	Identify the hostname or IP address of the Simple Mail Transport Protocol (SMTP) server to be used by the InfraStruXure Central server.
Port	Identifies the number of the port at the SMTP server used for communication with the InfraStruXure Central server.
SSL	Select to use the Secure Sockets Layer (SSL) protocol for communication between the InfraStruXure Central and SMTP servers.
Requires Logon	Select to define the **Username** and **Password**, the InfraStruXure Central server must use to log on at the SMTP server. **Note:** Enable this option only when using an SMTP server that requires logon access.

License Keys option

Use this option's elements to enter the license keys for the InfraStruXure Central Device Packs that identify how many devices the server can monitor, and for any applications that need access to information about those monitored devices, at the server.

Note: Change Manager and Capacity Manager are examples of applications that need to have license keys entered at the InfraStruXure Central server.

Element	Description
List	Identifies the license keys by **License Type**, and for **InfraStruXure Central Device Packs**, the number of devices each pack enables the server to monitor (**Node Count**), and how many of those devices are being monitored (**Used Node Count**).
Add License Key	Click to add a license key to the list.

NetBotz Appliance Credentials option

Use this option's elements to manage the list of credentials used for communication with the NetBotz Appliances.

Note: This option uses the same elements as the "NetBotz Appliance Credentials" display in the "Update Device Firmware" wizard. A change made to either, affects both.

Element	Description
List	Lists the available credentials, and identifies **Username**, **Password**, **IP Range**, and **Port Range** values for each. **Note:** A default **NetBotz** credential is provided, as well as a default **APC** credential used to communicate with NetBotz Appliances on the private LAN.
Add	Click to add a new credential.
Edit	Click to edit a selected credential.
Remove	Click to remove a selected credential.

"Add/Edit Credentials" display

Use this display to add or edit the credentials used for communication with the NetBotz Appliances.

Note: This display is accessed from the "NetBotz Appliance Credentials" display in the "Apply Firmware Updates" wizard, and from the **NetBotz Appliance Credentials** option in the "Server Administration Settings" display.

Element	Description
Username	Identify the username a credential will use to access NetBotz Appliances.
Password	Identify the password a credential will use to access NetBotz Appliances.
Verify Password	Retype the password.
IP Range	Define the range of IP addresses at which the credential can be used to communicate with NetBotz Appliances. For example:

	xxx.xxx.12.6: assigns a credential to a single IP address. **xxx.xxx.10-13.20-80**: assigns a credential to a specific set of IP addresses (20 through 80) at the 10, 11, 12, and 13 subnets. **xxx.xxx.14.***: assigns a credential to all IP addresses at subnet 14.
Port Range	Define the range of ports that a credential uses to access NetBotz Appliances. For example: **80**: uses port 80 only (the default value). **60-80**: uses ports 60 through 80, inclusive.

NetBotz Appliance Polling option

Use this option's elements to define how often the InfraStruXure Central server will start a new poll of its monitored NetBotz Appliances, for sensor and alert data (**Data Collection**), and device status (**Monitoring**), or to manually initiate a poll.

Click **Start** in the **Data Collection** section to poll the NetBotz Appliances for sensor and alert data; click **Start** in the **Monitoring** section to poll the NetBotz Appliances for device status.

Network Settings option

Use this option's elements to define the settings the InfraStruXure Central server uses to communicate on its public and private local area networks (LANs), as well as settings used while discovering devices on the private LAN.

Note: To apply changes in the **Public LAN1** or **Private LAN2** tabs, you must click **OK** when asked if you want to restart the server. You can log on after the server finishes rebooting, which can take a few minutes.

Public (LAN1) tab

Use this tab to define the settings the InfraStruXure Central server will use to communicate on the public LAN, the port for which is labeled **1** on the InfraStruXure Central server.

Note: Changes are applied only in response to a InfraStruXure Central server reboot.

Element	Description
Hostname	Identify the InfraStruXure Central server's hostname.
IP Address	Identify the public network address of the server.
Subnet	Identify the TCP/IP subnet address for the server's local network segment.
Gateway	Identify the IP address of the gateway.

Domain	Identify the name of the network domain on which the server resides.
Primary DNS	Identify the IP address of the primary Domain Name Service (DNS) server used to map IP addresses to domain names.
Secondary DNS	Identify the IP address of the DNS server used when the primary DNS server is busy or off-line.
Tertiary DNS	Identify the IP address of the DNS server used when the primary and secondary DNS servers are busy or off-line.

Private (LAN2) tab

Use this tab to define the settings the InfraStruXure Central server will use to communicate on the private LAN, the port for which is labeled **2** on the InfraStruXure Central server.

Note: Changes are applied only in response to a InfraStruXure Central server reboot.

Element	Description
IP Address	Identify the private network address of the InfraStruXure Central server.
Subnet Mask	Identify the TCP/IP subnet address for the local network segment. **Note:** When **Enable Private DHCP LAN** is selected, the **Subnet Mask** selection defines this address; otherwise, type in the subnet mask's IP address.
Enable Private DHCP LAN	Select to use the InfraStruXure Central server as a Dynamic Host Configuration Protocol (DHCP) server for the devices on the private LAN.
Private DHCP LAN	**When enabled**:
Starting and Ending IP Address	Define the range of IP addresses available to the DHCP LAN. The first two parts of the four-part IP addresses are defined by the **IP Address** value, while the last two parts are initially defined by the **Subnet Mask** selection. **Note:** You can edit the last 2 IP address values, except you cannot increase the Ending IP Address value: **Total available addresses** changes to **Invalid IP range** if you do.
Subnet Mask	A list of subnet mask addresses, each providing a different **Starting** and **Ending IP Address** range.
Total Available Addresses	Identifies how many addresses are available, based on the **Starting** and **Ending IP Address** range.

Private (LAN2) Discovery tab

Use this tab to define settings the InfraStruXure Central server will use when discovering SNMPv1 devices, or devices that use the APC DCal1 protocol, on its private Dynamic Host Configuration Protocol (DHCP) LAN.

Note: Changes are applied without an InfraStruXure Central server reboot.

Element	Description
Private Discovery Settings	**Enable Private DHCP Discovery**: Select to enable the InfraStruXure Central server to automatically discover any SNMPv1 devices, or devices that use the APC DCal1 protocol, on the private network. All other private network devices can be discovered by a device discovery process that searches the private network's IP addresses. **Read Community Name**: define the name to be used to discover SNMPv1 devices (**public** is the default).
Trap Registration	**On Discovery, Register for Priority Scanning (SNMP Trap Directed Polling)**: select to register the InfraStruXure Central server as a trap receiver at a selected APC SNMPv1 device. This allows for faster reporting of errors at that device by the server: as a trap receiver, the server will poll the device as soon as it receives an SNMP trap from that device; as a non-trap receiver, the server reports device alarms during normal scan intervals only. **Note:** Only APC SNMPv1 devices discovered after this option is selected have the InfraStruXure Central server registered as a trap receiver. **Write Community Name**: define the name that can be used to register the InfraStruXure Central server as a trap receiver at discovered APC SNMPv1 devices (**private** is the default).
Reset APC Devices	Click to reset private LAN APC devices to use new IP addresses. **Note:** The **Write Community Name** is used to reset the APC devices.

Remote Monitoring option

Use this option's elements to register the InfraStruXure Central server for the Remote Monitoring Service (RMS) support available from APC, and to select the devices you want RMS to monitor.

The **Remote Monitoring** option has two tabs.
Note: For a review of the features and benefits that RMS offers, visit the RMS website: http://rms.apc.com .

Configure RMS tab

Use this tab to register the InfraStruXure Central server with APC's Remote Monitoring Service (RMS), to change any RMS registration after you have registered, or to tie an existing RMS account to the InfraStruXure Central server.

RMS can remotely monitor your InfraStruXure Central server and the devices it manages, and notify you of events via e-mail, pager, or phone.

Element	Description
Registration Settings	Click to register an RMS customer for the InfraStruXure Central server, or to edit the settings for an existing RMS customer.
Enable RMS	Select to enable RMS, or deselect to disable RMS, after the server is registered for this support. **Note:** RMS is disabled, by default.
Send Test Event	Click to send an event to the user account associated with the RMS registration, to ensure that the InfraStruXure Central server is communicating with RMS.
http://rms.apc.com	Click to access the RMS web site for more information about this feature, or to log on as a registered RMS customer.

RMS Devices tab

Use this tab to review which of the InfraStruXure Central server devices are being monitored by RMS.

Element	Description
List	Identifies the devices that an InfraStruXure Central server monitor, by **Hostname**, **Type**, **Model**, and **Location**. A **Monitored** column identifies which devices are monitored by RMS.
Re-register Devices	Click to re-register the devices with RMS.
Refresh Device List	Click to refresh the device list when changes have been made to the devices monitored by RMS.

Registering for RMS support

You use the **Configure RMS** tab to create an account with APC's RMS service, and register your InfraStruXure Central server with RMS.

1. In the the **Settings** menu, select **Server Administration Settings**.
2. In the "Server Administration Settings" display, select **Remote Monitoring**.
3. In the **Configure RMS** tab, click **Registration Settings**.
4. In the "Choose RMS Settings Type" display, select **New Customer**, and click **Next**.
5. In the "RMS Contact Information" display, provide the required information, and click **Next**.
6. In the "RMS Company Information" display, provide the required information, and click **Finish**.
7. Contact RMS for information about how to complete the registration of the InfraStruXure Central server and its monitored devices.

   Note: The telephone number is provided by the **Contact Us** link at the RMS website: http://rms.apc.com .

Editing RMS customer settings

You can use the "Registration Settings" wizard to edit your RMS customer settings if any of your contact or company information has changed.

Note: You can logon at the RMS website to edit an existing RMS customer's settings, as well: http://rms.apc.com .

1. Select **Server Administration Settings** in the **Settings** menu.
2. In the "Server Administration Settings" display, select the **Remote Monitoring** option.
3. In the **Configure RMS** tab, click **Registration Settings**.
4. In the "Choose RMS Settings Type" display, select **Existing Customer** and click **Next**.
5. In the "RMS Logon Settings" display, enter the RMS customer's **Username** and **Password** and click **Next**.
6. In the "RMS Contact Information" display, edit the information, as needed, and click **Next**.
7. In the "RMS Company Information" display, edit the information, as needed, and click **Finish**.

   Note: You do not need to contact RMS for changes made to RMS customer settings.

"Registration Settings" wizard

This wizard's displays step you through the process of registering an RMS customer for the InfraStruXure Central server, or editing the settings for an existing RMS customer.

"Choose RMS Settings Type" display

Use this display to select whether you want to register a RMS customer for the InfraStruXure Central Server for the first time (**New Customer**), or to access the settings for any existing RMS customer (**Existing Customer**).

Note: You cannot register more than one RMS customer for an InfraStruXure Central server, or other device.

"RMS Logon Settings" display

Use this display to access an existing RMS customer's settings by providing that customer's **E-mail** address and **Password**, whether that customer was registered for the InfraStruXure Central server or other device.

Note: This display only appears when you select Existing Customer in the "Choose RMS Settings Type" display.

"RMS Contact Information" display

Use this display to configure the contact information, including logon values, for a new or existing RMS customer.

Note: All information must be provided, except **Title**. No contact information is used by APC for anything other than providing support for the new or existing RMS customer.

"RMS Company Information" display

Use this display to provide company information for a new or existing RMS customer.

Note: No contact information is used by APC for anything other than providing RMS customer support; all information must be provided, except **Address 2**.

Server Access option

Use this option's elements to enable, disable, and configure settings associated with the four different network-accessible processes that can run on your InfraStruXure Central server: web server, SSH daemon, SNMP daemon, and SOCKS proxy.

Web Server tab

Use the top section of this tab to enable or disable HTTP and HTTPS web communication and identify the IP port the InfraStruXure Central server uses for each type of communication. Use the SSL Certificate section to manage (add, edit, or delete) the current Secure Socket Layer (SSL) certificate used for HTTPS communication.

HTTP and HTTPS settings

Note: Enabling and disabling HTTP or HTTPS access, or changing the ports used, can prevent devices from providing data to your InfraStruXure Central server.

Option	Description
Enable HTTP Port	Select to enable the InfraStruXure Central server to use HTTP, a non-secure Internet protocol, for web communication at the defined IP port.
Enable HTTPS Port	Select to enable the InfraStruXure Central server to use HTTPS, a secure Internet protocol, for web communication at the defined IP port.

Note: IP ports 1 - 65535 are valid, with the exception of ports 20, 21, 22, 23, 25, 123, 161, 162, and 389. These are ports reserved for use by NetBotz Appliances and by well-known protocols. Using these reserved ports creates a conflict that can result in operational difficulties.

SSL Certificate

This section provides information about the current SSL certificate, and allows you to modify that certificate, or, when a 3rd-party signed certificate is used, delete that certificate.

The InfraStruXure Central server generates a default, self-signed SSL certificate that can be used for secure HTTPS web communication. Two buttons are available to manage this certificate:

- **Modify Certificate**: used to access the "Modify Server SSL Certificate" wizard to add or create a new certificate.
  Note: Only enabled when the default, self-signed SSL certificate is in use.
- **Delete Signed Certificate**: used to remove a signed 3rd-party SSL certificate and revert back to using the default SSL certificate generated by the InfraStruXure Central server.
  Note: Only enabled when the default, self-signed SSL certificate has been replaced by a 3rd-party certificate.

Modifying the SSL certificate

You can use the "Modify Server SSL Certificate" wizard to create or add a new certificate. You also can create a certificate signing request to send to a certificate signing authority.

Creating a new self-signed certificate:

1. In the Web Server tab for the "Server Administration Settings" display's **Server Access** option, click **Modify Certificate**.
2. In the "Choose Certificate Action" display, select **Create New Self-Signed Certificate** and click **Next**.
3. In the "Specify Certificate Parameters" display, edit the parameters, as needed, and click **Next**.

   Note: **Country** is limited to two alphabetical characters.
4. In the "Update Certificate" display, click **Finish** to overwrite the default SSL certificate with a new, self-signed SSL certificate created by the InfraStruXure Central server.

   Note: You can log on to the server again after it finishes rebooting.

Creating a certificate signing request (CSR):

Use this procedure to create a certificate signing request to send to a certificate signing authority.

1. In the Web Server tab for the "Server Administration Settings" display's **Server Access** option, click **Modify Certificate**.
2. In the "Choose Certificate Action" display, select **Create Certificate Signing Request (CSR)** and click **Next**.
3. In the "Specify Certificate Parameters" display, edit the parameters, as needed, and click **Next**.

   Note: **Country** is limited to two alphabetical characters.
4. In the "Copy Certificate Signing Request" display, copy the provided CSR text to a text file.

   Note: You can manually select the text and use Ctrl+C, or right-click anywhere in the text to use the **Select All** and **Copy** options, to copy the CSR text.
5. Submit the CSR to the appropriate 3rd-party certificate authority for signing.
6. Use the **Add Certificate** option in the "Choose Certificate Action" display to add the newly signed certificate at the InfraStruXure Central server.

Adding a new signed certificate:

Use this procedure to import a 3rd-party signed SSL certificate.

1. In the Web Server tab for the "Server Administration Settings" display's **Server Access** option, click **Modify Certificate**.

2. In the "Choose Certificate Action" display, select **Add Certificate** and click **Next**.
3. In the "Add Certificate" display, use Ctrl+V to paste a copy of the certificate in the text box, or click **Import Certificate** to import the certificate from its text file, and click **Next**.
4. In the "Update Certificate" display, click **Finish** to overwrite the current SSL certificate with the new SSL certificate.

   Note: You can log on to the server again after it finishes rebooting.

"Modify Server SSL Certificate" wizard

Use this wizard's displays to create self-signed certificates, add signed Secure Socket Layer (SSL) certificates that the InfraStruXure Central server can use for secure, SSL-based HTTPS web communication, and to create a certificate signing request to send to a certificate signing authority.

"Choose Certificate Action" display:

Use this display to choose the action you want to perform using the "Modify Server SSL Certificate" wizard.

- **Create New Self-Signed Certificate**: replace the default SSL certificate with a new signed certificate generated by the InfraStruXure Central server.
- **Create Certificate Signing Request (CSR)**: use a CSR to access a copy of a new signed certificate to be imported using the **Add Certificate** option.
- **Add Certificate**: replace the current SSL certificate with the SSL certificate acquired using the **Create Certificate Signing Request (CSR)** option.

"Specify Certificate Parameters" display:

Use this display to edit the certificate parameters when creating a self-signed certificate (**Create New Self-Signed Certificate** selected in the "Choose Certificate Action" display) or when creating a certificate signing request (CSR) (**Create Certificate Signing Request (CSR)** selected in the "Choose Certificate Action" display).

Edit the parameters, as needed.
Note: **Country** is limited to two alphabetical characters.

"Copy Certificate Signing Request" display:

Use this display to copy (Ctrl+C) the provided CSR text to a text file you use to submit the CSR to a 3rd-party certificate authority for signing.

Note: The resulting SSL certificate can be imported to the InfraStruXure Central server using the **Add Certificate** option in the "Choose Certificate Action" display.

"Add Certificate" display:

Use this display either to paste a copy (Ctrl+V) of a signed SSL certificate or to import an SSL certificate using the **Import Certificate** button.

"Update Certificate" display:

Use this display to overwrite the current SSL certificate with a self-signed certificate that was created by the InfraStruXure Central server (**Create New Self-Signed Certificate** selected in the "Choose Certificate Action" display) or with a 3rd-party certificate that is imported to the server (**Add Certificate** selected in the "Choose Certificate Action" display).

Note: When you click **Finish**, you can log on to the server again after it finishes rebooting.

SSH Server tab

Use this tab to enable Secure Shell (SSH), a program that provides strong authentication and secure communications over insecure channels, to be used to log on at an InfraStruXure Central server over a network, from a command line, to execute commands at that server.

Note: Your InfraStruXure Central server supports SSH connections, but this support is primarily intended for use with APC support guidance in troubleshooting device issues.

Option	Description
SSH is currently running	Select to allow SSH access to the InfraStruXure server.
SSH starts at boot time	Select to start SSH whenever the server is turned on or rebooted.

SNMP Server tab

Use this tab to enable or disable the use of an SNMP agent at your InfraStruXure Central server, to define the community names and port setting used for SNMP access to monitored devices, and to identify the contact and location information for the server.

Element	Description
Enable SNMP Agent	Select to enable the SNMP agent settings.
Read-only Community Name	Define the community name used for read-only SNMP requests.
Read/Write Community Name	Define the community name used for read and write SNMP requests.
Port	Identify the number of the port used for SNMP agent communication.
System Contact	Identify the contact person for the InfraStruXure Central server.
System Location	Identify the location of the InfraStruXure Central server.

SOCKS Proxy tab

Use this tab to enable or disable the InfraStruXure Central server's built-in SOCKS v5 proxy server. This proxy server, which uses port 1080, allows users with proxy access to access devices that reside on the private DHCP LAN, by accessing the InfraStruXure Central server from the public LAN.

Server Backup/Restore option

Use this option's elements to automatically, on a scheduled basis, or manually create backup files for your InfraStruXure Central server's configuration data, or its configuration and repository data, and to use a backup file to manually restore the server data, if needed.

Note: If a server backup fails, an e-mail is sent to the **InfraStruXure Central Administrator** users that include an e-mail address as part of their user credentials.

Element	Description
List	Lists the backup entries by **Destination Server** and provides information about each entry. **Backup Type**: what data will be saved in backup files: • **Full**: all server data (configuration and repository) will be saved in every backup file. • **Synchronized**: only changes to server data (configuration and repository) will be saved after the initial backup file. • **Configuration**: only server configuration data will be saved in every backup file. **Schedule Enabled**: whether or not backup scheduling is enabled. **Scheduled Days/Time**: when automatic backups will occur. **Current Status**: Whether or not a backup is in progress.
Backup Details	Provides information about the backup entry selected in the list.
Backup Progress	Provides information about ongoing backup activity.
Add Backup	Click to add a backup entry to the list.
Edit Backup	Click to edit the backup entry selected in the list.
Remove Backup	Click to remove the backup entry selected in the list.
Start Backup	Click to manually start a backup using the entry selected in the list.
Stop Backup	Click to stop a manually-started backup. **Note:** An backup-cancelled e-mail will be sent to the **InfraStruXure Central Administrators** that include an e-mail address as part of their user credentials.
Restore from Backup	Click to use the "Restore from Backup" wizard to select a backup file to be used to restore the InfraStruXure Central server.

Managing the backup entries

At least one backup entry should be defined and used for creating scheduled backup files for the InfraStruXure Central server's configuration data, or it's configuration and repository data.

Note: To delete a backup entry, select it in the list and click **Remove Backup**.

1. Select **Server Administration Settings** in the **Settings** menu.
2. In the "Server Administration Settings" display, select **Server Backup/Restore**.
3. Select to edit or add a backup entry.
   - To edit a backup entry, select the listed entry and click **Edit Backup**.
   - To add a backup entry, click **Add Backup** and select **Windows Repository** or **NFS** in the "Choose Remote Mount Type" display.
4. In the appropriate settings display, do the following:
   a. Configure the **Windows Share** ("Windows Backup Share Settings" display) or **NFS Share** ("NFS Backup Share Settings" display) settings.
   b. Select whether you want to backup all server configuration and repository data for each backup (**Full**), just the changes to the server configuration and repository data for each backup (**Synchronized**), or just the configuration data (**Configuration**).
   c. Click **Test Mount**.

      Note: An error message will occur if the share settings are defined incorrectly.
   d. Click **Next** to edit the schedule used to automatically backup the server data, or **Finish**.

      Note: The default schedule settings will cause a backup to occur every Friday at 1:00 AM.
5. In the "Backup Schedule" display, select the days on which a backup will occur, and the time it will occur on those days.

"Choose Remote Mount Type" display

Use this display to select **Windows Share** or **NFS** as the remote mount type for the saved backup file.

"Windows Backup Share Settings" display

Use this display to add or edit the settings for a Windows share used to backup the InfraStruXure Central server's configuration data, or its configuration and repository data.

Element	Description
Server Hostname or IP	Identity the hostname or IP address of the Windows share server.
Username	Identify the username required to access the server.
Password	Identify the password required to access the server.
Verify Password	Retype the password.
Domain	Identify the domain to which the Windows share is connected.
Share	Identify he name of the Windows share.
Subdirectory	Identify the subdirectory in the Windows share that will be used to store data.

	Note: If no subdirectory is specified, data will be stored in the share's root directory.
Backup Type	Select the type of backup that will be performed. **Full**: each backup file will contain all server configuration and repository data. **Synchronization**: the first backup file will contain all server configuration and repository data, while subsequent files will contain only new or changed data. **Configuration**: each backup file will contain all server configuration data, but no repository data.
Test Mount	Click to test the Windows share settings.

"NFS Backup Share Settings" display

Use this display to add or edit the settings for a NFS share used to backup the InfraStruXure Central server's configuration data, or its configuration and repository data.

Element	Description
Server Hostname or IP	Identity the hostname or IP address of the NFS share server.
Share	Identify he name of the NFS share.
Subdirectory	Identify the subdirectory in the NFS share that will be used to store data. **Note:** If no subdirectory is specified, data will be stored in the share's root directory.
Backup Type	Select the type of backup that will be performed. **Full**: each backup file will contain all server configuration and repository data. **Synchronization**: the first backup file will contain all server configuration and repository data, while subsequent files will contain only new or changed data. **Configuration**: each backup file will contain all server configuration data, but no repository data.
Test Mount	Click to test the NFS share settings.

"Backup Schedule" display

Use this display to schedule when the InfraStruXure Central server's configuration data, or its configuration and repository data, will be backed up automatically.

Element	Description

Schedule Enabled	Select to have the InfraStruXure Central server data backed up automatically as defined by the Days and Time settings.
Days	Select the day, or days, the backups will occur.
Time	Select the time of day the backups will occur.

Using the "Restore from Backup" wizard

Use this wizard to select the backup file, whether at an existing or new location, you want to use to restore the InfraStruXure Central server configuration, or configuration and repository, data.

1. Select **Server Administration Settings** in the **Settings** menu.
2. In the "Server Administration Settings" display, select **Server Backup/Restore**.
3. Click **Restore from Backup**, and use the "Choose Backup Location Type" display to select whether you want to navigate to a backup file at an existing or new location.

Navigating to a backup file at an existing location

You can use the "Restore from Backup" wizard to select a backup file at the NFS or Windows share at which the InfraStruXure Central server saved that file.

1. In the "Choose Backup Location Type" display, select **Existing Backup Location**.
2. In the "Existing Backup Location" display, select the listed location.
3. In the "Restore from Backup" display, select the listed backup file, and click **Finish**.
4. Click **OK** when asked if you want to use the data from a previous date to restore your server.

   Note: The server will restart as a result of the restore process. You can log on after the server finishes rebooting, which can take a few minutes.

Navigating to a backup file at a new location

You can use the "Restore from Backup" wizard to select a backup file at the NFS or Windows share at which the InfraStruXure Central server did not save that file.

1. In the "Choose Backup Location Type" display, select **New Backup Location** and either **Windows Share** or **NFS**.
2. In the appropriate display, identify the **Windows Share** ("New Windows Backup Location" display) or **NFS Share** ("New NFS Backup Location" display) location of the backup file.
3. In the "Restore from Backup" display, select the listed backup file, and click **Finish**.
4. Click **OK** when asked if you want to use the data from a previous date to restore your server.

   Note: The server will restart as a result of the restore process. You can log on after the server finishes rebooting, which can take a few minutes.

"Restore from Backup" wizard

Use this wizard to restore your InfraStruXure Central server using a backup file at an existing or new share location.

"Choose Backup Location Type" display

Use this display to choose the location of the backup file you want to use to restore the InfraStruXure Central server's configuration data, or its configuration and repository data.

Option	Description
Existing Backup Location	Select to locate a backup file at a location that has been used to save your InfraStruXure Central server data.
New Backup Location	Select to locate a backup file from an archived location, a location where the current backup files are not being saved.

"Existing Backup Location" display

Use this display to select the location of the backup file from the list.

"Restore from Backup" display

Use this display to select the listed backup file you want to use to restore the InfraStruXure Central server.

Note: The **Backup Source** column identifies which server was the source of the backup file.

"New Windows Backup Location" display

Use this display to identify the Windows share location for the backup file you want to use to restore your InfraStruXure Central server.

Element	Description
Server Hostname or IP	Identity the hostname or IP address of the Windows share server.
Username	Identify the username required to access the server.
Password	Identify the password required to access the server.
Verify Password	Retype the password.
Domain	Identify the domain to which the server is connected.
Share	Identify the name of the Windows share that contains the backup file.
Subdirectory	Identify the subdirectory in the Windows share that contains the backup file. **Note:** If no subdirectory is specified, the backup file is stored in the share's root directory.

"New NFS Backup Location" display

Use this display to identify the NFS share location for the backup file you want to use to restore your InfraStruXure Central server.

Element	Description
Server Hostname or IP	Identity the hostname or IP address of the NFS share server.
Share	Identify he name of the NFS share.
Subdirectory	Identify the subdirectory in the NFS share that will be used to store data. **Note:** If no subdirectory is specified, data will be stored in the share's root directory.

Server Proxy Settings option

Use this option's elements to define the settings the InfraStruXure Central server must use to communicate through a proxy server.

Note: An InfraStruXure Central server needs to use the internet to communicate with APC to download firmware updates, for example, or for Remote Monitoring Service (RMS) support.

Element	Description
Use Proxy	Select to enable the proxy settings.
Proxy Host	Identify the hostname or IP address of the proxy server.
Port	Identify the port at the proxy server that the InfraStruXure Manager server will use to communicate with that server.
Username	Identify the username to be used to access the proxy server.
Password	Identify the password to be used to access the proxy server.
Test Proxy	Click to to make sure the InfraStruXure Central server can access the identified proxy server using the proxy settings you define.
Do not use proxy for the hosts below	Lists the internet hosts you want the InfraStruXure Central server to be able to communicate with directly, without using the proxy server.
Add	Click to add the IP address of a host to the list.
Remove	Click to remove a selected host from the list.

Storage Settings option

Use this option's elements to identify the **Repositories** the InfraStruXure Central server can use, to define the **Purge Settings** for the data stored in the repositories, and when the server connects to an Enterprise Server, to review the **Disk Array Status** for that server.

Note: If your organization uses multiple InfraStruXure Central servers, and Windows or NFS repository servers for remote storage, each InfraStruXure Central server should use its repository server: multiple InfraStruXure Central servers should not store data on the same remote repository.

Repositories tab

Use this tab to manage the repositories the InfraStruXure Central server can use, and review information about a selected repository.

Element	Description
List	Lists the local and remote repositories, and identifies each repository's **Status**, **Type**, **Maximum Capacity**, and **Conditions**.
Details	Identifies the **Type**, **Maximum Capacity**, and **Conditions** for the selected repository.
Usage	Provides information about the current usage for the selected repository, as well as detail about the **Type** of data that can be stored, as well as the alloted capacity (**Size**) and current usage (**Percentage**) for each **Type**.
Status Message	Provides status information when something occurred at the server for the selected repository, such as the server went offline, or the an authentication (**Username** or **Password**) value changed for a Windows repository. **Note:** This **Status Message** appears only when status at the selected repository's server has changed. If the problem persists, contact the Administrator for the affected repository server.
Use Remote Storage Only	Select to have the InfraStruXure Central server limited to using a remote repository, only (disabled when no remote repository is available). **Note:** If the remote is offline, the server will store data in the local repository until the remote becomes available.
Migrate to Remote	Click to migrate the server configuration and repository data currently stored in the local repository to the remote storage repositories. **Note:** Disabled when no remote repository is available.
Add Repository	Click to add a remote repository.
Edit Repository	Click to edit a selected remote repository.
Remove Repository	Click to remove a selected remote repository from the list.

Managing the remote repositories

At least one remote repository should be defined and used by the InfraStruXure Central server, rather than the local repository.

Note: If your organization uses multiple InfraStruXure Central servers, and Windows or NFS repository servers for remote storage, each InfraStruXure Central server should use its repository server: multiple InfraStruXure Central servers should not store data on the same remote repository.

You can add, edit, or delete any remote repository, but not the local repository.

Note: To delete a repository, select it in the **Repositories** tab, and click **Delete Repository**.

1. Select **Server Administration Settings** in the **Settings** menu.
2. In the "Server Administration Settings" display, select **Storage Settings**.
3. In the **Repositories** tab, select to edit or add a repository.
   - To edit a repository, select the listed repository and click **Edit Repository**.
   - To add a repository, click **Add Repository** and select **Windows Repository** or **NFS Repository** in the "Choose Repository Type" display.
4. In the appropriate settings display, do the following:
   a. Configure the **Windows Share** ("Windows Repository Settings" display) or **NFS Share** ("NFS Repository Settings" display) settings.
   b. Click **Test Repository Settings**.

      Note: An error message identifies why the test failed, if the share settings are defined incorrectly.
   c. Configure the **File System** settings, and click **Finish**.
5. Use the **Purge Settings** tab to define when data will be purged from all online repositories that are not in an error or read-only state.

"Choose Repository Type" display:

Use this display to select whether you want to add a **Windows Repository** or **NFS Repository**.

"Windows Repository Settings" display:

Use this display to add or edit the settings for a Windows repository.

This display has two sections and a **Test Repository Settings** button. This button must be used to test the **Windows Share** settings when adding a repository, or when changing more than the **Repository Name** during an edit of a repository.

You will be unable to add or edit the **File System** settings until the test is successful.

Note: The InfraStruXure Central server will generate an error message that identifies why a test failed. If the problem persists, contact the Administrator for the repository server you are trying to use.

Windows Share section:

Configure the settings that identify where the Windows repository will reside, and the username and password needed to access the repository.

Element	Description
Repository Name	Identify a name for the repository.
Server Hostname or IP	Identity the hostname or IP address of the Windows share server.

Username	Identify the username required to access the Windows share.
Password	Identify the password required to access the Windows share.
Verify Password	Retype the password.
Domain	Identify the domain to which the Windows share is connected.
Share	Identify he name of the Windows share.
Subdirectory	Identify the subdirectory in the Windows share that will be used to store data. **Note:** If no subdirectory is specified, data will be stored in the root directory of the share.

File System section:

Select whether the repository's file system is enabled, and, when enabled, whether it is read-only, and its maximum capacity.

Element	Description
Enabled	Select to enable the repository.
Read-only	Select if you want to allow only read access to the repository.
Free Space	Identifies how much free space is available for the repository.
Maximum Capacity	Identify the maximum capacity of the repository, based on the available **Free Space**. For example, if there is 79.85 gigabytes (GB) available, type in a number that is equal to, or less than **79.85**, and select **GB** from the drop-down menu.

"NFS Repository Settings" display:

Use this display to add or edit the settings for an NFS repository.

This display has two sections and a **Test Repository Settings** button. This button must be used to test the **NFS Share** settings when adding a repository, or when changing more than the **Repository Name** during an edit of a repository.

You will be unable to add or edit the **File System** settings until the test is successful.

Note: The InfraStruXure Central server will generate an error message that identifies why a test failed. If the problem persists, contact the Administrator for the repository server you are trying to use.

NFS Share section:

Configure the settings that identify where the NFS repository will reside.

Element	Description
Repository Name	Identify a name for the repository.
Server Hostname or IP	Identity the hostname or IP address of the NFS share server.
Share	Identify he name of the NFS share.
Subdirectory	Identify the subdirectory in the NFS share that will be used to store data. **Note:** If no subdirectory is specified, data will be stored in the root directory of the share.

File System section:

Select whether the repository's file system is enabled, and, when enabled, whether it is read-only, and its maximum capacity.

Element	Description
Enabled	Select to enable the repository.
Read-only	Select if you want to allow only read access to the repository.
Free Space	Identifies how much free space is available for the repository.
Maximum Capacity	Identify the maximum capacity of the repository, based on the available **Free Space**. For example, if there is 79.85 gigabytes (GB) available, type in a number that is equal to, or less than **79.85**, and select **GB** from the drop-down menu.

Purge Settings tab

Use this tab to define settings that affect automatic purges, or to manually purge the repositories.

Note: You can chose to include the repository data in the backup files created using **Server Backup/ Restore**, a **Server Administration Settings** option in the **Settings** menu.
The **Total Repository Usage** section identifies alloted capacity (**Size**) and current usage (**Percentage**) for each **Type** of data stored in all repositories, unless **Use Remote Storage Only** is selected in the **Repositories** tab. In that case, identifies capacity and usage for all remote repositories, only.

Note: If an error condition occurs at a repository, an e-mail is sent to the **InfraStruXure Central Administrators** that include an e-mail address as part of their user credentials.

Automatic Purge Settings

Use this section to define the settings for the conditions that will cause an automatic purge of the repositories.

Type	Description
Begin Purge	Identify the percentage of total capacity that will initiate a purge.
End Purge	Identify the percentage of total capacity that will cause the purge to end.
Warn of Purge	Identify the percentage of total capacity that will result in a warning that a purge may occur soon.
Send Warning E-mails	Select to send e-mails to the **InfraStruXure Central Administrators** that include an e-mail address as part of their user credentials, when the **Warn of Purge** threshold is reached.
Apply Purge Settings	Click to save changes to the settings.

Manual Purge

Use this section to perform a manual purge of the repositories.

Type	Description
Purge Data on or Before	Select the date for which all data stored on or before that date will be purged.
Choose the Types of Data to Manually Purge	Select to include **Alert Binary Data**, **Sensor Data**, **Untagged** or **All Surveillance Data**, or a combination of these choices, in the manual purge. **Note:** You can prevent tagged surveillance data from being purged by selecting **Untagged Surveillance Data** instead of **All Surveillance Data**.
Run Manual Purge	Click to purge the selected data for the defined range of dates.

Disk Array Status tab

Use this tab to view **Overall Status** and **Individual Disk Status** information for the disk array associated with an Enterprise Server.

Note: If a disk array status changes to degraded, an e-mail is sent to the **InfraStruXure Central Administrators** that include an e-mail address as part of their user credentials.

Time Settings option

Use this option's elements to define the date and time for the InfraStruXure Central server, or the identification of any NTP servers that will provide those date and time values, and regional settings.

Note: The InfraStruXure Central server must reboot before a change to any setting can take effect.

Date and Time elements

Element	Description
Enable NTP Server	When selected, a Network Time Protocol (NTP) server provides the date and time values for the InfraStruXure Central server; otherwise, these values are defined by the other **Date** and **Time** elements.
NTP Server 1 - 3	Identify the IP address or hostname of at least one NTP server, when **Enable NTP Server** is selected.
Use Client Settings	Click to use your client time and date settings at the server, when **Enable NTP Server** is not selected.
Date	Define the date the server will use, when **Enable NTP Server** is not selected.
Time	Define the time the server will use, when **Enable NTP Server** is not selected.
Calendar	Displays the current date, and can be used to define that date, when **Enable NTP Server** is not selected.

Regional Settings elements

Element	Description
Server Locale	Select the locale at which the InfraStruXure Central server is physically located. **Note:** The server's measurements (metric or US standard) and date formats will be matched to the formats commonly used at the selected locale.
Use 24-hour clock	Select to have the InfraStruXure Central server use a 24-hour clock.
Server Time Zone	Select the time zone in which the InfraStruXure Central server is located.

Graphing and reporting feature

You can create graph-format and table-format reports for the device sensors for the monitored SNMP devices, and for the device sensors at all the devices that connect to the monitored NetBotz Appliances.

The following views have a **Custom Device Report** option in a right-click **Graphing and Reporting** menu, and a **Custom Device Report** icon, either of which can be used to initiate a device sensor report:

- **Device Groups** view: click the **Custom Device Report** option or icon to access the "Custom Device Report" wizard with all device sensors listed for all devices assigned to the selected device group.
  Note: The right-click **Graphing and Reporting** menu in this view also has options for various sensor types. Selecting one of these options accesses information for up to 50 sensors of the selected type, for the selected device group, in a **Graph View**.
- **Device View** and **Map View**: click the **Custom Device Report** option or icon to access the "Custom Device Report" wizard with all device sensors listed for the device or set of devices selected in the view.
- **Active Alarms** view and **Alarm History** view: click the **Custom Device Report** option or icon to access the "Custom Device Report" wizard with the device sensors for the device or set of devices (**Active Alarms** view only) associated with the alarms selected in the view.
  Note: All device sensors associated with a selected alarm's device will be listed, with the sensor for that alarm selected in that list.

Once you create a report, you can export a report as a.txt or.csv file (table), or as a.bmp,.jpg, or.png file (graph), without saving the report. You can also save your report's criteria to create a report you can reuse in the future, as well as schedule running and exporting the report on a periodic basis.

"Custom Device Report" wizard

Use this wizard to create graph-format and table-format reports for the sensors selected when you click the **Custom Device Report** option in the right-click **Graphing and Reporting** menu, or the **Custom Device Report** icon in a view.

In addition, you can use this wizard to save the report in the **Saved Reports** view, and to schedule the periodic export of the saved report.

"Specify Device Sensors" display

Use this display to create a graph-format or table-format report for the device or device sensors you select in the **Select Sensors** section.

What sensors are listed in this section depends on the the view used to access the "Custom Device Report" wizard:

- **Device Groups** view: lists all sensors for all devices in the selected device group.
- **Device View** or **Map view**: lists all sensors for a selected device or set of devices.

- **Active Alarms** view: lists all sensors for a device associated with the selected alarm, or for the devices associated with a set of alarms.
- **Alarm History** view: lists all sensors for the device associated with the selected alarm.

Note: In addition to the elements described in the following table, this display has the same **Chose Date**, **Select Sensors**, and **Highlight Alerting Sensor** elements as the "Edit Graph" and "Edit Report Criteria" displays.

Element	Description
Run Graph	Click to view a graph-format report for up to a maximum of 50 device sensors, before you save the report. **Note:** The more sensors you include in a graph-format report, the more obscured the sensor data will be in that graph. This button is disabled when more than 50 sensors are selected.
Run Report	Click to view the table-format report for the selected device sensors, before you save the report. **Note:** This button is disabled when more than 1024 sensors are selected.
Next	Click to use the "Specify Device Report Name and Scheduling" display to name and save the report in the **Saved Reports** view, as well as to schedule the periodic export of the report, if desired.

"Specify Device Report Name and Scheduling" display

Use this display to save the report in the **Saved Reports** view by defining a name for the report, and, if desired, defining how and when the report will be periodically exported.

Note: The following elements are shared by two other displays: the "Edit Device Sensor Report" display accessed from the **Saved Reports** view, and the "Save Report Criteria" display accessed from the view for any saved or unsaved report.

Element	Description
Report Name	Define the name that will identify the report in the **Saved Reports** view.
Save Report Criteria	**Enable Export**: Select to enable the report to be exported on a scheduled basis. **Export Name**: Select the name of an existing export configuration. **Add Export**: Click to use the "Add Export" wizard to add a new export configuration. **Delimiter**: Select how the report data will be delimited for export: **Comma**, **Semicolon**, **Space**, or **Tab**. **Note:** Reports are exported on a scheduled basis as text only.
Scheduling	**Days**: Select the day or days of the week for the exports.

	Time: Select the time of day for the exports.

Graph View

This view provides data, in the form of a graph and device sensor list, for up to 50 sensors associated with a right-click **Graphing and Reporting** sensor option selected in the **Device Groups** view. For example, If you select **Air Flow**, the **Graph View** will provide information for up to 50 sensors that measure air flow for the devices in the selected device group.

Note: For information about the available sensor options, see Alert Thresholds under Alert Settings (Settings menu).

The **Graph View** is identical to the graph-format reports that are generated using **Custom Device Report**, a right-click **Graphing and Reporting** option available in several different views, with two major differences:

- A graph-format report can provide information about many different types of sensors; a **Graph View** only provides information about one type of sensor at a time.
- A graph-format report can be saved and exported on a periodic basis; a Graph View cannot be saved, or exported on a periodic basis.

Each **Graph View** identifies the selected sensor and device group, and the time frame, at the top of the view. You can use the device sensor list columns and button icons to do the following:

- Click a column title to sort the list in ascending or descending order based on that column's information.
- Edit the date range, or change the view to display more (maximum of 50) or less of the available sensors, using the "Edit Graph" display (**Edit Graph** icon).
  Note: The "Edit Graph" display is identical to the "Edit Report Criteria" display used to edit the date range or selected sensors for graph-format or table-format reports; only the name is different.
- Save a copy of the graph as a *.bmp (the default selection), *.jpg, or *.png file (**Save Copy of Graph** icon).
- Select to display information about a different type of sensor (**Change Graph Type** icon drop-down menu options).
  Note: You also can select to display information about a different type of sensor by selecting a different **Graphing and Reporting** sensor option in the **Device Groups** view, or select a different device group, to view information about the currently selected sensor for the devices in that group.

Graph section

Provides a graphic representation of the values reported by the device sensors included in a Graph View or graph-format report, over the period of time selected for the view or report.

- Every device sensor is represented by its own color, as identified in the device sensor list.
- The time frame is identified below the title, and labeled along the bottom of the graph.
- For a **Graph View**, the sensor's value range is labeled along the left-side of the graph.
- For graph-format reports, which can cover multiple types of sensors, one sensor value range is labeled along the left-side of the graph, while any other value ranges for the report's sensors are labeled to the right of the graph.

Sensor list section

Lists and provides information about each device sensor included in a **Graph View** or graph-format report, including the color used to represent each sensor's values in the graph.

Column	Description
Color	The color used for the sensor's values in the graph. **Note:** You can deselect the color to remove a sensor's values from the graph, or select (the default), to include the sensor's values.
Parent Device	**InfraStruXure Central** for SNMP devices, or a NetBotz Appliance model (**WallBotz 500**, for example), for devices monitored by a NetBotz Appliance.
Monitored Device	The device label.
Sensor	The sensor name.
Units	The unit of measurement for numeric sensors, only.
Low	The low value measured by numeric sensors only, during the report's time span.
High	The high value measured by numeric sensors only, during the covered time span.
Average	The average value measured by numeric sensors only, during the covered time span.

Report views

A **Saved Reports** view is available, as well as views for each report format.

Saved Reports view

This view allows you to view, edit, or delete saved reports.

Note: Reports are saved using the "Specify Device Report Name and Scheduling" display in the "Custom Device Report" wizard, or by using the **Save Report Criteria** icon in the view for a table-format or graph-format report that was run in the "Select Report Criteria" display before it was saved. Each saved report is listed by name, and includes information about whether periodic export of the report has been **Scheduled** (**Yes** or **No**), and when scheduled, the **Scheduled Days** and **Scheduled Time**. You can use the table columns, right-click options, and button icons at the top of the view, to perform the following functions:

- Click a column title to sort the list in ascending or descending order based on that column's information.
- Delete a selected report (**Delete** option or icon).
- View a graph-format version of a selected report (**View the Report as a Graph** option or icon).
- View a table-format version of a selected report (**View the Report as a Table** option or icon).

- Edit the date range or sensors for a selected report using the "Edit Report Criteria" display (**Edit Report Criteria** option or icon).
  Note: The "Edit Report Criteria" display is identical to the "Edit Graph" display used to edit the date range or selected sensors for a **Graph View**: only the name is different.
- Edit the name or export properties for a selected report using the "Edit Report Scheduling and Exporting" display (**Edit Report Scheduling and Exporting** option or icon)
- Manage the export configurations that can be used for scheduled report exports using the "Scheduled Export Configuration" display (**Scheduled Export Configuration** icon).
  Note: You also can use **Scheduled Export Configuration**, a **Graphing and Reporting** option in the **Settings** menu, to perform this function.

Graph-format reports

This report format provides data, in the form of a graph and device sensor list, for up to 50 device sensors.

Note: You can access a graph-format report view by clicking **Run Graph** in the "Custom Device Report" wizard's "Select Device Sensor" display, or by selecting a report in the **Saved Reports** view and electing to view it as a graph.

The name (***Device Sensor Report (Graph)**, for an unsaved report) and time frame is identified at the top of each report. You can use the device sensor list columns and button icons, to do the following:

- Click a column title to sort the list in ascending or descending order based on that column's information.
- Edit the date range or sensors for a selected report using the "Edit Report Criteria" display (**Edit Report Criteria** icon).
  Note: The "Edit Report Criteria" display is identical to the "Edit Graph" display used to edit the date range or selected sensors for a **Graph View**: only the name is different.
- Edit the report name or export properties using the "Save Report Criteria" display (**Save Report Criteria** icon).
- Save a copy of the report as a *.bmp (the default selection), *.jpg, or *.png file (**Save Copy of Graph** icon).

Table-format reports

This report format provides sensor data, in the form of table that lists all device sensors that were included in the report.

Note: You can access a table-format report view by clicking **Run Report** in the "Custom Device Report" wizard's "Select Device Sensor" display, or by selecting a report in the **Saved Reports** view and electing to view it as a table.

The name (***Device Sensor Report (Table)**, for an unsaved report) and time frame is identified at the top of each report. You can use the search feature, table columns, and button icons, to do the following:

- Type text in the **Search** field to locate a specific device or sensor in the report, or to narrow the list to a particular set of device sensor entries.
- Click a column title to sort the list in ascending or descending order based on that column's information.
- Edit the date range or sensors for a selected report using the "Edit Report Criteria" display (**Edit Report Criteria** icon).

Note: The "Edit Report Criteria" display is identical to the "Edit Graph" display used to edit the date range or selected sensors for a **Graph View**: only the name is different.

- Edit the report name or export properties using the "Save Report Criteria" display (**Save Report Criteria** icon).
- Save a copy of the report as a *.csv (the default selection) or *.txt file (**Save Report Data** icon).
- Browse through a multiple-page report (**Go to** arrow icons, and a box that identifies the page number).

Column	Description
Device	The device label.
Parent Device	**<hostname> (InfraStruXure Central**} for SNMP devices, or the IP address or hostname of a NetBotz Appliance for devices monitored by that appliance.
Sensor	The sensor name.
Time	The date and time at which a change in the sensor value was sensed.
Value	The value measured at the identified date and time.
Unit	The unit of measurement for numeric sensors, only.
Status	The sensor status, when an active alarm exists: **Warning**, **Error**, **Critical**, or **Failure**.

Button icons (report views)

The report views have icons you can use to perform various functions.

Saved Reports icons

Icon	Description
📈	Use this **View the Report as a Graph** icon to view a selected report as a graph.
▤	Use this **View the Report as a Table** icon to view a selected report as a table.
📊	Use this **Edit Report Criteria** icon to edit the time frame or sensors you want a selected report to cover.
💾	Use this **Edit Report Scheduling and Exporting** icon to edit the name or export and schedule properties for a selected report.
✖	Use this **Delete** icon to delete a selected report.

Icon	Description
⬅	Use this **Scheduled Export Configuration** icon to manage a list of the export configurations that can be used for scheduled exports for reports.

Graph-format and table-format report icons

These report views share three icons; the table report view also has **Go to** arrow icons you can use to browse through a multiple-page report, with a box that identifies the page being viewed.

Icon	Description
💾	Use this **Save Report Criteria** icon to edit the name or export and schedule properties for a selected report.
⬅	Use this **Save Copy of Graph** icon for a graph-format report to save a copy of the report as a *.bmp, *.jpg, or *.png file. Use this **Save Report Data** icon for a table-format report to save a copy of the report as a *.txt or *.csv file.
📊	Use this **Edit Report Criteria** icon to edit the time frame or sensors you want a selected report to cover.

"Edit Report Scheduling and Exporting" display

Use this display to edit the name and export and scheduling properties for a report selected in the **Saved Reports** view.

Note: This display uses the same elements as described for the "Custom Device Report" wizard's "Specify Device Report Name and Scheduling" display.

"Save Report Criteria" display

Use this display to save a previously unsaved report in the **Saved Reports** view by defining a name for the report, and, if desired, defining how and when the report will be periodically exported.

Note: This display uses the same elements as described for the "Custom Device Report" wizard's "Specify Device Report Name and Scheduling" display.

"Edit Graph" or "Edit Report Criteria" display

Use this display to edit the time frame or device sensors selected for a **Graph View** ("Edit Graph" display), or for a graph-format or table-format report ("Edit Report Criteria" display).

Note: This display's elements also are used in the "Custom Device Report" wizard's "Specify Device Sensors" display.

Element	Description
Chose Date	**Relative**: select to use a drop-down menu option that identifies a period of time you want the report to cover. **Range**: select to use to define the Start and End dates for the period of time you want the report to cover.
Select Sensors	**Search** and **Clear**: use to search for a specific sensor, or to narrow the list to include only those sensors that include your typed text. **Sensors list**: select the device sensors you want a report to include. The list includes all sensors for the devices that were selected when **Custom Device Report** was clicked, with the following information provided for each sensor: • **Device**: device label • **Sensor**: sensor type • **Alarm State**: current sensor status • **Location**: device location, if known • **Device Status**: current device status • **Hostname**: device hostname or IP address **Select/Deselect All**: use to select to include all sensors in the report, or to deselect the currently selected sensors. **Note:** If more than 50 sensors are selected, you cannot create a graph-format report.
Highlight Alerting Sensors	Select to highlight the **Value** for sensors that have active alarm conditions in table-format reports. These sensors will be highlighted in red.

Scheduled Export Configuration option and icon

Use this **Custom Device Report** option in the **Settings** menu, or the **Scheduled Export Configuration** icon in the **Saved Reports** view, to manage a list of export configurations that can be used for the scheduled export of reports.

The "Scheduled Export Configuration" display this option and icon access has the following elements.

Element	Description
List	Lists the available export configurations, and provides the following information about each: **Export Name**: the name defined for the export configuration.

	Export Type: the type of export used (E-mail, FTP, etc.). **Server Hostname**: the hostname or IP address of the server used, if any. **Username**: the username used to access the server, if any.
Add Export	Click to use the "Add Export" wizard to add an export configuration.
Edit Export	Click to use the "Edit Export" display to edit a selected export configuration's settings.
Remove Export	Click to delete a selected export configuration.

Managing the export configurations

You can add new export configurations, or edit existing configurations, using the "Scheduled Export Configuration" display.

Note: To remove an export configuration, select it in the list and click **Remove Export**.

Adding a new export configuration

1. Select **Scheduled Export Configuration**, the **Custom Device Report** option in the **Settings** menu, or click the **Scheduled Export Configuration** icon in the **Saved Reports** view.
2. In the "Scheduled Export Configuration" display, click **Add Export** to access the "Add Export" wizard.
3. In the "Choose Export Type" display, select the type of export configuration you want to add.
4. In the settings display for the selected export type, define the settings.

   Note: Each export type uses the its own settings display to add or edit an export configuration.
5. Click **Test Export** to test the export settings.

   Note: You need to verify the test was successful. For example, for e-mail settings, verify an e-mail was received.

Editing an export configuration

1. Select **Scheduled Export Configuration**, the **Custom Device Report** option in the **Settings** menu, or click the **Scheduled Export Configuration** icon in the **Saved Reports** view.
2. In the "Scheduled Export Configuration" display, select a listed export configuration, and click **Edit Export**.
3. In the settings display for the selected export configuration, define the settings.

   Note: Each export type uses the its own settings display to add or edit an export configuration.
4. Click **Test Export** to test the edited export settings.

   Note: You need to verify the test was successful. For example, for e-mail settings, verify the e-mail was received.

"Add Export" wizard

Use this wizard to select the type of export configuration you want to add, and to define the settings for that configuration.

Note: When you click **Edit Export** in the "Scheduled Export Configuration" display, you access the 'Edit Export" display, the same display, except in name, that was used to add the export configuration.

"Select Export Type" display

Use this display to select the type of export you want to add.

Option	Description
FTP Export	Click to add FTP settings.
E-mail Export	Click to add e-mail settings.
HTTP Export	Click to add HTTP settings.
Windows Export	Click to add Windows settings.
NFS Export	Click to add NFS settings.

"FTP Export Settings" display

Use this display to add or edit an export configuration that exports a report's data to a specified FTP server.

Element	Description
Export Name	Define the name for the FTP export settings.
Server Hostname or IP	Identify the hostname or IP address of the FTP server at which reports can be saved.
Port	The port the server uses for FTP communication (**21**, by default).
Use Passive Transfer	Select to use passive FTP transfers when communicating with the FTP server. **Note:** Passive FTP transfers can be useful if your InfraStruXure Central server is communicating across a firewall.
Username	Identify the name used to access the FTP server.
Password	Identify the password used to access the FTP server.
Verify Password	Retype the password.
Target Directory	Identify the path to be used for storing reports at the defined server. This path should always be relative to the default directory associated with the username that accessed the server. **Note:** If the directories you define for the path do not exist, they will be created automatically.
Test Export	Click to test the export settings. **Note:** Verify the test data actually was saved at the target directory on the FTP server.

"E-mail Export Settings" display

Use this display to add or edit an export configuration that exports a report's data to specified e-mail addresses.

Note: The SMTP server the InfraStruXure Central server uses to send e-mail saved report data is defined by the **E-Mail Settings** option in the "Server Administration Settings" display.

Type	Description
Export Name	Define the name for the e-mail export settings.
Subject of Message	Define the subject of the e-mail message that will be generated and sent.
Body of Message	Define the body of the e-mail message that will be generated and sent.
E-mail Addresses	Lists the e-mail addresses to which reports will be sent.
Add	Click to add an e-mail address to the list.
Remove	Click to remove a selected e-mail address from the list.
Test Export	Click to test the export settings. **Note:** Verify an e-mail message actually was received.

"HTTP Export Settings" display

Use this display to add or edit an export configuration that exports a report's data to a specified HTTP address using an HTTP Post.

Element	Description
Export Name	Define the name for the HTTP export settings.
Target URL	Identify the full URL to where reports will be posted at the target server.
Username	Identify the name needed to post HTTP data to the server at the specified **Target URL**.
Password	Identify the password needed to to post HTTP data to the server at the specified **Target URL**.
Verify Password	Retype the password.
SSL Options	Select **No verification**, **Verify certificate**, or **Verify certificate and hostname**.
Test Export	Click to test the export settings. **Note:** Verify the test data actually was posted and saved at the target server.

"Windows Export Settings" display

Use this display to add or edit an export configuration that exports a report's data to a specified Windows share server.

Element	Description
Export Name	Define the name for the Windows export settings.
Server Hostname or IP	Identify the hostname or IP address of the Windows share server.
Username	Identify the name needed to connect to the share at the Windows server.
Password	Identify the password needed to connect to the share at the Windows server.
Verify password	Retype the password.
Domain	Identify the domain to which the Windows share is connected.
Share	Identify the name of the shared folder at the Windows server.
Subdirectory	Identify the subdirectory to be used to store reports. **Note:** The subdirectory field is optional: if no subdirectory is specified, data will be stored in the **Share** root directory.
Test Export	Click to test the export settings. **Note:** Verify the test data actually was saved in the proper folder on the Windows server.

"NFS Export Settings" display

Use this display to add or edit an export configuration that exports a report's data to a specified UNIX server that uses the Network File Sharing (NFS) protocol.

Element	Description
Export Name	Define the name for the NFS export settings.
Server Hostname or IP	Identify the hostname or IP address of the UNIX server running NFS that you want to recieve the exported report data.
Share	Identify the name of the directory used for file sharing on the server.
Subdirectory	Identify the subdirectory to be used to store reports. **Note:** The subdirectory field is optional: if no subdirectory is specified, data will be stored in the **Share** root directory.
Test Export	Click to test the export settings. **Note:** Verify the test data actually was saved at the NFS server, in the correct **Share** and subdirectory (if used).

Surveillance feature

Surveillance is a license key-based upgrade designed for use with the InfraStruXure Central server. This feature enhances your ability to use the Camera Pods and CCTV Adapter Pods associated with monitored NetBotz Appliances for surveillance purposes.

Note: The help for this feature assumes a Surveillance license is registered with the InfraStruXure Central server, and the license has been enabled for each camera.

With the Surveillance feature and cameras licensed, you can do the following:

- View live feeds in the **Thumbnails** view for all cameras associated with the NetBotz Appliances in a group selected in the **Device Groups** view.
- View live feeds in a **Camera** view for a camera selected in the **Thumbnails** view.
- Retrieve, view, and export recorded clips.
- Configure the capturing and recording of clips.
- Stream audio to and from properly configured cameras.

Licensing Surveillance and cameras

A Surveillance license must be registered at the InfraStruXure Central server before you can use the Surveillance feature. In addition, each camera must be licensed before its Surveillance features can be used.

Note: If you do not have a valid Surveillance license, a **No Surveillance License Installed** message is displayed at the top of the **Thumbnails** view.
Each InfraStruXure Central server comes with a trial Surveillance license that allows you to evaluate the Surveillance features before purchasing a license. When that license expires, the following will occur:

- Previously recorded clips are preserved but can be viewed only when a surveillance license is registered.
- No new clips can be generated.
- No live camera feeds will be available.

Registering the Surveillance license

1. Select **License Keys**, a **Server Administration Settings** option in settings menu, or click **Add License Key** that appears next to the **No Surveillance License Installed** message at the top of the **Thumbnails** view.
2. Click **Add License Key**.
3. In the "Add License Key" display, type in your Surveillance license key, and click OK.

Enabling the license for the cameras

The license can be enabled and disabled (the default condition) for each camera.

Note: You can use this procedure to configure any of the the **Surveillance Settings** for one or more cameras.

1. Select **Surveillance Settings** in the **Settings** menu to enable multiple cameras at the same time, or select this same option in the right-click menu for a thumbnail, to enable that camera only.

   Note: If you selected **Surveillance Settings** in a thumbnail's right-click menu, go to step 4.
2. In the "Select Camera Type" display, select the type of camera to be licensed.
3. In the "Select Surveillance Devices" display, select the cameras to be licensed.
4. In the "Surveillance Settings" display, enable the License Camera option at the top of the display.

Surveillance perspective

This perspective provides ready access to the surveillance views, features, and configuration settings. It is accessed by clicking the **Surveillance** button located directly below the **Updates** menu.

Note: All surveillance functions can be performed from the **Monitoring** perspective, by adding the **Thumbnails** view to that perspective (select **Thumbnails**, the **Surveillance** option in the **Window** menu).
By default, two views appear in the Surveillance perspective. These views, along with **Surveillance Settings**, a **Settings** menu option, allow you to perform all InfraStruXure Central server surveillance functions.

- **Device Groups** view: used to select which group will have information about its associated NetBotz Appliance cameras displayed in the Thumbnails view.
- **Thumbnails** view: displays live-feed views for all cameras associated with the selected device group.
  Note: Each thumbnail can access a **Camera** view that displays a live-feed view for the selected thumbnail's camera only.

Device Groups view in the Surveillance perspective

This view in the **Surveillance** perspective operates a little different than it does in the **Monitoring** perspective.

- You can use it to manage the location of cameras only, by dragging their thumbnails from the **Thumbnails** view for one group into a different group in the **Device Groups** view.
  Note: You can hold the Ctrl key down to drag a copy of a camera from the **Thumbnails** view for one group into another group in the **Device Groups** view without removing the camera from the group displayed in the **Thumbnails** view.
- This view in the **Surveillance** perspective has two right-click menu options that are not available in the **Monitoring** perspective.
  Note: Two right-click menu options in the **Monitoring** perspective (**Map View Settings** and **Show Alarm History**), are not available in the **Surveillance** perspective.
  - **Surveillance Settings**: allows you to configure settings for the cameras in a selected device group.
    Note: **Surveillance Settings** in the **Settings** menu allows you to configure the settings for cameras in all device groups; **Surveillance Settings** in the **Thumbnails** view allows you to configure the settings for cameras selected in that view.
  - **Retrieve Clips**: accesses the "Recorded Camera Clips" display for all cameras in a selected device group.

Thumbnails view

This view shows all of the cameras assigned to a selected device group. Each thumbnail shows a low frame-rate, real-time feed from a camera. When a thumbnail receives a new frame, it is highlighted to show any activity that happened for that camera for that frame.

All surveillance features, including all configuration settings that affect surveillance, can be accessed from this view using its thumbnails, right-click options, and button icons.

Note: Which thumbnails are displayed depends on which group is selected in the **Device Groups** view. In addition, a unlicensed camera will have a grayed out image showing where the camera is pointing, with a prohibited symbol that indicates the camera will not function until it is licensed, and when the InfraStruXure Central server has lost communication with a camera, the thumbnail will be black with a grey x.

- Access the "Surveillance Settings" display to configure one or more cameras (select **Surveillance Settings** in a right-click menu for a selected camera's thumbnail).
  Note: **Surveillance Settings** in the **Settings** menu allows you to configure the settings cameras for all device groups; **Surveillance Settings** in the **Device Groups** view allows you to configure cameras for a selected device group.
- Access the "Camera Settings" display to configure the cameras at the monitored NetBotz Appliances (select **NetBotz Appliance Camera Settings** in a right-click menu for a selected camera's thumbnail).
- Access the "Recorded Camera Clips" display to retrieve, view, and tag clips for a selected camera (select **Retrieve Clips** in the thumbnail's right-click menu, or use the 🎞 icon).
- Double-click a thumbnail to access its **Camera** view (or select **Open Camera View** in the thumbnail's right-click menu).
- Use the **Menu** icon (▽) to define what information is included with the thumbnails.
- Sort the thumbnails by the type of information that can be provided with the thumbnails (use the ↓ icon to access the "Sort Surveillance Thumbnails" display}.
- Use the **Search** and **Clear** elements to filter the **Thumbnails** view to display only the thumbnails that include your typed text.
- Access the "Device Launch Settings" display to define the settings used to access the web interface at a selected camera's NetBotz Appliance (select **Device Launch Settings** in the thumbnail's right-click menu).
- Launch to the web interface at a selected camera's NetBotz Appliance (select **Launch to Device** in the thumbnail's right-click menu).
- View the Device View listing for a selected camera in the Monitoring perspective (select **View in Monitoring Perspective** in the the thumbnail's right-click menu).

Button icons (Thumbnails view)

In addition to standard minimize and maximize icons, three icons are available to perform specific **Thumbnails** view and surveillance functions.

Icon	Description
↓	Click this **Sort By** icon to access the "Sort Surveillance Thumbnails" display, which allows the user to choose the criteria for sorting the displayed thumbnails.
🎞	Click this **Retrieve Clips** icon to access the "Recorded Camera Clips" display for the selected cameras.

Icon	Description
▽	Click this **Menu** icon to select the camera-associated data to display under each thumbnail. • **Label** • **Address** • **Location** • **Status** • **Licensed** • **Model** • **Device Groups** • **Description**

"Sort Surveillance Thumbnails" display

Use this display to sort the thumbnails in the **Thumbnails** view. Based on the chosen sorting category, displayed thumbnails are sorted alphanumerically.

Select the radio button next to the criteria you want to use to sort the displayed thumbnails.

Category	Description
Label	Sort by **Label**.
Location	Sort by **Location**.
Status	Sort by **Status**.
Model	Sort by model number of the camera's NetBotz Appliance.
Description	Sort by user-entered description.
Address	Sort by IP address or hostname.
Last Motion	Sort by which cameras are detecting motion, and for how long. For example, three cameras (X, Y, and Z) are detecting motion, Camera X for five seconds, Y for four seconds, and Z for three seconds: Camera X is in the first position of the Thumbnails view, Y in the second, and Z in the third; if Camera X stops detecting motion, it moves to the last position, Y moves to the first position, and X moves to the second. **Note:** This option, which is the default option, is helpful if you want to focus your attention on cameras that are currently showing activity.
Licensed	Sort by license status.
Device Groups	Sort by the device groups to which the cameras are assigned. If a camera is assigned to multiple groups, the camera is sorted according to the first device group listed.

Camera view

Displays a real-time view of the camera feed along with information about the selected NetBotz Appliance.

The **Camera** view consists of two areas, the displayed real-time feed from the selected device, and a **Camera Information** area.

The **Camera Information** area contains **Label**, **Address**, **Location**, **Status**, **Licensed**, **Model**, **Device Groups**, and **Description** information for the camera.

The following icons are located on the upper right-hand side of the view:

Icon	Description
👂	Click this **Listen** icon to hear the accompanying audio stream for the selected device. **Note:** Disabled when no audio is available.
💬	Click this **Talk** icon to send audio to be played at the device. **Note:** This feature is only available on certain models and requires a microphone on the user's side, and a set of external speakers on the device side.
🖥	Click this **Resolution** icon to display a list of the available resolutions for the feed. The currently selected resolution is marked with a check mark. To select a new resolution, highlight the desired entry.

Two-Way Audio

When connected to a device capable of capturing and broadcasting sound, you can transmit sounds to and from the device through the InfraStruXure Central server.

You can use the **Camera** view controls to stream audio from camera pods that have microphones, and to use a microphone connected to your system to send audio to camera pods that have connected speakers.
Note: For two-way audio to work, the camera must be able to connect directly to the client on a public accessible network.

- To listen to streaming audio from the currently selected Camera Pod (if available) click the 👂 button.
  Note: More than one client can listen to the audio stream simultaneously.
- To transmit audio from your system to speakers that are connected to the selected Camera Pod, click the 💬 button while speaking into your system's microphone.
- 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.
- While the 💬 button is depressed it will lock the audio transmission so only your client can send audio to the selected camera pod.

NetBotz Appliance Camera Settings option

Use this right-click menu option in the **Thumbnails** view to access the "Camera Settings" wizard associated with **Camera Settings**, a **NetBotz Appliance** option in the **Settings** menu, and with **Camera Settings**, a right-click **NetBotz Appliance** menu option in the **Device Groups** view.

The "Camera Settings" wizard has two displays:

- "Select Camera" display: accessed by the **NetBotz Appliance Camera Settings** option when multiple cameras are selected in the **Thumbnails** view, this display is used to chose which camera you want to configure.
- "Camera Settings" display: accessed either from the "Select Camera" display, when multiple cameras have been selected, or directly, when a single camera is selected in the **Thumbnails** view. This display has three configuration options, two of which affect how cameras operate during surveillance activities:
  - **Alarm Data Capture**: settings that affect the capture of images for alarms only.
  - **Image Settings**: settings that affect the image quality, and other settings, used for alarm and surveillance activities.
  - **Masking**: specify user-specified masks used to ignore motion in areas of an image, and to prevent regions of the image from being seen, during alarm and surveillance activities.
    Note: The camera settings, which are set at the NetBotz Appliance associated with a selected camera, are independent from the surveillance feature: **Camera Settings**, the **NetBotz Appliance** option in the **Settings** menu and **Device Groups** view, is available with or without a surveillance license. For more information about these settings, see Camera Settings option under NetBotz Appliance Configurations (Settings menu).

Surveillance Settings options

Three options are available to access a "Surveillance Settings" display used to configure how the InfraStruXure Central server affects and responds to cameras at monitored NetBotz Appliances.

One option can be used to access the "Surveillance Settings" display directly for a single camera: select **Surveillance Settings** in a right-click menu for a selected camera's thumbnail when only that thumbnail is selected in the **Thumbnails** view.

All three options can access this display as part of the "Surveillance Settings" wizard:

- Select **Surveillance Settings** in the right-click menu for a selected camera's thumbnail, when multiple thumbnails are selected in the **Thumbnails** view, to configure those cameras.
- Select **Surveillance Settings** in a device group's right-click menu to configure cameras for that device group.
- Select **Surveillance Settings** in the **Settings** menu to configure cameras for all device groups.

"Surveillance Settings" display

Use this display to configure how the InfraStruXure Central server affects and responds to cameras at monitored NetBotz Appliances.

General Surveillance Settings

These settings are used by the InfraStruXure Central server to manage the selected camera or cameras. They configure the server's behavior with regards to a camera.

Element	Description
License Camera	Select this option to apply an available Surveillance license to each selected camera. If you deselect this option, the selected camera's surveillance is disabled, and its license can be used to enable surveillance for a different camera. **Note:** Disabled when no license is available.
Thumbnail Activity Timeout (seconds)	Define how long a selected camera's thumbnail will be highlighted before returning to normal when a motion is detected: the minimum is **10**, the maximum is **120**, and the default is **30**.
Include Audio	Select to include the audio stream from a camera saved with that stream's relevant image clips (not selected, by default). **Note:** The camera must be configured to send audio; otherwise, this option is not available. If the camera is not configured to always send audio, only white noise will be recorded if **Include Audio** is selected. The camera setting can be accessed through the APC NetBotz Advanced View application.
Generate Digital Signature	Select to generate a digital signature when a surveillance clip is archived. **Note:** Digital signatures are designed to ensure that the signed media has not been altered in any way.

Server Settings

These settings are used to identify the InfraStruXure Central server (the current server, by default) to which data from a selected camera or cameras will be sent, and to define **Port** and **SSL Options** used to communicate with that server.

Note: A "Server settings unavailable when cameras are on both the Public Network (LAN1) and the Private Network (LAN2)" appears in this section when configuring multiple cameras using "Surveillance Settings" display, and some of those cameras are on the Private LAN, and some on the Public LAN. You cannot assign Private LAN server settings to a Public LAN camera, and vice versa.

Element	Description
InfraStruXure Central server	Identify the name of the InfraStruXure Central server where data from the selected camera will be sent. **Note:** By default, the name of the current InfraStruXure Central server is provided.
Port	Identify the port used by the server to connect with the selected camera.

	80 is the default value for HTTP communication when the **Connect using SSL Option** is disabled. **443** is the default value for HTTPS communication when the **Connect using SSL Option** is enabled. **Note:** The port number must match the port number defined in the identified InfraStruXure Central server's **Web Server** tab for **Server Access**, a **Server Administration Settings** option in the **Settings** menu. Otherwise a NetBotz Appliance associated with the selected camera or cameras cannot send surveillance data to the server successfully.
Connect using SSL	Select to have the server use the Secure Sockets Layer (SSL) protocol when communicating with the selected camera (not selected, by default).
SSL Options	Select the method of verification to be used when licensed cameras attempt to connect to the server using the SSL protocol. **No Verification**: requires SSL support on the server (do not send data without it), but accepts any certificate provided by the server (i.e. self signed certificates will be allowed). This is the default setting. **Verify Certificate**: requires SSL support on the server (do not send data without it), and only accepts 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**: requires SSL support on the server (do not send data without it), and only accepts 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). **Note:** Disabled when **Connect using SSL** is not selected.

Surveillance Activation Settings

These settings control how the InfraStruXure Central server responds to motion detected at the selected camera or cameras.

Element	Description
Post Mode	Select when clip images (and, optionally, audio) from the camera will be stored on the server.

	Send on Motion Detected the camera will send clips to be archived whenever its motion sensor is activated (the default selection). **Send Continuously During Alerts that are Configured to Trigger Cameras**: the camera will send clip images to be stored whenever an alert triggers the camera. **Send on Motion Detected During Alerts that are Configured to Trigger Cameras**: the camera will send clip images to be archived if motion is detected during an alert. **Disabled**: no surveillance data will be automatically stored. **Note:** When using a post mode that requires a camera to be triggered by an alert, that camera must be selected by an alert threshold's **Cameras to Trigger** option in the **Advanced** tab of the threshold's "Configure Settings" display. For more information, see Alert Thresholds under Alert Settings(Settings menu).
Event Send Retry (seconds)	Specify how many seconds the camera will wait before it attempts to post again, if it receives no response when attempting to send a clip to the InfraStruXure Central server (a minimum of **5**, the default, and a maximum of **60**).
Camera Resolution	Select the resolution used for the images captured by the camera. **Note:** The available sizes depend on the capabilities of the selected camera, with larger image resolutions requiring increased amounts of storage space.
Target Image Capture Rate	Set the number of frames per second to be recorded when a clip is captured (1 frame per second, by default).
Event Duration Trigger (seconds)	Set the amount of delay between the start of an event and the beginning of a clip's capture.
Advanced Scheduling	Click to use the "Advanced Scheduling" display to specify when the camera is enabled and disabled (always enabled, by default).

Using post mode:

Use the four **Post Mode** setting options to determine what conditions will trigger the capture of data from the camera.

Note: When using a post mode that requires a camera to be triggered by an alert, the camera must be selected by the **Camera to Trigger** option for the alert threshold that the alert is responding. Right-click the device in the **Device** or **Map View** and use an **Alert Thresholds** option to edit an existing threshold or add a new one.

Disabled:

The **Disabled** option prevents data from the camera from being archived, even during an alert.

You may want to set a camera to **Disabled** if you need to temporarily disable capture on a camera for a non-repeating interval of time.

Note: If you want to disable capturing for a repeating interval of time, you should use the **Advanced scheduling** option on the "Surveillance Settings" display.

Send Continuously During Alerts that are Configured to Trigger Cameras:

Choose this option if you need to create a complete auditable record of all activity (and non-activity) that occurs for the duration of an alert configured to trigger the camera.
Note: An alert can result in a camera's surveillance data being continuously sent only when that alert is in response to an alert threshold which has that camera selected by that threshold's **Camera to Trigger** option.

Surveillance events created using the **Send Continuously During Alerts that are Configured to Trigger Cameras** 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.

Note: You may not want to use this setting with alerts that are set to **Return to normal requires user input**. If a delay occurs before the alert is resolved, this setting can generate very large clips.

You can use the **Send Continuously During Alerts that are Configured to Trigger Cameras** mode under the following circumstances:

- You are in a high security environment where you are required to have a complete audit record of all time-stamped 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 this option 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.

You can use the **Send on Motion Detected** setting 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 that are Configured to Trigger Cameras:

Choose this option if you need to create records of any movement that occurs in the installation location for the duration of an alert configured to trigger the camera, but a visual record of the time that passes between detected motion is not needed.

Note: An alert can result in a camera's surveillance data being sent when motion is detected only when that alert is in response to an alert threshold which has that camera selected by that threshold's **Camera to Trigger** option.

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.

You could use the **Send on Motion Detected During Alerts that are Configured to Trigger Cameras** 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 the **Advanced scheduling** option, 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.

"Advanced Scheduling" display:

Use this display to define the specific periods of time, for each day of the week, during which an associated activity will be disabled (by default, scheduling is enabled 24 hours a day, seven days a week).

Note: This display is used to schedule when an alert action will be enabled and disabled, using the action's settings display, or to schedule when a camera is enabled or disabled, using the "Surveillance Settings" display.

The table provides cells for 15-minute increments, and columns for every day of the week. You can do all of the following to schedule when an alert action, or camera, is enabled:

- Click a column title to enable or disable all of that day's cells.
- Drag your mouse from one cell to another cell in a column, to enable or disable a set of cells.
- Drag your mouse from a cell in one column to a cell in another column, to enable or disable an identical set of cells for each of the selected days.
- Click a single cell.
  Note: The NetBotz Appliance also can schedule a camera's surveillance activity. The camera will not capture data when either the InfraStruXure Cental server or the NetBotz Appliance has surveillance disabled; both must have surveillance enabled, to capture data.

"Surveillance Settings" wizard

Use the "Surveillance Settings" wizard to define the "Surveillance Settings" display settings for the cameras selected by **Surveillance Settings** in the **Thumbnails** view, **Device Groups** view, or **Settings** menu.

- **Surveillance Settings** in a thumbnail view's right-click menu accesses the wizard for multiple selected cameras.
  Note: When the thumbnail for only one camera is selected, the "Surveillance Settings" display is accessed directly.
- **Surveillance Settings** in a device group's right-click menu accesses the wizard for for the cameras associated with that device group.
- **Surveillance Settings** in the **Settings** menu accesses the wizard for the cameras associated with all device groups.

The "Surveillance Settings" wizard uses three displays, in addition to the "Surveillance Settings" display: two to select the cameras to be configured, and one that reports the results of that configuration.

"Select Camera Type" display

Use this display to select what type of cameras you want to configure: **320/420 Series**, **550/500/455/450/355 Series**, **CCTV Devices**, or **Other Cameras**.

Note: Only cameras of the selected type will be listed in the "Select Surveillance Devices" display that appears when you click **Next**.

"Select Surveillance Devices" display

Use this display to select the camera or cameras you want to configure. This display lists all NetBotz Appliances the InfraStruXure Central server is monitoring.

What cameras are listed depends on the type selected in the "Select Camera Type" display, and the **Surveillance Settings** option used.
Note: If none of the selected cameras match the type of camera selected in the "Select Camera Type" display, no cameras are listed.

- **Surveillance Settings** in the **Settings** menu: all cameras of the selected type at all monitored NetBotz Appliances.
- **Surveillance Settings** right-click option in the **Device Groups** view: all cameras of the selected type at all monitored NetBotz Appliances assigned to the selected device group.
- **Surveillance Settings** right-click option in the **Thumbnails** view: all cameras of the selected type for the selected thumbnails.
  Note: When only one camera is selected in the **Thumbnails** view, the right-click **Surveillance Settings** option accesses the "Surveillance Settings" display directly.

"Configured Surveillance Devices" display

Use this display to review a list of the surveillance devices that were configured using the "Surveillance Settings" display.

Note: Only the cameras you just configured are listed, and not any previously configured cameras.

Surveillance clips

Surveillance clips are generated as a result of detected motion, alarm, or motion and alarm, depending on how surveillance for each camera is set up.

Surveillance clips have the ability to be much longer in length, and larger in size, than camera capture clips for alarms: surveillance clip settings (such as resolution and frame rate) are independent of the camera capture settings for alarms.

- Inactivity (no motion) of 10 seconds or more will cause a new clip to be created the next time motion is detected.
- Inactivity of less than 10 seconds, will add new frames to the current surveillance clip.

The settings that control the generation of surveillance clips are located in the "Surveillance Settings" display accessed by the **Surveillance Settings** options in the **Settings** menu, right-click menu in the **Device Groups** view, or right-click menu in the **Thumbnails** view.

Note: The settings that control the generation of alarm clips are controlled by the **Alarm Capture Data** option in the "Capture Settings" display, a display accessed by **Camera Settings**, a **NetBotz Appliance Configuration** option in the **Settings** menu and the **Device Groups** view right-click menu, or by **NetBotz Appliance Camera Settings**, a right-click menu option in the **Thumbnails** view.

Surveillance clips are stored on the InfraStruXure Central server and can be tagged with metadata that allows users to search for specific clips. The location where the server stores clips is defined using **Storage Settings**, a **Server Administration Settings** option in the **Settings** menu.

The size of a surveillance clip is based on the resolution and frame rate of the camera that generated it. These settings are controlled by a camera's "Surveillance Settings" display settings.

You may export clips in AVI, Signed AVI, or MPEG-1 formats. You can also export the currently viewed image as a JPG file. If audio data for a clip exists, it must be exported to a separate file.

Digital signatures

NetBotz devices provide the capability to attach a digital signature to the generated clip. This signature is used by the verification utility to determine if any tampering with the clip occurred. If a clip has a digital signature attached to it, the **Is Signed** column in the clip listing pane of the "Recorded Camera Clips" display reports **Yes**, and the "Clip Viewer" display will show the digital signature icon (✏) in color.

InfraStruXure Central ships with a Windows batch file and a Linux script located at the root directory of the InfraStruXure Central application that can authenticate the existence of a clip's digital signature. Both are run using the same syntax structure:

Windows: avivrfy.bat avi1 avi2 avi3

Linux: avi-verify avi1 avi2 avi3

This syntax allows you to check multiple AVI files by including each file's name in the command line, with a space separating each name.

When the the verification utility is run, it returns a message for each file that states whether the digital signature is valid.

Audio support

Audio can be captured from camera devices equipped with audio sensors.

Audio data is stored in the OGG Vorbis codec file format, with an.ogg file extension. You need an audio player that supports this file format in order to play back the exported file.

Note: If your media player cannot play the.ogg file format, you may need to download an additional codec to support the audio file format. Consult your media player help or documentation for details on installing additional codecs.

"Recorded Camera Clips" display

Use this display to retrieve clips by date or tag/description, and to view, tag, export, and delete existing surveillance clips.

This display only retrieves clips for the camera or cameras associated with the **Retrieve Clips** right-click menu option or icon (🎞) used to access it.

- The cameras selected in the **Thumbnails** view when the **Retrieve Clips** option or icon is used (the display's description identifies the selected cameras).
- The cameras in the group selected in the **Device Groups** view when the **Retrieve Clips** option or icon is used (the display's description identifies the selected device group).

The display has three areas, each with elements that provide for a specific function: a retrieve clips section, a select clips section, and an **Overview**.

Retrieve clips section

This section consists of the elements used to identify and retrieve the clips for a specified **Choose Date** time frame, and when **Search by Tag** is enabled, limit the clips to those that match the provided **Tag/Description** information.

Element	Description
Choose Date: Relative	Enables searching by relative time to the current time. The available values are: **Last Hour**, **Last 6 hours**, **Last 12 hours**, **Last Day**, **Last Week**, **Last Month**, **This Day**, **This Week**, **This Month.** Values that start with "Last" use the current time and date and search backward for the specified time period. Values that start with "This" use the current date and search the corresponding time period that matches the criteria. For example, if the current date and time is February 22nd at 4:00pm, and you select **Last Month**, you will get all surveillance clips recorded since January 22nd at 4:00pm. If you selected **This Month**, you would see a listing of all clips recorded since February 1st at 12:00am. The **Relative** setting defaults to **Last Hour**. **Note:** The weekly period begins at 12:00am on Sunday and ends Saturday night at 11:59pm.
Choose Date: Range	Enables searching for recorded clips during the dates identified by **Start Date** and **End Date**. The **Start Date** is the earliest date that will be checked for clips. The **End Date** is the most recent date that will be checked for clips. **Note:** Both the **Start Date** and **End Date** default to the current date.
Tag/Description	Select to search only for clips that include the typed tag data or clip descriptions, that were recorded during the Choose Date time frame, for the cameras selected when the "Recorded Camera Clips" display was accessed.

	For example, typing "fan" will retrieve only clips that have tags or descriptions that contain "fans", "cooling fans" "heating fan", etc. recorded for the selected cameras during the defined time frame. You can select a tag from the drop-down menu to the right of the text field which lists all the tags added to recorded clips for the selected cameras.
Retrieve Clips	Click **Retrieve Clips** to search the repository for all clips that match the currently selected criteria.

Select clip section

This section lists the clips that were retrieved as a result of the current search, and allows you to view, tag, or export one clip at a time, or delete one or more clips.

Clips can be sorted by clicking any column heading.

Action Button	Description
List	Lists and provides information about the retrieved clips. **Camera**: camera associated with the clip. **Start Time**: date and time the clip started. **Duration**: how much time the clip involves. **Frames**: how many frames the clip contains. **Tags**: any tag assigned to the clip. **Is Signed:** whether the clip is signed or not. **Has Audio**: whether audio is associated with the clip.
View	Click to use the "Clip Viewer" display to view, tag, or export the clip selected in the list.
Tag	Click to use the "Edit Clip Tags and Description" display to enter information into the **Tag** and **Description** fields for the clip selected in the list.
Export	Click to use the "Export Clip" display to export the clip selected in the list in an **MPEG-1**, **AVI**, **Signed AVI**, **Current Image,** or **Audio** format.
Delete	Click to delete the clip or clips selected in the list.

Overview section

This area displays provides a thumbnail for the clip selected in the list, and provides any tag or description associated with that clip.

Area	Description
Clip Thumbnail	Displays a small version of the first frame of the clip selected in the list.
Tag Area	Displays tag information, if any exists.

Description Area	Displays description information, if any exists.

"Clip Viewer" display

Use this display to view, tag, and export a selected clip.

Element	Description
Camera Information	This area at the top of the display provides the following information: • **Label**: the label that identifies the camera. • **Hostname**: the hostname of IP address of the camera's NetBotz Appliance.
View Pane	Shows the content of the clip.
Play/Pause (▶ and ⏸)	Click the **Play** icon to start the clip; click the **Pause** icon to pause the playback on the current image. You may begin playing the clip during the load sequence, if you desire.
Clip Slider Bar	Drag the control left or right to find a specific frame within the clip. The number to the right of the bar shows the currently displayed frame. You also can click the up and down arrows to the right of the slider bar to advance or rewind the clip by a single frame. The beginning and ending date and time of the clip are displayed below the slider bar.
Export icon (⇱)	Click this icon to access the "Export Clip" display.
Tag icon (🏷)	Click this icon to access the "Edit Tags and Description" display.
Audio icon (🔈)	If there is audio associated with the current clip, this icon is displayed in black; if there is no audio, the icon is grayed out.
Digital Signature icon (✏)	If the clip has a digital signature associated with it, this icon is displayed in color; if the clip is unsigned, the icon is grayed out.
Status area	Displays the loading status of the selected clip: **Loading** or **Loading Complete**.
Clip Information	Displays the following information about the current clip: • **Total Frame Count** • **Duration** • **Resolution** • **Tags** • **Description**

"Edit Clip Tags and Description" display

Use this display to add text strings to surveillance clips as a **Tag** or **Description**.

Text contained in the **Tag** or **Description** fields can be used as search criteria when attempting to retrieve a specific clip.

Text Fields	Description
Tags	Enter text into the **Tags** field to associate the data with the selected clip as metadata. This data can be used to refine future searches to only clips containing the appropriate keywords.
Description	The **Description** field can be used to enter a longer description of the contents or context of the clip. The contents of the description field can be searched on from the "Recorded Camera Clips" display, but will not be listed in the drop-down list of available tags. **Note:** The **Description** field cannot be longer than 65536 single-byte characters.

"Export Clip" display

Use this display to export the selected clip in an **MPEG-1**, **AVI**, **Signed AVI** (if the digital signature option is enabled), **Current Image**, or **Audio** format.

Note: This display can be accessed from the "Clip Viewer" display, or from the **Clip** option in the "View Alarm Details" display available for the **Active Alarms** and **Alarm History** views, using the **Export Clip** icon (📤).

Element	Description
Data Format	Use to select the desired format as the output type. • **MPEG-1** **Note:** Disabled when a clip consists of a single frame. • **AVI** • **Signed AVI** (see below) • **Current Image** • **Audio** The **Signed AVI** format is only available if the clip was captured by a camera with the **Generate digital signature** option in the "Surveillance Settings" display enabled. **Note:** The **Signed AVI** option is only available if the NetBotz Appliance has the optional Premium Software Module installed. If the **Current Image** option is selected, the currently displayed frame will be saved as a JPG file.

	When clips are recorded, the images and audio are saved as separate files. Therefore, an exported clip cannot contain both image and audio data. The audio can be saved to a separate file by selecting the **Audio** option. **Note:** If a clip contains audio data, but the audio capture option on the remote device was not activated, only white noise will be recorded.
Filename	Use to set the location and the filename of the exported clip.