Online Help

EcoStruxure IT Data Center Expert

Version 9.2.0

What's new in EcoStruxure IT Data Center Expert 9.2.0

Learn more about the new features available in Data Center Expert 9.2.0 release.

Desktop client

This release contains new features and enhancements including:

- **Required passwords for backups**

  A password is now required for all backup configurations, and administrators are alerted at login to set passwords on existing backup configurations if they are not present. To configure a backup password, go to **System > Server Administrator Settings > Server Backup/Restore**.
- **Administrators can terminate other users' sessions**

  Administrators can now terminate all active Desktop Client, Web Client, and REST API sessions from the **Logged On Users** view. Access this view by clicking the **User: [name]** indicator in the bottom-right status bar of the desktop client. The terminated user receives a notification and is logged out of the client.
- **Improved chained certificate imports**

  You can now import DCE server chained SSL certificates into the desktop client change certificate wizard. Go to **System > Server Administration Settings > Server Access > Change Certificate...**

  When importing a certificate chain, certificates must be provided in the correct order: **Server/Leaf Certificate —> Intermediate Certificate(s) —> Root Certificate**. Importing certificates in an incorrect order may prevent chain validation and can result in misleading errors, such as a private key mismatch.

Web client

This release contains new features and enhancements including:

- **Device Groups Tree**

  All device groups are now displayed and selectable in the **Monitoring** tab. The **Active Alarms** list and **Devices** list are automatically filtered based on the selected group.
- **Improved device list in Monitoring**

  The Devices section is now displayed as a table, making it easier to browse devices. You can filter the list, customize displayed columns, and export the device list data to CSV or TXT files.
- **Administrators can terminate other users' sessions**

  Administrators can now view and terminate all active Desktop Client, Web Client, and REST API sessions. To access it, click the **View Status** icon in the upper-right corner of the web client and select the **Logged On Users** tab. The terminated user receives a notification and is logged out of the client.
- **Desktop notifications for alarms**

You can now receive desktop notifications for qualifying alarms. Enable the feature in **User Preferences** and configure the minimum alarm severity for notifications. Notifications are displayed even when the application tab is active.

- **Icon notifications for new alarms**

  You can now enable icon notifications in **User Preferences**. A notification indicator is displayed on the browser tab icon when new alarms arrive while you are away from the tab. The indicator is cleared when you return and interact with the application.
- **Request device scan**

  In the **Monitoring** tab, server and device administrators can now request a device scan from the **More actions** menu **> Request Scan**.
- **Export Reports as PNG**

  Reports can now be exported as a single image including both the chart and table.
- **Edit a device's label and type**

  In the **Monitoring** tab, server and device administrators can now use **More actions > Edit Settings** to change a device's label or type, or reset either value to its default.
- **New dashboard drawer**

  In the **Dashboards** tab, click **Show Dashboard List** to search for dashboards. Dashboards now display a scope indicator icon, with a multi-user icon for global dashboards and a single-user icon for personal dashboards.
- **Filter alarms by device or group**

  In the **Alarms** tab, you can now filter the alarms list without leaving the page. Open the **Filter alarms by device or group** drawer from the toolbar to choose which devices and groups to include.
- **New reports table view**

  Saved Reports can now be browsed in a table view, allowing you to sort and filter reports by criteria such as name, sensors, start date, and end date.
- **Larger sensor result sets in Reports**

  Added selectable sensor result page sizes (25, 50, 100, 200, and 500), making it easier to generate reports for large sensor sets.
- The event log now includes entries for backup/restore password changes.

General

- **Device scan and upgrade events added to event log**

  Device scans initiated through **Request Device Scan** and DCE server upgrades now generate dedicated event log entries. This makes it easier to identify device scan activity and distinguish upgrade-related restarts from expected or unexpected restart events.
- **REST API best practices**

  Added REST API best practices to the Help documentation in the web client to improve guidance on API usage and integration.
- **Improved subscription expiration warning emails**

  Subscription license expiration notifications sent 90, 60, and 30 days before expiry now identify the functionality affected by license expiration, including software updates, device firmware updates, and camera clip retrieval and export capabilities.
- **Added support for SNMP Opaque OID types for float and double values**

Note: If your device requires Opaque SNMP OIDs, any existing third-party DDFs may need to be updated to support them. If updates are needed, submit a DDF request through the support request page .

Visit the EcoStruxure IT Help Center for more information about Data Center Expert.

About Help

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

To open help in a separate Help browser window, select **Help Contents** in the **Help** menu.

To open the **Help** view for the currently selected view, select **Dynamic Help** in the **Help** menu, or by press F1. This **Help** view provides access to information directly related to the selected view; 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.

Select **What's New** in the **Help** menu to see information about new features and enhancements.

Click **EcoStruxure IT Help Center** in the **Help** menu to access the most up-to-date Data Center Expert documentation online. Visit the help center

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 EcoStruxure IT Data Center Expert	Opens the "About Data Center Expert" display which provides copyright information, version information and whether FIPS mode is active or inactive on the client and server, and the MAC address and serial number of the Data Center Expert server. Click the Copy button to easily capture the version information, and the MAC address and serial number.

"About Data Center Expert" display

This display, accessed by selecting **About** in the **Help** menu, provides software version and build numbers, the MAC address of the Data Center Expert server, and copyright information.

A unique serial number is generated for the Data Center Expert virtual appliance at startup and is available in this display.

The serial number for a Data Center Expert hardware server is available only on its serial number sticker.

Note: Please have the software version and build numbers, and the Data Center Expert server MAC address and serial number available when contacting support.

Console features

The Data Center Expert 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 console provides the Data Center Expert client access to server functions and features. This console has the following major elements:

- An application bar that provides access to **Monitoring**, **Surveillance**, **Alarm Configuration**, and **Reports** perspectives and views
- Seven main menus (**File**, **Device**, **Alarm Configuration**, **Updates**, **System**, **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 four 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 Data Center Expert server using **License Key** in the "Server Administration Settings" display accessed by **Server Administration Settings** in the **System** menu.
- **Alarm Configuration** provides options used to configure how the Data Center Expert server reports alarm conditions.
- **Reports** provides access to reports about the devices the Data Center Expert server monitors.

When you log on to your Data Center Expert server, the console opens with the **Monitoring** perspective displayed; **Monitoring**, **Surveillance**, **Alarm Configuration** , and **Reports** buttons below the main menus allow you to switch between perspectives.

Monitoring

This perspective opens with five 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.
- **Virtual Sensors** view: allows users with Device Administrator or Server Administrator to create, modify, and delete virtual sensors.

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.
- **Custom Properties Editor** view: allows you to add, edit, or remove custom property keys, and modify their value, on devices and sensors selected in the Device View or Map View.
  Note: The value of a custom property key must be modified one device or sensor at a time.
- **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 Data Center Expert server monitors.
- **Firmware Update Status** view: allows you to view information about the status of ongoing update processes for monitored SNMP devices and NetBotz Appliances.
- **Device Configuration Status** view: allows you to view information about the status of ongoing configuration processes for monitored SNMP devices and NetBotz Appliances.

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.

Alarm Configuration

This perspective opens with two views displayed, by default.

- **Navigation** view: provides a list of device groups and devices monitored by the Data Center Expert server, and allows you to create thresholds by device or by device group, and add them to notification policies.
- **Threshold Alarm Configuration** view: provides a list of thresholds associated with the device group or device selected in the **Navigation** view, and allows you to modify thresholds by type or by device, and add them to notification policies.
- **Device Alarm Configuration** view: provides a list of device alarms associated with the device group or device selected in the **Navigation** view, and allows you to modify alarms by type or on the device that reports the alarm.
- **Notification Policies** view: allows you to create and edit the policies used by the Data Center Expert server to generate alarm notifications, and view the thresholds you have added to those policies.

Reports

This perspective opens with the **Available Reports** displayed by default, including Sensor History Reports, **Snapshot Reports** , and Saved Sensor Reports. When an available report is generated, that report appears in its own view.

Snapshot Reports include:

Battery Age

Device Type Inventory

Environmental Humidity

Environmental Temperature

UPS Runtime

Main menus

A menu bar immediately below the console title bar provides seven menus, with options that control or configure Data Center Expert features and functions.

Menu	Options
File	**Change Server**: closes the session, and accesses the " Data Center Expert Logon" display. **Reboot Server**: reboots the Data Center Expert server. **Note:** When a reboot finishes, an e-mail is sent to the **Data Center Expert Administrator** users that include an e-mail address as part of their user credentials. **Shut Down Server**: shuts down the Data Center Expert server. **Client Preferences**: accesses settings specific to the Data Center Expert client you use. **Exit**: closes the Data Center Expert client.
Device	**Add Devices**: accesses the "Device Discovery" wizard used by the Device discovery processes. **Create Virtual Sensor**: accesses options to create a virtual sensor used to monitor the average or total value of multiple numeric sensors of the same sensor type. **SNMP Device Communication Settings**: accesses options used to configure various functions for how the Data Center Expert server communicates with, and monitors, SNMP devices. **Modbus Device Communication Settings**: accesses options used to configure various functions for how the Data Center Expert server communicates with, and monitors, Modbus devices. **Note:** Modbus support is a separately-licensed feature. **NetBotz Appliance Communication Settings**: accesses options used to configure various functions for how the Data Center Expert server communicates with, and monitors, NetBotz Appliances. **NetBotz Appliance Configuration**: accesses an **Alert Settings** option used to define the alert notifications generated by each monitored NetBotz Appliance, as well as options used to configure various functions at the monitored NetBotz Appliances.

Menu	Options
	APC SNMP Device Configuration: accesses settings used to select an APC SNMP device or saved configuration file, and use it to configure settings at the other APC SNMP Devices monitored by the Data Center Expert server. **Manage Custom Property Keys**: accesses settings used to create, modify, or remove user-created property keys for monitored devices. **Surveillance Settings**: accesses settings used to configure various functions for the surveillance devices at monitored NetBotz Appliances.
Alarm Configuration	Defines how the Data Center Expert server performs notifications when thresholds and device alarms are triggered for its monitored devices. **Create Thresholds**: accesses options used to define the threshold alarms for devices monitored by the Data Center Expert server. **Create Notification Policy**: accesses settings used to create a notification policy used by the Data Center Expert server to generate alarm notifications. **Manage Alarm Actions**: accesses settings used to create, modify, and delete alarm actions from the Data Center Expert server. **Network Management System Integration**: accesses settings used to enable the Data Center Expert server to send SNMPv1/SNMPv3 traps to defined Network Management System consoles for alarms that occur at the monitored SNMP, Modbus, and NetBotz Appliances, and associated devices.
Reports	Provides options used to generate Sensor History reports and Snapshot reports, and manage the export configurations that are used to export reports on a scheduled basis. **Generate Sensor History Report**: accesses the "Report Criteria" display used to generate Sensor History and Custom Sensor History reports. **Snapshot Reports**: generates the selected snapshot report for the device groups specified. **Manage Export Scheduling**: accesses the display used to schedule when reports will be automatically exported.
Updates	Provides options used to update the Data Center Expert server and its monitored NetBotz Appliances and SNMP devices. **Apply Firmware Updates**: accesses the "Select Device Update" display used to download firmware updates to monitored NetBotz Appliances or SNMP devices. **Apply Server Updates**: accesses the "Apply Server Update" display used to update the Data Center Expert server. **Schedule Update Checks**: accesses settings used to schedule when the Data Center Expert server will check for available APC device firmware updates.
System	**Server Administration Settings**: accesses options used to configure a wide range of Data Center Expert server functions. **Users and Device Group Access**: accesses the "Users and Device Group Access" display used to manage the users, the Monitoring and Surveillance access those users have to the device groups, and the authentication servers that provide remote access to the Data Center Expert server. **Building Management Settings**: accesses settings used to configure the MODBUS TCP Output Module support that allows a Building Management System to monitor status for the devices managed by the Data Center Expert server.

Menu	Options
	Note: MODBUS TCP Output Module support is a separately-licensed feature.
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**, **Surveillance**, and **Alarm Configuration** perspectives. **Alarms**: **Active Alarms** and **Alarm History** **Alarm Configuration**: **Navigation**, **Notification Policies**, **Threshold Alarm Configurations**, and **Device Alarm Configurations** **Device**: **Device Groups**, **Device View**, **Map View**, **Virtual Sensors**, **Saved Discoveries**, **Custom Properties Editor**, **Device Configuration Status**, and **Firmware Update Status**. **Surveillance**: **Thumbnails** only
Help	Provides options used to access the help, and information about the application. **EcoStruxure IT Help Center**: Provides access to the most up-to-date Data Center Expert documentation online. Visit the help center **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**, **Surveillance**, **Alarm Configuration**, or **Reports** perspective. **About EcoStruxure IT Data Center Expert** : Opens the display that provides software version and build numbers, the MAC address and serial number of the Data Center Expert server if available, and copyright information.

Status bar

Reports information about the Data Center Expert 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.
Devices	The number of devices the Data Center Expert 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.

User	The username you used to log on, and the hostname or IP address of your Data Center Expert client. Clicking this area accesses the "Logged on Users" display that identifies all users logged on at the server. **Note:** A lock icon is displayed in the status bar when the user is logged on using SSL.
Progress indicator	Shows the status loading device alarms, sensors, thresholds and other services when the Data Center Expert client starts.

"Logged on Users" display

Use this display to review information about users currently logged on to the server.

Display columns

The display shows the following information for each logged-on user:

- **Username** - The username of the logged-on user.
- **Client** - The hostname or IP address of the user's Data Center Expert client.
- **Logon Time** - The date and time when the user logged on.
- **Client Type** - The type of client being used: Desktop Client, Web Client, or REST API Client.

Terminating user sessions

Server administrators can terminate other users' sessions by selecting a user from the list and clicking the **Terminate Session** button. This feature allows administrators to:

- Force a user to log out if their session needs to be ended.
- Free up resources by terminating inactive or unused sessions.
- Respond to security concerns by immediately ending a user's access.

Note: You cannot terminate your own current desktop session. The terminated user will receive a notification that their session has been ended by an administrator.

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.

"Configure Columns" display

Use this display, accessed by the ( ) icon, to identify the columns that appear in various views and displays.

Initial setup requirements

The following actions should have been performed during the Data Center Expert 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 **System** menu, and then selecting **Network Settings** in the "Server Administration Settings" display.

With those actions performed, you can log on to the Data Center Expert desktop client and configure the server to use all of the Data Center Expert 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.

You can then use a browser to launch to the IP address or hostname of the Data Center Expert server, and access the **Data Center Expert web client**, a real-time overview of active alarms and device details for that server on a computer, tablet, or mobile device.

The Data Center Expert server includes a trial subscription license to monitor 5 nodes. The trial license expires after 90 days. A subscription license is then required.

Minimum setup requirements

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

1. If the Data Center Expert client is installed on your machine, go to step 3. Otherwise, do the following:
   a. Use a browser to launch to the IP address or hostname of the server.
   b. Log in to the **Data Center Expert web client** using the Administrator **Username** and **Password**, and click **Download Client** in the upper right corner.
2. Click **I agree** to accept the software license agreement, and follow the on-screen instructions to install the Data Center Expert client.
3. Launch your client and log on at the Data Center Expert server using the Administrator **Username** and **Password**.
4. Enable the Data Center Expert subscription license to start monitoring more than 5 nodes. Otherwise, go to step 5.
   a. Select **Server Administration Settings > License** in the **System** menu.
   b. Upload the license response file associated with the DCE server from the mySchneider Software Management website.
5. Make sure the administrator credentials include the e-mail address of the person you want notified when alarm conditions directly related to Data Center Expert server operations occur.
   a. Select **Users and Device Group Access** in the **System** menu.
   b. Select the **Data Center Expert Administrator** (**apc**, by default) in the **User and User Group Details** section of the **Users** tab, and click **Edit User**.
   c. Edit the **E-Mail Address** credential, if needed.
   Note: You can change the default **Username** and **Password** values, as well.
6. Define the e-mail settings the Data Center Expert server will use to send e-mails to the administrator when alarm conditions related to the server operations occur.

   a. Select **Server Administration Settings > E-mail Settings** in the **System** menu.
   b. Define the **Primary** and **Secondary** tab settings, as needed.
7. Add a remote NFS or Windows share repository the Data Center Expert server can use instead of the local repository.
   a. Select **Server Administration Settings > Storage Settings** in the **System** menu.
   b. Use the **Repositories** tab to add a remote repository.
   c. 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 Data Center Expert server configuration data, or its configuration and repositories data.
   a. Select **Server Administration Settings** in the **System** 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 (includes 200 and 750 series NetBotz appliances), SNMPv3 (includes 200 and 750 series NetBotz appliances), Modbus devices, and NetBotz Appliances (includes 300-500 series NetBotz appliances) you want your server to monitor.
   Note: All four device types require their own discovery process, not only on the public LAN, but on the private LAN, as well.
   a. Select **Add Devices** in the **Device** menu, or click the green + icon in the **Device View**.
   b. Select which type of device you want to discover (SNMPv1, SNMPv3, NetBotz Appliance, or Modbus TCP), 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 Data Center Expert server to monitor (SNMPv1, SNMPv3, NetBotz Appliance, or Modbus TCP), on both the public and private LANs.
10. Define any or all the alarm notifications you want available to the Data Center Expert server for any SNMPv1, SNMPv3, and Modbus devices discovered during step 9.
    Note: Additionally, each NetBotz Appliance has its own unique profiles it can use for alarm conditions at the devices it monitors (see step 13).

    The Data Center Expert server has a **Default** notification policy. Device alarms and communication link status thresholds for all monitored devices are included in the **Default** notification policy at device discovery.

    You must create at least one alarm action, and add it to the **Default** notification policy, or another notification policy you create, before the Data Center Expert server can generate alarm notifications for conditions that occur at monitored SNMP and Modbus devices.

    a. Select **Manage Alarm Actions** in the **Alarm Configuration** menu.
    b. Click **Create** to access the Alarm Action wizard.
    c. In the "Choose Alarm Action Type" display, select the type of alarm you want to create, and click **Next**.
    d. In the "Configure Alarm Action" display for the selected action, define the settings you want the action to use, and click **Finish** to exit the wizard.
11. Add alarm actions to the **Default** notification policy.
    a. In the **Alarm Configuration** perspective, in the **Notification Policies** view, select the **Default** notification policy. Right-click and select **Edit**.

Note: To create a new notification policy, right-click or use the **Create Notification Policy** icon.

b. Click **Add** to configure the alarm actions to add to the notification policy. Click **Manage Actions** to create alarm actions, or modify or remove existing alarm actions on the Data Center Expert server.
Note: You click **Choose Thresholds** to add user-created thresholds, for the device groups or devices selected, to the **Default** notification policy . Communication link status thresholds for monitored SNMP and Modbus devices are added to the **Default** notification policy at device discovery.

c. Check-mark one or more actions to configure their notification options, check-mark the actions you want to add to the notification policy, and click **OK**.

12. Create thresholds for sensor types supported by monitored devices.

    a. Select the sensor type on which you want to add a threshold from the **Create Thresholds** option in the **Alarm Configuration** menu. Alternatively, select a device group or device, and right-click to select the **Create Thresholds** option.
    b. In the "Select Threshold Type" display, select the threshold type you want to add, and click **Next**.
    c. In the "Select Sensors" display, select the sensor or sensors for which you want to add thresholds, and click **Next**.
    d. In the "Create Threshold" display, define the settings, and, if desired, click **Threshold Scheduling** to configure when the Data Center Expert server will generate notifications if the threshold becomes active. Click **Next**.
    e. In the "Select Notification Policies" display, select the notification policies to which you want to add the alarm threshold, and click **Finish** to exit the wizard.

13. Define any or all the alert actions you want available to any NetBotz Appliances discovered during step 9, to associate with the alert profiles used for alert notifications. Each NetBotz Appliance has its own unique profiles it can use for alarm conditions at the devices it monitors.
Note: An alert action must be available to the Data Center Expert server, and to each monitored NetBotz Appliance, for use with their alert profiles.

    a. Select **Alert Actions**, a **NetBotz Appliance Configuration > Alert Settings** option in the **Device** menu.
    b. In the "Select Alert Action Type" display, select an action.
    c. In the "Select Next Action" display, select **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 Data Center Expert server and monitored NetBotz Appliances.

14. Add at least one alert action to the one of the alert profiles used by each NetBotz Appliance for alert notifications.
Note: The profiles at a NetBotz Appliance may have been defined already. You can edit it to make sure someone in your organization is notified when problems occur.

    a. Select **Alert Profiles**, a **NetBotz Appliance Configuration > Alert Settings** option in the **Device** menu.
    b. In the "Select Parent Device" display, select the parent device (the individual NetBotz Appliance) associated with the profile you want to configure.
    c. In the "Select Alert Profile" display, select the alert profile you wish to modify, and click **Next**.
    d. Configure the alert 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 alert profile used by each monitored NetBotz Appliance.

Other support and feature setup requirements

Once the minimum setup requirements are defined, you can begin to configure the Data Center Expert 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 and user groups that you want to have access to the server, and define the monitoring and surveillance access that non- EcoStruxure IT Administrators users and user groups will have at the exiting device groups, by selecting **Users and Device Group Access** in the **System** menu.
- Customize the **Map View** for a group selected in the **Device Groups** view, by using the **Map Settings** and **Map Label Settings** right-click options in the **Map View**.
- Define any new alert actions, alert thresholds, and alert profiles you want to use for the NetBotz Appliances the Data Center Expert server monitors, using the **NetBotz Appliance Configuration > Alert Settings** options in the **Device** menu.
- Create virtual sensors to view and monitor the average or total value of multiple numeric sensors of the same sensor type, using the options in the **Virtual Sensors** view.
- Define any new alarm actions, thresholds, and notification policies you want to use for the SNMP and Modbus devices the Data Center Expert server monitors, using the options in the **Alarm Configuration** menu.
- Define the remaining administration settings, as needed, using **Server Administration Settings** in the **System** menu.
- Configure the settings the Data Center Expert server uses to communicate with its monitored SNMP devices, as needed, using **SNMP Device Communication Settings** in the **Device** menu.
- Configure the settings the Data Center Expert server uses to communicate with its monitored Modbus devices, as needed, using **Modbus Device Communication Settings** in the **Device** menu.
- Configure settings the Data Center Expert server uses to communicate with its monitored NetBotz Appliances, as needed, using **NetBotz Appliance Communication Settings** in the **Device** menu.
- Define custom property keys that describe monitored devices using the **Add Custom Property** option in the **Monitoring** perspective or **Custom Properties Editor** view.
- Manage custom property keys using the **Custom Properties Editor** view or **Manage Custom Property Keys** option in the **Device** menu.
- Configure the settings that affect how the surveillance equipment operates, using **Surveillance Settings** in the **Device** menu.
  Note: At least one camera must be defined as licensed to configure these settings.
- Define the settings for your Data Center Expert client, using **Client Preferences** in the **File** menu.
- Define how often you want the Data Center Expert server to check for firmware updates available from APC, using **Schedule Update Checks** in the **Updates** menu.
- Configure the settings the Data Center Expert 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 **Generate Sensor History Report** option in the **Device Groups** view, **Device View**, and **Map View**.
- Configure the Data Center Expert server to send SNMPv1traps and SNMPv3 informs to defined Network Management System consoles for alarms that occur at the monitored SNMP, Modbus, and NetBotz Appliances, and associated devices, using **Network Management System Integration** in the **Alarm Configuration** menu.
- Configure settings at one or more of the monitored APC SNMP devices, using **APC SNMP Device Configuration** in the **Device** menu.
- Select devices to enable for Modbus support, a separately licensed feature, using the **Building Management Settings** option in the **System** menu.

Data Center Expert Web Client

The Data Center Expert web client provides a real-time overview of active alarms and device details for the Data Center Expert server. The Data Center Expert web client is available on a computer, tablet, or mobile device with an internet browser, in English only.

To access the Data Center Expert web client, you use a browser to launch to the IP address or hostname of the Data Center Expert server, and provide a valid username and password for that server.
Note: To log in to the Data Center Expert web client, a user must have at least View Access for one device group that contains a minimum of one device.

For more information, see the help in the Data Center Expert web client.

Data Center Expert Virtual Appliance

The Data Center Expert server is available as a virtual appliance, supported on VMware ESXi 7.0.3. The full-featured demo of the virtual appliance monitors up to five device nodes and one surveillance node. You can purchase a license key to upgrade to a production version to monitor additional device nodes and activate supported applications, or to migrate from a Data Center Expert server hardware version to a Data Center Expert virtual appliance.

Note: VMware ESXi 4.1.0 was used as the reference virtualization platform during the development of the Data Center Expert 7.x virtual appliance, and is the first supported virtualization platform. The Data Center Expert virtual appliance is delivered as an OVA (Open Virtualization Archive), expected to function properly on any virtualization platform that supports this format, or has an appropriate converter utility.

To use the full-featured demo version of the Data Center Expert virtual appliance, you download the *.ova file from the APC web site, and deploy it to your virtualization platform using the default hardware configuration. For more information, see Data Center Expert virtual appliance equivalent configurations.

The demo version monitors a maximum of five device nodes and one surveillance node by default. You must upgrade the Data Center Expert virtual appliance demo to the production version to monitor 25 device nodes (as displayed in the Data Center Expert client "License Keys" display), add license keys to monitor additional nodes, or activate supported applications.
Note: You can add an additional network adapter to enable private networking, or add additional hard disks to increase storage, after the OVA template is deployed.

To upgrade the demo to the production version, you must purchase and apply an activation key, available on the APC web site. To monitor additional device nodes or activate supported applications, you must purchase and apply node license keys and application license keys for the virtual appliance.

To migrate a Data Center Expert hardware server to a virtual appliance, you must purchase and apply an activation key, and contact APC Support for new node license keys and application license keys for the virtual appliance. To receive these keys, you are required to provide a unique MAC address and serial number for the Data Center Expert virtual appliance, and for the Data Center Expert hardware server you are replacing.

A unique serial number is generated for the Data Center Expert virtual appliance at startup. It is displayed in the "About Data Center Expert" display, accessed from the **Help** menu. **Note:** The serial number for a Data Center Expert hardware server appears only on its serial number sticker.

This section of the Data Center Expert Virtual Appliance help fully describes deploying the Data Center Expert virtual appliance, and the upgrade and migration processes. It is available as a separate printable document on the APC web site.

Deploying and configuring a Data Center Expert virtual appliance

The Data Center Expert virtual appliance demo version monitors up to five device nodes and one surveillance node. You can upgrade to a production version after the OVA is deployed.

1. Download the *.ova file from the APC web site.
2. In your virtualization platform client interface, browse to the location of the *.ova file, and load the OVA. This may take several minutes.

   Alternatively, you may have the option to specify the URL for the *.ova file in your virtualization environment client interface.
3. Follow the prompts to accept the end user license agreement, and respond to options required to configure the OVA.

   Select thin provisioned disk format to allocate storage space on demand. Select thick provisioned disk format to allocate all storage space immediately.

Configuring the network settings

You must provide the MAC Address, IP Address, hostname, and network settings before using the Data Center Expert virtual appliance.

1. Select the Data Center Expert virtual appliance you created, and select the option to edit the virtual machine settings.
2. Specify the MAC Address for the virtual appliance manually.

   A unique MAC Address is required for each Data Center Expert . If the MAC Address originally assigned to the virtual appliance is changed, an error will occur on the primary interface, and the virtual appliance will not start.
3. Power on the virtual appliance.
4. In the console view, login to the virtual appliance using `apcsetup` as the username and password.
5. Within five seconds, press `m` to modify the settings.
6. Follow the prompts to specify the IP Address, hostname, subnet mask, and DNS servers for the virtual appliance.
7. After the virtual appliance has restarted, type its IP Address or hostname into a browser to login to the Data Center Expert client.

Adding an additional network adapter

You can add one additional network adapter to enable private networking. You cannot remove a network adapter once it has been added.

1. Gracefully shut down the virtual appliance.
2. Select the Data Center Expert virtual appliance, and select the option to edit the virtual machine settings.
3. Select the options to add an ethernet adapter.
4. Specify the type and the network connection.

   Ensure this connection is mapped correctly, particularly when the DHCP server will be enabled on the private network interface.
5. Power on the virtual appliance.
6. In the console view, login to the virtual appliance using `apcsetup` as the username and password.
7. Within five seconds, press `m` to modify the settings.
8. Accept the settings you configured previously, or modify settings if needed.
9. Press `y` to accept the **Enable private network interface** option.
10. Specify whether you want to enable the DHCP server on the private network interface.

Upgrading a Data Center Expert virtual appliance demo version to production

To upgrade from the demo to the Data Center Expert virtual appliance production version, you must install the activation key.

1. Purchase the activation key for the virtual appliance.
2. Login to the Data Center Expert client. In the "License Keys" display, accessed from the **Server Administration Settings** option in the **System** menu, and apply the activation key.
3. Apply the new virtual appliance node license keys and application license keys you received from APC Support.

   The upgrade is complete one you have applied the license and application keys. If you want to modify the virtual appliance settings, continue to Step 4.
4. In your virtualization platform client, gracefully shut down the Data Center Expert virtual appliance.
5. Select the option to edit the Data Center Expert virtual appliance settings.
6. Modify the hardware, if necessary.

   See help for Deploying and configuring a Data Center Expert virtual server, and Data Center Expert virtual server equivalent configurations.
7. Power on the virtual appliance.

Migrating a Data Center Expert hardware server to a virtual appliance

To migrate a Data Center Expert hardware server to a virtual appliance, you must purchase and apply an activation key. Additionally, you must contact APC Support for new node license keys and application license keys for the virtual appliance.

1. Perform a back up of the Data Center Expert hardware server, using the **Server Backup/Restore** option, accessed from the **Server Administration Settings** option in the **System** menu.
2. Deploy the demo version OVA, and configure it using the hardware equivalents for the Data Center Expert Basic, Standard, or Enterprise server from which you are migrating. **The available disk space for the virtual appliance must be greater than the disk space used by the hardware server.**

You cannot restore to a virtual appliance with fewer CPU, fewer network adapters, less RAM, or less available disk space than the hardware server.

See help for Deploying and configuring a Data Center Expert virtual appliance, and Data Center Expert virtual appliance equivalent configurations.

3. Perform a restore on the virtual appliance, using the **Server Backup/Restore** option, accessed from the **Server Administration Settings** option in the **System** menu.

   You cannot restore to a virtual machine other than the Data Center Expert virtual appliance.
4. Apply the activation key to the virtual appliance.
5. Login to the Data Center Expert client. In the "License Keys" display, accessed from the **Server Administration Settings** option in the **System** menu, apply the new node license keys and application license keys you received from APC Support.

Adding disk space to a virtual appliance

To increase storage for the virtual appliance, you must create additional hard disks.

You cannot change the size of an existing hard disk, or remove a hard disk once it has been created. An error will occur on the primary interface, and the Data Center Expert virtual appliance will not start.

1. Gracefully shut down the virtual appliance.
2. In your virtual server console, select the option to add a hard disk.
3. Choose the hard disk size.

   See Data Center Expert virtual server equivalent configurations.
4. Choose thin or thick provisioning.
5. Power on the virtual appliance.

Changes in the disk space will take effect once the Data Center Expert virtual appliance has restarted. Do not shut down the virtual appliance while the disk reconfiguration process is running.

The "Storage Settings" display, accessed from the **Server Administration Settings** option in the **System** menu, shows the total storage space available for the virtual appliance, not the individual hard disks.
Note: To store large amounts of surveillance data, using a remote repository is recommended.

About changing hardware resource settings for the Data Center Expert virtual appliance

After you have deployed the OVA, you can make changes to the Data Center Expert virtual appliance settings from your virtualization platform client interface. You use `apcsetup` as the username and password.

Network settings: You can configure an additional network adapter to enable the private network (APC LAN) as the apcsetup user or through the Data Center Expert client.

MAC Address settings: A unique MAC address is required for each Data Center Expert virtual appliance. If the MAC address originally assigned to the primary or secondary network interface is changed, an error will occur on the primary interface, and the virtual appliance will not start. A message will be displayed indicating the MAC address expected before normal startup will be allowed.

Hard disk settings: To increase storage for the virtual appliance, you can create additional hard disks. You cannot change the size of an existing hard disk, or remove a hard disk once it has been created. An error will occur on the primary interface, and the Data Center Expert virtual appliance will not start.

Changes in the disk space will take effect once the Data Center Expert virtual appliance has restarted.

The "Storage Settings" display, accessed from the **Server Administration Settings** option in the **System** menu, shows the total storage space available for the virtual appliance, not the individual hard disks.
Note: To store large amounts of surveillance data, using a remote repository is recommended.

RAM settings: You can add RAM to the Data Center Expert virtual appliance. You must gracefully shut down the virtual appliance to configure the settings.

CPU settings: You can add CPUs to the Data Center Expert virtual appliance. You must gracefully shut down the virtual appliance to configure the settings.
Note: VMware supports fault tolerance on virtual machines with 1 CPU only. Please refer to your vendor's documentation for more information about fault tolerance.

Hardware resource configuration guidelines

Use the DCE sizing guide to determine the hardware resources necessary for a Data Center Expert virtual appliance to monitor a given number of device nodes.

Note: VMware supports fault tolerance on virtual machines with 1 CPU only. Please refer to your vendor's documentation for more information about fault tolerance.

The disk space required to monitor a given number of nodes varies according to the device types monitored and the amount of data you want to store. The minimum hard disk size is 18 GB.

To determine whether to add another hard disk, you can view available disk space in the "Storage Settings" display, accessed from the **Server Administration Settings** option in the **System** menu. View this display periodically to help determine how quickly the virtual appliance consumes disk space.
Note: To store large amounts of surveillance data, using a remote repository is recommended.

Fault tolerant configuration guidelines

Use the DCE sizing guide to determine the hardware resources necessary for a Data Center Expert virtual appliance fault tolerant configuration.

VMware supports fault tolerance on virtual machines with 1 CPU only. Please refer to your vendor's documentation for more information about fault tolerance.

Note: The actual number of device nodes supported varies according to the device types discovered.

Minimum and maximum Data Center Expert virtual appliance configurations

For information about supported configurations equivalent to Data Center Expert Basic, Standard, and Enterprise servers, see the DCE sizing guide .

Note: The actual number of device nodes supported varies according to the device types discovered.
Note: VMware supports fault tolerance on virtual machines with 1 CPU only. Please refer to your vendor's documentation for more information about fault tolerance.

Data Center Expert server equivalent configurations

The Data Center Expert virtual appliance equivalent configurations are based on Data Center Expert Basic, Standard, and Enterprise server hardware configurations in the DCE sizing guide .

Hardware Server	Virtual Appliance Equivalent
Data Center Expert Basic	Up to 500 device nodes supported 4 GB RAM 4 CPU
Data Center Expert Standard	Up to 2000 device nodes supported 8 GB RAM 8 CPU
Data Center Expert Enterprise	Up to 4000 device nodes supported 16 GB RAM 16 CPU

Server Administration Settings (System menu)

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

E-mail Settings option

Use this option's elements to enable your Data Center Expert 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 Data Center Expert server e-mail notifications.

These settings are used by the Data Center Expert server to send e-mail alarm notifications for monitored SNMP and Modbus devices, and for e-mail messages related to Data Center Expert server functions, such as storage disk status and repository purge messages.

E-mail notifications for Data Center Expert server system events are sent in batches every two minutes. These notifications repeat every five minutes, then every ten minutes, then every hour until the event clears. No notification is sent when the event clears.

Note: Up to a two-minute delay in sending a notification is possible, depending upon when the event occurred, or when the notification should repeat, in relation to the interval at which email notifications are sent.

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

"Server SSL Certificates" display

Use this display to manage the SSL certificates on the **Data Center Expert** server used for secure communication with an SMTP server, Active Directory or OpenLDAP server, or a NetBotz Appliance.

For information about discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

You access this display from the **Server SSL Certificates** option in **Server Administration Settings**, a **System** menu option.

When you select **NetBotz Appliance** in the device discovery process, and select the security mode **Require SSL, validate certificates** option, use this display to add the certificate from the NetBotz Appliance you want to discover to the **Data Center Expert** server first. Otherwise, device discovery will not complete successfully.

Adding and removing server SSL certificates does not require the **Data Center Expert** server to reboot.

IMPORTANT: FIPS mode requires that certificates must include the Subject Alternative Name with the fully qualified domain name (FQDN) and IP address of the monitored device or connected server. New certificates may be required.

Element	Description
List	**Subject**: The name of the certificate. **Issued to (Organization)**: The name of the organization to which the certificate was issued. **Issued by (Organization)**: The name of the organization that issued the certificate. **Issued on**: The date the certificate was issued. **Expires on**: The date the certificate expires.
Add	Accesses the display used to import a certificate from a file, or paste a certificate into the text field.
Remove	Remove the selected certificate from the **Data Center Expert** server.
View	View details of the selected certificate.

License option

The EcoStruxure IT Data Center Expert server uses a subscription license to enable the software.

If your subscription has expired or the node count exceeds the amount allowed by your subscription, purchase a subscription or amend your existing subscription on mySchneider Software Management, https://www.se.com/myschneider/software/license .

Learn more about mySchneider Software Management

All device nodes including SNMP devices, Modbus devices, and NetBotz cameras for surveillance are included in the subscription node count. Separate licensing is not required.

DCE trial licenses including the Virtual Appliance trial license (AP94VMTRL) are for 5 nodes and expire after 90 days. A subscription license is then required.

- AP9465 - DCE Basic server, supports up to 540 nodes (525 nodes + 15 cameras)
- AP9470 - DCE Standard server, supports up to 2150 nodes (2025 nodes + 125 cameras)
- AP9475 - DCE Enterprise server, supports up to 4275 nodes (4025 nodes + 250 cameras)s

For details about sizing your DCE server or VM, see the DCE sizing guide .

Some DCE features are not available once the subscription license expires:

- Camera clip retrieval and export

  Note: The server will continue to collect camera clip data.
- DCE server software update
- Device firmware update

DCE server software updates and device firmware updates are not available with a trial license or when the number of monitored devices exceeds the subscription node count.

Element	Description
Server ID	The DCE server MAC address, used to associate the server with a DCE device in mySchneider Software Management
Node Count	The number of nodes allowed by the DCE subscription license
Used Node Count	The number of nodes currently monitored by the DCE server
Expires On	The date the DCE server subscription license expires. Server administrators will receive an email at 90, 60, and 30 days before expiration and when the license expires.
Expired	Whether the DCE server subscription license is expired, Yes or No
Trial	Whether the DCE server subscription license is a 5-node, 90-day trial license, Yes or No. Server administrators will receive an email prompt to obtain a subscription license.
Update License...	Upload the license response file from mySchneider Software Management to enable the DCE software with a new or amended subscription license. **IMPORTANT**: You must upload the response file within 30 days from the time it was generated.

Map Settings

Configure whether devices and sensors are automatically placed on maps. The Data Center Expert client must be restarted after disabling or re-enabling maps.

Element	Description
Normal	Devices and sensors are automatically placed on maps when devices are added to device groups, the default. All map features are available.
Automatic placement disabled	Maps must be manually edited to place devices and sensors on maps. All other map features are available.
Maps disabled	Map view is not displayed in the Data Center Expert client. Any maps that were associated with device groups will not be updated.

Network Settings option

Use this option's elements to define the settings the 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. The Data Center Expert server is not a multi-homed server.

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 Data Center Expert server will use to communicate on the public LAN, the port for which is labeled **1** on the Data Center Expert server.

Note: Changes are applied only in response to a Data Center Expert server reboot.

Element	Description
Hostname	Identify the Data Center Expert 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) Network A tab

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

Note: Changes are applied only in response to a Data Center Expert server reboot.

When **Reset APC Devices** is selected on the DHCP Discovery tab, only the devices on Network A, defined by the Data Center Expert server IP address and subnet mask, will be reset.

The Data Center Expert server is not a multihomed server. The private LAN (LAN2) is a private network used to communicate with devices monitored by the Data Center Expert server only. Integration with other network configurations, such as routing to a public LAN or redundant links, is not supported.

Element	Description
IP Address	Identify the private network address of the Data Center Expert 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 DHCP on Network A	Select to use the Data Center Expert server as a Dynamic Host Configuration Protocol (DHCP) server for the devices on the private LAN, Network A, enabled by default.
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.
Apply server time zone offset on Private LAN	Check-mark to assign the Data Center Expert server's time zone offset to the devices on the private LAN.

Private (LAN2) Network B tab

Use this tab to define the settings the Data Center Expert server will use to communicate on the private LAN, the port for which is labeled **2** on the Data Center Expert server. Devices with static IP addresses can be discovered on Network B on the private LAN.

Note: Changes are applied only in response to a Data Center Expert server reboot.

When **Reset APC Devices** is selected on the DHCP Discovery tab, devices on private LAN Network B, defined by its IP address and subnet mask, will not be reset.

The Data Center Expert server is not a multihomed server. The private LAN (LAN2) is a private network used to communicate with devices monitored by the Data Center Expert server only. Integration with other network configurations, such as routing to a public LAN or redundant links, is not supported.

Element	Description
Enable Network B on Private LAN	Select to use Network B on the Data Center Expert server private LAN for devices with static IP addresses.
IP Address	Identify the private network address of the Data Center Expert server private LAN Network B, 192.168.16.1 by default.
Subnet Mask	Identify the TCP/IP subnet address for the private LAN network B segment, 255.255.255.0 by default; otherwise, type in the subnet mask's IP address.

Private (LAN2) DHCP Discovery tab

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

Note: Changes are applied without a Data Center Expert server reboot.

Element	Description
Private Discovery Settings	**Enable Private DHCP Discovery**: select to enable the Data Center Expert 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 Data Center Expert 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 SNMPv1 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 Data Center Expert server registered as a trap receiver. **Write Community Name**: define the name that can be used to register the Data Center Expert server as a trap receiver at discovered APC SNMPv1 devices (**private** is the default).
Reset APC Devices	Click to reset private LAN APC devices, on Network A only, to use new IP addresses. **Note:** The **Write Community Name** is used to reset the APC devices.

Server Access option

Use this option's elements to enable, disable, and configure the security policy and settings associated with the different network-accessible processes that run on your Data Center Expert server: web server, SSH server, SNMP server, and security policy.

Web Server tab

Use the Ports section of this tab to enable or disable HTTP web communication and identify the IP port the Data Center Expert server uses for HTTP and HTTPS communication. Use the SSL Certificate section to change the current Secure Socket Layer (SSL) certificate used for HTTPS communication.

HTTP and HTTPS settings

Note: Enabling and disabling HTTP access or changing the HTTP or HTTPS ports used can prevent devices from providing data to your Data Center Expert server.

Option	Description
Enable HTTP Port	Select to enable the Data Center Expert server to use HTTP, a non-secure Internet protocol, for web communication at the defined IP port. HTTP is disabled by default.
Enable HTTPS Port	The Data Center Expert server always uses HTTPS, a secure Internet protocol, for web communication. You can specify the IP port, 443 by default.
Enable HTTP Strict Transport Security	Allow the Data Center Expert server to add an HTTP Strict Transport Security (HSTS) entry to HTTP response headers. This automatically redirects HTTP connections to HTTPS. If you select HTTP, it is recommended that you enable HSTS unless it prevents older NetBotz Appliances from posting successfully. Learn more about HSTS

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

Provides information about the current SSL certificate and allows you to change the certificate.

The Data Center Expert server generates a default, self-signed SSL certificate that can be used for secure HTTPS web communication.

- **Change Certificate**: Accesses the "Change 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.

Changing the SSL certificate

You can use the "Change 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 **Change 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 Data Center Expert 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 **Change 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 Data Center Expert 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 **Change 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.

"Change Server SSL Certificate" wizard

Use this wizard's displays to create self-signed certificates, add signed Secure Socket Layer (SSL) certificates that the Data Center Expert 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 Data Center Expert 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 Data Center Expert 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 Data Center Expert 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.

Session Settings option

Control how long a user session will remain connected while there is no user-initiated activity.

If the session remains idle beyond the session inactivity timeout, the user will be automatically logged out.

Element	Description
Enable session inactivity timeout	Check to enable and configure the timeout setting.
Session inactivity timeout (minutes)	Choose the time the session will stay connected while there is no user-initiated activity. The default is 5 minutes. **Note**: Allowing more than 30 minutes of inactivity is considered a security risk and is not recommended.

SSH Server tab

Secure Shell (SSH), a program that provides strong authentication and secure communications over insecure channels, is used to log on at a Data Center Expert server on the network,from a command line to execute commands at that server.

Note: SSH is primarily intended for use with technical support guidance in troubleshooting device issues.

Option	Description
SSH is currently running	Enabled by default. Allows SSH access to the Data Center Expert server. Disabling SSH will cause the SSH daemon to be terminated. No new SSH sessions will be allowed. Existing SSH sessions will not be affected.
SSH starts at boot time	Enabled by default. Starts 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 Data Center Expert 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 Data Center Expert server.
System Location	Identify the location of the Data Center Expert server.

Security Policy tab

Configure the system-wide cryptographic policy used by the Data Center Expert server. Crypto policies are a system component that configure the core cryptographic subsystem security policies instead of using individual configurations.

Select one of the cryptographic policies the Data Center Expert server supports:

- **Future**: Most restrictive to withstand near-term future attacks
- **Default**: Secure settings for current threat models
- **Legacy policy**: Least restrictive for maximum compatibility
- **DCE**: Custom policy, less restrictive than Default and more restrictive than Legacy
- **FIPS**: A policy level that conforms to FIPS 140 requirements

These policies are applied consistently to running services and are kept up to date as part of Data Center Expert software updates.

When a new policy is set, the web server and SSH server on the DCE server will restart.

The DCE policy is selected by default. The DCE policy is similar to the Legacy policy except that the DCE policy does not allow any RC4 or 3DES based ciphers.

See the documentation for security policy definitions from Red Hat here .

FIPS

Federal Information Processing Standards (FIPS) govern how devices and systems use cryptography and other information technology.

These standards were created by the National Institute of Science and Technology (NIST) to protect government data, and ensure those working with the government comply with certain safety standards before they have access to data.

When a system is in FIPS mode, it uses algorithms and libraries that comply with FIPS standards, and may also use additional data protection features. FIPS mode may also disable or restrict certain functions that don't comply with FIPS standards.

Note: In DCE, CIFS (Windows) mounts do not work when FIPS mode is enabled. MD5 authentication is required for CIFS, which is not supported in FIPS mode.

Server Backup/Restore option

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

The backup is delivered as a single file with a .dce file extension for easier filename filtering.

Note: If a server backup fails, an email is sent to the **Data Center Expert Administrator** users that include an email 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.
Configure Backup Password...	Set the password the Data Center Expert server will use to encrypt new backup files. A backup password must be configured before creating or editing a backup configuration.
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 email will be sent to the **Data Center Expert 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 Data Center Expert server.

Managing the backup entries

At least one backup entry should be defined and used to create scheduled backup files for the configuration data on the Data Center Expert server, or its configuration and repository data.

To delete a backup entry, select it in the list and click **Remove Backup**.

IMPORTANT: Windows mounts do not work when FIPS mode is enabled. MD5 authentication is required for CIFS (Windows), which is not supported in FIPS mode.

1. Select **Server Administration Settings** in the **System** 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 Data Center Expert server's configuration data, or its configuration and repository data.

The backup is delivered as a single file with a .dce file extension for easier filename filtering.

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 the 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.
Security	Specify the NT LAN Manager authentication level: NTLM, NTMLi, NTLMv2, NTLMv2i, NTLMSSP, or NTLMSSPi.
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 Data Center Expert 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 the 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.
Protocol	Select the transport protocol: UDP or TCP.
Version	Select the NFS version: v2.0, v3.0, v4.0, or v4.1.
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 Data Center Expert server's configuration data, or its configuration and repository data, will be backed up automatically.

Element	Description
Schedule Enabled	Select to have the Data Center Expert 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 Data Center Expert server configuration, or configuration and repository, data.

1. Select **Server Administration Settings** in the **System** 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 Data Center Expert 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 Data Center Expert 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 Data Center Expert 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 Data Center Expert 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 Data Center Expert 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 Data Center Expert 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 Data Center Expert server.

The backup is delivered as a single file with a .dce file extension for easier filename filtering.

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.
Security	Specify the NT LAN Manager authentication level: NTLM, NTMLi, NTLMv2, NTLMv2i, NTLMSSP, or NTLMSSPi.
Backup Type	Specify the backup type: Full, Syncronized, or Configuration.

"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 Data Center Expert server.

Element	Description
Server Hostname or IP	Identity the hostname or IP address of the NFS share server.
Share	Identify the 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.
Protocol	Select the transport protocol: UDP or TCP.
Version	Select the NFS version: v2.0, v3.0, v4.0, or v4.1.
Backup Type	Specify the backup type: Full, Syncronized, or Configuration.

Server Proxy Settings option

Use this option's elements to define the settings the Data Center Expert server must use to communicate through a proxy server.

Note: A Data Center Expert server needs to use the internet to communicate with APC to download firmware updates, for example.

Element	Description
Use Proxy	Select to enable the proxy settings.
Proxy Hostname/IP	Identify the hostname or IP address of the proxy server.
Port	Identify the port at the proxy server that the Data Center Expert 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 make sure the Data Center Expert server can access the identified proxy server using the proxy settings you define.
Do not use proxy server for the following addresses	Lists the internet addresses you want the Data Center Expert 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 Data Center Expert 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 Data Center Expert servers, and Windows or NFS repository servers for remote storage, each Data Center Expert server should use its repository server: multiple Data Center Expert servers should not store data on the same remote repository.

Repositories tab

Use this tab to manage the repositories the Data Center Expert 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**, **Status**, and **Condition** 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 allotted 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 Data Center Expert 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 Data Center Expert server, rather than the local repository.

Note: If your organization uses multiple Data Center Expert servers, and Windows or NFS repository servers for remote storage, each Data Center Expert server should use its repository server: multiple Data Center Expert servers should not store data on the same remote repository.

You can add, edit, or delete any remote repository, but not the local repository.

To delete a repository, select it in the **Repositories** tab, and click **Delete Repository**.

IMPORTANT: Windows mounts do not work when FIPS mode is enabled. MD5 authentication is required for CIFS (Windows), which is not supported in FIPS mode.

1. Select **Server Administration Settings** in the **System** 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 Data Center Expert 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 the 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.
Security	Specify the NT LAN Manager authentication level: NTLM, NTMLi, NTLMv2, NTLMv2i, NTLMSSP, or NTLMSSPi.
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.

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 Data Center Expert 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.

The backup is delivered as a single file with a .dce file extension for easier filename filtering.

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 the 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.
Protocol	Select the transport protocol: UDP or TCP.
Version	Select the NFS version: v2.0, v3.0, v4.0, or v4.1.

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 choose to include the repository data in the backup files created using **Server Backup/Restore**, a **Server Administration Settings** option in the **System** menu. The **Total Repository Usage** section identifies allotted 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 **Data Center Expert 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. Depending on how data is stored, the actual percentage may be below the configured value.
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 **Data Center Expert 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 Created 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 **Alarm History Data**, **Alarm 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 **Data Center Expert Administrators** that include an e-mail address as part of their user credentials.

Syslog Settings option

Configure settings to forward event log messages to an external Syslog server.

All the data in the event log messages are transmitted over Syslog, including usernames, email addresses, and information about share locations.

Note: Syslog functionality may differ depending on the Syslog server being used.

Element	Description
Enable Syslog integration	Check to forward event log messages to an external Syslog server.
Syslog server address	Specify the hostname or IP address of the Syslog server.
Port	Specify the port for the Syslog server, 514 by default.
Message format	Specify the message format for the Syslog server, RFC_3164 by default.
Facility	Specify the facility for the Syslog server, AUDIT by default.
Line terminator	When TCP is selected, specify a line terminator, \r\n by default.
Use SSL	Check to enable SSL.
Timeout	How long the server will wait to connect to the Syslog server using SSL, 5 seconds by default.
Maximum retries	The number of times the server will attempt to connect to the Syslog server using SSL, 2 by default.
Apply and Test	Click to to apply settings to your DCE server. Check the destination Syslog server to verify your configuration.

Time Settings option

Use this option's elements to define the date and time for the Data Center Expert server, or identify any NTP servers that will provide those date and time values, and specify regional settings.

Note: The Data Center Expert server must reboot before a change to any setting can take effect.

Date and Time elements

Element	Description
Enable Data Center Expert as NTP Server	Checkmark to select whether a Network Time Protocol (NTP) server you specify provides the date and time values for the Data Center Expert server; otherwise, these values are defined by the **Date** and **Time** elements or **Use Client Time**.
Use Remote NTP Server Time	When selected, a Network Time Protocol (NTP) server you specify provides the date and time values for the Data Center Expert server; otherwise, these values are defined by the **Date** and **Time** elements or **Use Client Time**.
Set NTP Time Manually	When selected, the NTP time is provided by the **Date** and **Time** elements or **Use Client Time**.
NTP Server 1 - 3	Identify the IP address or hostname of at least one NTP server, when **Use Remote NTP Server Time** is selected.
Date	Define the date the server will use, when **Enable Data Center Expert as NTP Server** is not selected, or when **Enable Data Center Expert as NTP Server** and **Set NTP Time Manually** are selected.
Time	Define the time the server will use, when **Enable Data Center Expert as NTP Server** is not selected, or when **Enable Data Center Expert as NTP Server** and **Set NTP Time Manually** are selected.
Use Client Time	Click to use your client time and date settings at the server, when **Enable Data Center Expert as NTP Server** is not selected, or when **Enable Data Center Expert as NTP Server** and **Set NTP Time Manually** are selected.
Calendar	Displays the current date, and can be used to define that date, when **Enable Data Center Expert as NTP Server** is not selected, or when **Enable Data Center Expert as NTP Server** and **Set NTP Time Manually** are selected.

Regional Settings elements

Element	Description
Server Locale	Select the language the Data Center Expert server will use for messages, such as e-mails. By default, the server uses the language associated with the **Server Time Zone** setting, or **English (U.S.)**, if the associated language is not supported. **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 Time on Server	Select to have the Data Center Expert server use a 24-hour clock.
Server Time Zone	Select the time zone in which the Data Center Expert server is located.

Client Preferences (File menu)

Use this option's display to define settings that apply to your Data Center Expert client only.

Audio Settings

Use this option to select whether your Data Center Expert 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 Provided Audio File	Select the sound you want your client to play from the drop-down list of files provided for the Data Center Expert client.
Select Custom Audio File	Browse to the AIFF, AU, WAV, or MIDI formatted audio file you want your client to play.
Test Sound	Click to hear the sound for the **Select Provided Audio File** or **Select Custom Audio File** selection.

Browser Settings

Use this option to select the web browser your Data Center Expert client will use to connect to the web interface at a monitored device.

Element	Description
Use the Default OS Web Browser	Select to use the operating system default web browser to open a browser window external to the **Data Center Expert** client (the default).
Use an Alternate Web Browser	Select to use an alternate web browser to open a browser window external to the **Data Center Expert** client.
Path	Identify the location of the alternate web browser executable file.
Browse	Click to browse to the executable file for the web browser you want to use, if necessary, to select its **Path**.
Test Browser	Click to verify that the selected browser can access the APC home page.
Use the Internal Web Browser when Launching to Devices	Check-mark to use the Data Center Expert client web browser to open a browser in a view inside

	the **Data Center Expert** client (the default selection). **Note:** Use this option, when you specify Device Launch Settings, to automatically log in to the web interface of devices that use basic authentication. See "Device Launch Settings" display under Monitored Devices.

Client Language Settings

Use this option to select the language you want your Data Center Expert client to use. The selected language will be used for all options, displays, status messages, thresholds, and settings, with the exception of messages, such as e-mails, sent by the Data Center Expert server, and identification information sent by monitored devices.

The default setting is **Use OS Locale**, which selects to use the language associated with your client's location, if that language is supported. Otherwise, English is the default **Use OS Locale** language.

Note: **Server Locale**, accessed by selecting **Time Settings**, a **Server Administration Settings** option in the **System** menu, allows you to select the language the Data Center Expert server uses for its messages.

Custom Property Settings

Use this option to select whether to show a popup option when a custom property is added, or to automatically add a column to the **Device View** for a newly created custom property.

Note: The default settings allow a popup option to appear, and columns to be added to the **Device View** and "View Device Sensors" display, for each new custom property key created.

When a custom property key is created using the **Manage Custom Property Keys** option in the **Device** menu, or the **Add Custom Property** option in the right-click menu of the **Custom Property Editor**, **Device View**, or **Map View**, a popup option appears, by default, to select whether to add the new custom property key to the **Device View** as a column. You can uncheck the **Show popup option when custom property key is added** option, check-marked by default, to disable the popup option.

Additionally, a new column can be added to the **Device View** when each new custom property key is created. You can uncheck the **Add a new column to the Device view for each new custom property key created** option, checkmarked by default, to prevent new columns from being created for every new custom property key.

To add, modify, or remove custom property keys, you use the **Manage Custom Property Keys** option in the **Device** menu.

To show columns for custom property keys in the **Device View**, you use the **Configure Column** icon in that view.

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, using the **Total Devices Shown** setting (**500**, by default), and to select to have devices with active **Critical**, **Error**, and **Failure** alarms highlighted in red, using the **Highlight Priority Alarms** setting.

Note: Only the **Device View** is affected by the **Total Devices Shown** and **Highlight Priority Alarms** settings.
The **Total Devices Shown** setting does not limit the number of devices the Data Center Expert 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**.

Monitored devices

The Data Center Expert server can monitor and manage APC, MGE, Modbus TCP, 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 Data Center Expert server can monitor APC, MGE, Modbus TCP, 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).
- Modbus TCP Output devices
- 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 Data Center Expert server can provide only **Type** (**SNMP Device** only), on-line or communication lost **Status**, **Hostname**, and **Groups** information.
Model ID SNMP support	The Data Center Expert server can report **Model** information, in addition to the information provided for basic SNMP support.
Full SNMP support	The Data Center Expert 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 OIDs**, an **SNMP Device Communication Settings** option in the **Device** menu.	

Device Definition File (DDF)

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

- DDF files, for third-party and Modbus devices, may be available from APC Technical support.

- You can use **Device Definition Files**, an **SNMP Device Communication Settings** and **Modbus Device Communications Settings** option in the **Device** menu, to check the APC website for new or updated DDFs, and download those files to the Data Center Expert server.
- APC SNMP devices that use a Network Management Card (NMC) version of 3xx or higher have a DDF file that the Data Center Expert must download at discovery time. This DDF file contains information about the alarm conditions the device can report.

Launch to device feature

The Data Center Expert server has the ability to launch to any discovered device that supports an HTTP/HTTPS web interface.

You can launch up to ten devices at once.

Access the device 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 Data Center Expert 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.

The **Always use the external browser** setting in the Device Launch Settings display overrides the internal browser setting configured in File > Client Preferences.

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 the Data Center Expert 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**.

The Data Center Expert server uses these settings to connect to the web interface at any monitored device (**Launch to Device**, a right-click option in the **Device View** and **Map view**).

You specify the username and password used to automatically log in to the web interfaces of APC SNMP devices with the following Network Management Card and firmware revisions:

- rPDU with Network Management Card firmware revision 3.7.1 and higher.
- APC SNMP devices with a Network Management Card (AP9617, AP9618, or AP9619) with firmware revision 3.7.0 and higher.
- APC SNMP devices with a Network Management Card (AP9630, AP9631, AP9635) with firmware revision 5.1.0 and higher.

Note: You cannot automatically login to the web interfaces of APC SNMP devices monitored by NetBotz Appliance versions 320, 420, and 500.

When **Use the Internal Web Browser when Launching to Devices** is selected in the **Client Preferences** option of the **File** menu, you can double-click the device, or select the right-click option **Launch to Device**, to automatically login to the web interface of devices that use basic authentication without being prompted for credentials.

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 used for browser communication at a selected device: **80** is the default for **HTTP**; **443** is the default for **HTTPS**.
Username	Identify the username used to login to the device.
Password	Identify the password used to login to the device.

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.

"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**.

Element	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 Data Center Expert 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 device labels, sensors, and sensor values, and custom property keys, if any.
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.

This " **View Device Sensors**" display also has right-click options to manage the list of sensors and sensor values.

Option	Description
Edit Custom Properties	Allows you to add a custom property, or modify the value of an existing property, for the selected sensors.

Delete Sensors	Allows you to remove a sensor with a sensor value of unplugged. This option is available for SNMP devices only. **Note:** When you delete a sensor, all historical data for that sensor is also deleted.
Change State To:	Allows you to change the state of sensors that report state values.

When a user has Device Group Monitoring View Access or higher, and accesses the " **View Device Sensors**" display from a camera, the display has a **Camera** tab.

Element	Description
Automatically fit to window	Checkmark to fit the image to the display.
Resolution	Select the resolution you want to use to display the real-time feed for the selected camera.

"Change Device Type" display

Use this display to select the appropriate device type for a third party device with no device type defined, or to more accurately define a monitored SNMP device, Modbus device, or NetBotz Appliance.

The selected device type and its associated icon will be displayed in **Map View** and the **Type** column in **Device View** in the **Monitoring** perspective, and the **Navigation** view in the **Alarm Configuration** perspective. You can select the 'Default' setting to change the icon and device type back to its original type.

Device Label Settings display

Define a custom label to display in the Device View's Label column for the selected SNMP or Modbus device. Otherwise, the default device label is displayed.

Element	Description
Use default device label	Checked by default. Clear the check mark to specify a custom device label.
Custom device label	Modify the label for the selected SNMP or Modbus device.

"Custom Label Settings" display

Use this display to define a custom identifier to display for the selected device or set of devices in a map. You must select one device at a time to also define a specific sensor value to display instead of the sensor value you set in Map Settings.

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

Element	Description
Show Identifier	Check-mark to select the identifier to show for the selected device or set of devices.
Display the value set in Map Settings	Select to make sure no changes are made to the sensor value label settings you set in the **Map Settings** option for the selected device.
Choose a specific sensor value	Select to choose a specific sensor value to show for the selected device. **Note:** You cannot configure the sensor value when multiple devices are selected.
List	Select the sensor you want to use from the available sensor list.

"Device Launch Settings" display

Use this display to define how the Data Center Expert 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**.

The Data Center Expert server uses these settings to connect to the web interface at any monitored device (**Launch to Device**, a right-click option in the **Device View** and **Map view**).

You specify the username and password used to automatically log in to the web interfaces of APC SNMP devices with the following Network Management Card and firmware revisions:

- rPDU with Network Management Card firmware revision 3.7.1 and higher.
- APC SNMP devices with a Network Management Card (AP9617, AP9618, or AP9619) with firmware revision 3.7.0 and higher.
- APC SNMP devices with a Network Management Card (AP9630, AP9631, AP9635) with firmware revision 5.1.0 and higher.

Note: You cannot automatically login to the web interfaces of APC SNMP devices monitored by NetBotz Appliance versions 320, 420, and 500.

When **Use the Internal Web Browser when Launching to Devices** is selected in the **Client Preferences** option of the **File** menu, you can double-click the device, or select the right-click option **Launch to Device**, to automatically login to the web interface of devices that use basic authentication without being prompted for credentials.

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

	default for **HTTP**; **443** is selected by default for **HTTPS**.
Username	Identify the username used to login to the device.
Password	Identify the password used to login to the device.

"Outlet Control" display

Use this display to control the outlets on supported APC Rack PDU devices.

You must specify the write community name for the Rack PDU device at device discovery, or in the "Edit Device Scan Settings" display, accessed from the **Device Scan Settings** option of the **SNMP Device Communication Settings** option in the **Device** menu.

You can configure delay parameters for the outlets via SNMP or by logging into the device.

A "Communication Error" is displayed when the Rack PDU device does not respond to a command for any reason, for example, when the write community name identified in the "Device Scan Settings" display is incorrect.

User permissions defined in the "Modify Device Group Access" display, accessed from the **Users and User Groups** option in the **System** menu, determine which users have access to outlet control. Data Center Expert Server Administrators, Device Administrators, and Device Viewer users with monitoring access set for **Administration Access** or **View and Control** can access outlet control.

CAUTION: When you perform a command at an outlet that is part of an outlet group, that command will be executed at all outlets in the group. The Data Center Expert server cannot determine which outlets are part of an outlet group.

Element	Description
List	**Name**: Select one or more outlets to control. **Status**: The status of the outlet.
Command	Select the command you wish to perform at the selected outlets. **Note:** Only the commands supported by the selected device are listed.
Refresh Status	Click to update the status of the outlets.
Perform Command	Click to perform the command at the outlets selected.

"Rack Access Control" display

Use this option's configuration display to control locks on rack doors monitored by the selected NetBotz Rack Access PX-HID, or Rack Access Pod 170 devices associated with the selected NetBotz Appliance.

Note: You must select one NetBotz Rack Access Device or NetBotz Appliance at a time to configure Rack Access Control.

IMPORTANT: The Select all option in Rack Access > Control unlocks only one door on NetBotz 250 and 750 appliances. The NetBotz 250 and 750 do not allow both doors to be unlocked at the same time.

Element	Description
List	Checkmark to select one or more locks, one or more associated Rack Access Pod 170 devices, or the NetBotz Appliance or NetBotz Rack Access Device.
Door State	The current state of the door, **Open**, or **Closed**
Handle State	The current state of the door handle, **Up**, or **Down**
Lock State	The current state of the lock, **Locked**, or **Unlocked**
Lock/Unlock	Press to lock or unlock the selected doors.

Note: The state of the door, handle, or lock is **Unplugged** when the Rack Access Pod 170 has been removed from the NetBotz Appliance.

You can right-click a NetBotz Rack Access Device, NetBotz Appliance, or Rack Access Pod 170 to expand or collapse the list of door locks (**Expand** or **Collapse** option).

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**.

Note: **Device View Settings**, a **Client Preferences** option in the **File** menu, has a **Total Devices Shown** setting that defines the maximum number of devices that can be listed in the **Device View** at any one time (**500**, by default), and a **Highlight Priority Alarms** setting that selects to have devices with active **Critical**, **Error**, and **Failure** alarms highlighted in red in the **Device View** (disabled, by default).
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 **Configure Columns** 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 the information in that column.
  - 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, or use the right-click **Launch to Device** option for a device.
    Note: By default, the web interface of devices requiring basic authentication is displayed as a view using the internal web browser. You can use the **Launch**

in External Browser icon in that view to log on to the web interface in an external browser.

- 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, Modbus devices, or NetBotz Appliances to be monitored by the Data Center Expert server (**Add Devices** option or the green + icon).
  - Delete devices that you no longer want the Data Center Expert server to monitor (**Delete Devices** option or the x icon).
    Note: This option is disabled for a device that has a NetBotz Appliance as its parent device.
  - Generate a report or graph for the historical values of the sensors at selected devices (**Generate Sensor History Report** option or **Generate Custom Sensor History Report** 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, and the username and password to be used by the Data Center Expert server to communicate with monitored devices (**Device Launch Settings** option).
    Note: For monitored APC SNMP and Modbus devices, the default username and password "apc" is provided by default.
  - Control the outlets at a selected APC devices (**Outlet Control** 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 Data Center Expert server to stop monitoring those devices (**Remove Device from Group** option).
  - Request that the Data Center Expert server immediately scan selected devices for sensor values, without waiting until the server would normally scan those devices (**Request Device Scan** option).
    Note: This option is unavailable for NetBotz Appliances, and devices that have a NetBotz Appliance as their parent device.
  - View all the values being reported by the sensors at selected devices (**View Device Sensors** option).
  - Select the appropriate device type for a third party device, or more accurately define an SNMP device (**Change Device Type** option).
  - Configure the device to use its default label or specify a custom label (**Device Label Settings** option).
  - Create thresholds for a selected device, or set of devices (**Create Thresholds** option).
    Note: For information about this option, see **Create Thresholds** option, under **Alarm Configuration**.
  - Configure selected APC SNMP devices to use the same values for shared settings (**APC SNMP Device Configuration** option).
    Note: An **APC SNMP Device Configuration** option is also in the **Device** menu. For information about these options, see **APC SNMP Device Configuration**.
  - Access an option to lock or unlock rack doors using the **Rack Access Control** option for a main NetBotz Appliance, or any of its associated Rack Access Pod 170 devices.
    Note: The **Rack Access Control** option is available only when a Rack Access Pod 170 is connected to the selected NetBotz Appliance.
  - Access a specific configuration option for a selected NetBotz Appliance or camera pod (**NetBotz Appliance Configuration** options).
    Note: A **NetBotz Appliance Configuration** option is also in the **Device** menu. For information about these options, see **NetBotz Appliance Configuration**.

- 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.
- Disable or re-enable notifications for any SNMP or Modbus device, or device group (**Enter/Exit Maintenance Mode** options).
- Create a custom property, or edit the value of an existing property, for the selected devices or sensors (**Add Custom Property** option).
- Access the **Custom Properties Editor** view to add, modify, or remove custom properties for selected devices or sensors (**Open Custom Properties Editor** option).
- Create a virtual sensor for a selected device, or set of devices (**Create Virtual Sensor** option).
  Note: For information about this option, see Virtual Sensors 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 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 right-click a main NetBotz Appliance entry, or any of its Rack Access 170 devices, to lock or unlock rack doors using the **Rack Access Control** option.
  Note: The **Rack Access Control** option is available only when a Rack Access Pod 170 is connected to the selected NetBotz Appliance.
- 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 **Configure Columns** 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 the severity settings for each threshold. For example, a door sensor can be set to report **Informational** status for an open door.
Model	The device model, if known. For example, **Silcon DP310E** for an APC 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 Data Center Expert 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.
Label	The label defined for a device.
Maintenance Mode	Indicates a device is in Maintenance Mode, and alarm notifications for that device have been disabled (**Yes**), or not in Maintenance Mode, and alarm notifications are enabled (**No**), the default.
Groups	The names of any device groups a device belongs to, including **All Devices** and **Unassigned**.
MAC Address	The unique network interface identifier for the device.
Contact Name	The name of the contact associated with the device.

Button icons (Device View)

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

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

Icon	Description
	Use this Export Device List icon to save a copy of the device list as a *.csv (the default selection) or *.txt file.
	Use this **Add Devices** icon to initiate a device discovery process used to add SNMP devices, Modbus devices, or NetBotz Appliances to be monitored by the Data Center Expert server.
	Use this **Delete Devices** icon to delete devices that you no longer want the Data Center Expert server to monitor.
	Use this **Custom Sensor History Reports** icon to create a report or graph for the historical values of the sensors at selected devices (see Reports feature).
	Use this **Configure Columns** icon to identify the columns to be included in the device list.

Map View features

The Map view presents devices as icons on a customizable graphic background. Devices and sensors are automatically placed on maps by default. You can change this in the System > Server Administration Settings > Map Settings option.

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 Devices, Groups, or Sensors in Map** icon, or right-click option, to search and select device groups and sensors by label, or devices by IP address, location, hostname, model name or device label.
    Note: Boolean operators are not supported.
    Note: You can search and select device groups, devices, or sensors regardless of whether the identifier is shown on the map. For more information about identifiers and other icon settings, see **Map Settings** .
- 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 (**Auto-Arrange** 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 define how icons are displayed (**Map Settings** option or icon).
  - Select sensor values to be displayed by the icons (**Custom Label Settings** option or icon).
  - Select the appropriate device type for a third party device, or more accurately define an SNMP device (**Change Device Type** option).
- 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 Data Center Expert server to monitor (**Delete Devices** option).
    Note: This option is disabled for a device that has a NetBotz Appliance as its parent device.

- Initiate the process used to create a report or graph for the historical values of the sensors at selected devices (**Generate Sensor History Report** option 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 Data Center Expert server to communicate with monitored devices (**Device Launch Settings** option).
  Note: For monitored APC SNMP and Modbus devices, the default username and password "apc" is provided by default.
- Control the outlets at a selected APC device (**Outlet Control** option).
- Log on to the web interface at a selected device, if it has one (**Launch to Device** option).
- Request that the Data Center Expert server immediately scan selected devices for sensor values, without waiting until the server would normally scan those devices (**Request Device Scan** option).
  Note: This option is unavailable for NetBotz Appliances, and devices that have a NetBotz Appliance as their parent device.
- View all the values being reported by the sensors at selected devices (**View Device Sensors** option).
- Create a custom property, or edit the value of an existing property, for the selected devices or sensors (**Add Custom Property** option).
- Access the **Custom Properties Editor** view to add, modify, or remove custom properties for selected devices or sensors (**Open Custom Properties Editor** option).
- Configure selected APC SNMP devices to use the same values for shared settings (**APC SNMP Device Configuration** option).
  Note: An **APC SNMP Device Configuration** option is also in the **Device** menu. For information about these options, see **APC SNMP Device Configuration**.
- Create thresholds for a selected SNMP or Modbus device, or set of devices (**Create Thresholds** options).
  Note: For information about these options, see **Create Thresholds** , under **Alarm Configuration** menu.
- Disable or re-enable notifications for any SNMP or Modbus device, or device group (**Enter/Exit Maintenance Mode** options).
- Access an option to lock or unlock rack doors using the **Rack Access Control** option for a main NetBotz Appliance, or any of its associated Rack Access Pod 170 devices.
  Note: The **Rack Access Control** option is available only when a Rack Access Pod 170 is connected to the selected NetBotz Appliance.
- Access a specific configuration option for a selected NetBotz Appliance or camera pod (**NetBotz Appliance Configuration** options).
  Note: For information about these options, see **NetBotz Appliance Configuration** under **Device** menu.
- Add or edit alert thresholds for a selected NetBotz Appliance or devices that have a NetBotz Appliance as their parent device (**Alert Thresholds** options under **NetBotz Appliance Configuration**).
  Note: For information about these options, see **Alert Thresholds** options, under **Alert Settings** in the **NetBotz Appliance Configuration** option of the **Device** menu.
- Edit camera settings for a selected NetBotz Appliance or cameras that have a NetBotz Appliance as their parent device (**Camera Settings** option under **NetBotz Appliance Configuration**).
- Create a virtual sensor for a selected device, or set of devices (**Create Virtual Sensor** option).
  Note: For information about this option, see Virtual Sensors view.

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/Exit Edit Map** icon to reposition devices within the map, and save the new positions.
	Use this **Find Devices, Groups, or Sensors in Map** icon to search and select device groups and sensors by label, or devices by IP address, location, hostname, model name or device label. **Note:** Boolean operators are not supported.
	Use this **Map Settings** icon to define the background, as well as how icons are displayed.
	Use this **Auto-Arrange** icon to reset the device icons back to their default positions.
	Use this **Custom Label Settings** icon to select the identifier and sensor values to be displayed for the **Map View** devices.

Creating a customized background

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

1. Access the " Map Settings" display by selecting the right-click **Map Settings** option, or clicking the **Map Settings** icon, in the **Map View**:
2. In the " **Map Settings** " display **Map Background** section, select **Custom Background** .
3. Click **Select Image**, 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. Repeat steps 1 through 3 for the **Map Views** of the other device groups.

Customizing the device icons

Use the " Map Settings" display 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 Settings** option, or clicking the **Map Settings** icon, in the **Map View**.
2. In the " Map Settings" display, select the **Map 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.
   - When identifiers 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 " Map Label Settings" display to select an identifier to display for all devices and sensors in a **Map View**, and to select a sensor value to display on all devices on the map that report the sensor. Use the " **Custom Label Settings** " display to select a custom identifier or sensor value to be displayed for a specific device in a map.

Selecting Map Label Settings for all devices in a map

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

1. Select the **Map Settings** right-click option, or the **Map Settings** icon at the top of the **Map View**. Select the Map Label Settings option.
2. Check-mark the **Show Identifier** option, and select an identifier from the list.
3. Make sure the **Show Value** option is check-marked.
4. Select the sensor you want to use from the available sensor list.

Selecting Custom Label Settings for a selected device or set of devices

You can select a device or set of devices in a **Map View**, and select an identifier to display instead of the identifier set in the **Map Settings** display. You must select one device at a time to also define a custom value to display for a specific sensor.

1. Select the device or set of devices in the **Map View**.
2. Select the **Custom Label Settings** right-click option, or the **Custom Label Settings** icon at the top of the **Map View**.
3. Check-mark the **Show Identifier** option, and select the identifier you want the device or set of devices to display.
4. When one device is selected, define the sensor value you want the device to display, by choosing one of the following options:
   - Select **Display the value set in** **Map Settings** if you want the selected device to use the settings defined in the Map Settings display.
   - Select **Choose a specific sensor value**, and select the sensor you want to use from the available sensor list, if you want the selected device to use a custom setting.

"Add to Map" display

Use this display to select the device groups, devices, and sensors to add to a map.

You access this display from the right-click menu in a map, after **Edit Map** is selected. You use three tabs, **Sensors**, **Devices**, and **Device Groups**, to select the sensors, devices, or device groups you want to add to the map.

You can use the **Search** field to filter the list on each tab based on the text you type.

Note: Only the Boolean operators AND, OR, and NOT are supported.

You can select the **Configure Columns** icon on the **Sensors** and **Devices** tabs to identify the columns that appear in the display. You can click the column headers to sort the list in ascending or descending order.

The **Unassigned** group is automatically added to the map for the **All Devices** group. Any device group you create, and any device you add to a device group, is automatically added to the map for the selected device group. Sensors must be added to a map manually.

When all the device groups, devices, or sensors available for the selection are already added to the map, the list on the **Sensors**, **Devices**, or **Device Group** tabs is empty. When a device group, device, or sensor has not been added to the map, or has been removed from the map, it is listed on the appropriate tab, and can be added to the map at a later time.

Element	Description
Sensors tab	Displays all available sensors, for every device in every device group, not already on the map. **Note:** Sensors are not added to a map by default. They must be added manually from this display.
Devices tab	Displays the devices, in every device group, not already on the map. **Note:** When the device group you select contains only devices, the list in the **Devices** tab is at first empty. Devices are added to the map by default.
Device Groups tab	Displays no device groups until one or more device groups are removed from the map. **Note:** When the device group you select contains only device groups, the list in the **Device Groups** tab is at first empty. Device groups are added to the map by default.

"Map Settings" display

Use this display to access Map Settings options used to define how the background and icons will appear in a **Map View** for a device group.

Map Settings option

Use this option to customize how the background and icons will look in a **Map View**.

Element	Description
Custom Background	Click to select a graphic to use as a custom background.
Select Image	Click to browse to and select the graphic you want to use for the custom background.
Save	Click to save the selected background image as a file at your local machine.
No Background	Click to use a blank background.
Grid Background (Default)	Click to use a blank-tiled background, the default.
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.
Identifier Orientation	Choose how to show the identifier you selected in **Map Label Settings** or **Custom Label Settings**, if any. **Horizontal** will show the identifier below the icon, horizontally, and **Vertical** will show the identifier to the right of the icon, vertically.
Icon Preview	Shows the affect of applied **Sizing** and **Identifier** definition on how icons will appear in a **Map View**. **Note:** Sensor values are always shown below the icon, horizontally, and are not shown in the Icon Preview.

Map Label Settings option

Use this option to define the identifier and sensor value labels to display for all devices and sensors on a map.

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

Element	Description
Show Identifier	Check-mark to select the identifier to show for all devices and sensors on a map.
Show Value	Check-mark to show the value of the selected sensor for all devices on the map that report that sensor.
List	Select the sensor for which you want to show the value.

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

All the sensors for every device in the selected device group's **Map View** are listed. 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 sensor, only devices that have that exact sensor will report the value.

Devices that report the selected sensor will update with the sensor value except for the following:

- Devices that do not report the sensor value.
- Devices that have a different sensor defined in the **Custom Label Settings** display. **Note:** You can also use the **Custom Label Settings** display to select a new sensor value label for one device on a map without affecting the sensor value labels at any other devices.

Virtual Sensors view

This view allows users with Device Administrator or Server Administrator access to view, create, modify, and delete virtual sensors for the Data Center Expert server. A virtual sensor allows you to view and monitor the average or total value of multiple numeric sensors of the same sensor type.

A virtual sensor can include numeric sensors for any device in any device group monitored by the Data Center Expert server, including other virtual sensors.

A virtual sensor starts recording historical data when it is created. The value of the virtual sensor is calculated and updated only when all the devices monitoring the included sensors have been scanned. The value of the virtual sensor is a single value data point, representing the weighted average or weighted total of all the historical sensor data collected since the last calculation.

Only Device Administrators and Server Administrators can create virtual sensors.

To create a virtual sensor, you select whether you want it to report the average value or the total value for the sensors you want to include. You then select a combination of sensor type, device groups, and devices to filter the list of available sensors. Only device groups and devices containing sensors of the selected sensor type are shown.
Note: You can select the sensor type **Other Numeric** only when all sensors for the selection use the same unit of measure. You cannot create a virtual sensor for state sensors.

After you select the sensors you want to include in the virtual sensor, you identify a name for the virtual sensor, and specify the device group in which you want to create its virtual device parent.

For each virtual sensor created, a virtual device parent is also created and added to the **Device View** and the **Map View**. You can right-click the **Virtual Device** parent, and select **View Device Sensors** to view the virtual sensor. You can view all the virtual sensors monitored by the Data Center Expert server in the Virtual Sensors view.
Note: You cannot create a virtual sensor directly from sensors you manually added to the **Map View**.

Both physical and virtual devices are included in the device count in the **Device View**, and the status bar at the bottom of the display. Virtual devices are not included in the **Used Node Count** in the "License" display, accessed from the **Server Administration Settings** option in the **System** menu.

Right-click options, and button icons at the top of the view, perform the following functions:

- Create a virtual sensor in the specified device group (**Create Virtual Sensor** option or icon).
- Modify the name of the virtual sensor, and add or delete sensors included for the selected virtual sensor (**Edit Virtual Sensor** option or icon).
- Remove the selected virtual sensor from the Data Center Expert server (**Delete Virtual Sensor** option or icon).
- Generate a report or graph for the historical values of the selected virtual sensor (**Generate Sensor History Report** option or icon).
- Create thresholds for the selected virtual sensor (**Create Threshold** option).
  Note: For information about this option, see **Create Thresholds** option, under **Alarm Configuration**.
- Identify the selected virtual sensor in the **Device View** or **Map View** (**Select Virtual Device** option).

Four menus provide access to create a virtual sensor:

- Right-click menu **Create Virtual Sensor** in the **Device Groups** view of the **Monitoring** perspective.
- Right-click menu **Create Virtual Sensor** in the **Device View** of the **Monitoring** perspective.
- Right-click menu **Create Virtual Sensor** in the **Map View** of the **Monitoring** perspective.
- **Create Virtual Sensor**, an option in the **Device** menu.

Creating a virtual sensor

1. Access the **Create Virtual Sensor** option:
   - Right-click one or more devices in the **Device View** or **Map View**.
   - Right-click a device group in the **Device Groups** view.
   - Select **Create Virtual Sensor** from the **Device** menu.
   - Select the **Add** icon in the **Virtual Sensors** view.
2. Select whether you want the virtual sensor to report the **Average** value or the **Total** value of the sensors to be included.
3. Select the sensor type for the virtual sensor.

   You can select the sensor type **Other Numeric** only when all sensors for the selection use the same unit of measure. You cannot create a virtual sensor for state sensors.
4. Select the device groups containing the sensors you want to include in the virtual sensor. This option is available when you select **Create Virtual Sensor** from the **Device** menu, or from the **Add** icon in the **Virtual Sensors** view.

   Only device groups containing sensors of the selected sensor type are shown.
5. Select the devices containing the sensors you want to include in the virtual sensor.

   Only devices containing sensors of the selected sensor type are shown.
6. Select the sensors you want to include in the virtual sensor.

   Only sensors of the selected sensor type are shown.
7. Identify a name for the virtual sensor.

   This virtual sensor name appears in the **Label** column for both the virtual device parent and virtual sensor.
8. Specify the device group in which you want to create the Virtual Device parent for the virtual sensor.
9. Click **Finish** to create the Virtual Device parent and the virtual sensor.

   The Virtual Device parent is added to the **Device View** and the **Map View**, with an unaddressable IP Address. You access the virtual sensor from the right-click menu, **View Device Sensors**, or from the **Virtual Sensors** view.

   The Virtual Device is added to the device count only. It is not added to the Used Node Count for the node license.

"Choose Device Groups" display

Use this display to choose the device groups containing the sensors you want to add to the virtual sensor. Only device groups containing the selected sensor type are shown.

"Choose Devices" display

Use this display to choose the devices that monitor the sensors you want to add to the virtual sensor. Only devices monitoring the selected sensor type are shown.

A **Search** field and **Clear** button allow you to filter the list to display only the device groups that include your typed text.

A **Configure Columns** icon allows you to define which columns are displayed.

Column	Description
Type	The type of device.
Hostname	The hostname, or IP address, if no hostname is defined, for a monitored device or NetBotz Appliance, or <not addressable> for a virtual device.
Label	The label defined for a device.
Location	The location associated with a device, if known.
Model	The device model, if known.
Parent Device	Identifies the Data Center Expert server, for devices directly monitored by the server, or the hostname or IP address for a NetBotz Appliance and its supported devices.
Device Groups	The names of any device groups a device belongs to, including **All Devices** and **Unassigned**.
<Custom Property Key Name>	A custom property key, identified by name.

"Choose Sensors" display

Use this display to choose the sensors to add to the virtual sensor. Only sensors of the selected sensor type are shown.

A **Search** field and **Clear** button allow you to filter the list to display only the sensors that include your typed text.

A **Configure Columns** icon allows you to define which columns are displayed.

Column	Description
Sensor	The name of the sensor.
Current Reading	The last reported value for the sensor.
Hostname	The hostname, or IP address, if no hostname is defined, for the device or NetBotz Appliance monitoring the sensor, or <not addressable> for a virtual device.
Unit of Measure	The unit of measurement for the sensor.
Device Type	The type for the device monitoring the sensor.
Device Model	The model for the device monitoring the sensor.

Device Label	The label defined for the device monitoring the sensor.
Parent Device	Identifies the Data Center Expert server, for devices directly monitored by the server, or the hostname or IP address for a NetBotz Appliance and its supported devices.
<Custom Property Key Name>	A custom property key, identified by name.

"Destination Device Group" display

Use this display to choose the device group in which to create the virtual device parent for the virtual sensor. The **Virtual Device** parent cannot be created in the **All Devices** group.

For each virtual sensor created, a virtual device parent is also created and added to the **Device View** and the **Map View**.

"Virtual Sensor Name" display

Use this display to specify a name for the virtual sensor.

This virtual sensor name appears in the **Label** column for both the virtual device parent and virtual sensor.

"Edit Virtual Sensor" display

Use this display to modify the selected virtual sensor.

Note: You cannot edit a virtual sensor until all sensors included in the virtual sensor are loaded.

A **Name** field allows you to modify the name of the selected virtual sensor.

A **Search** field and **Clear** button allow you to filter the list to display only the sensors that include your typed text.

You can click the **Configure Columns** icon to define which columns appear in the list. The columns provide information for listed sensors.

Element	Description
List	Provides information about each virtual sensor in the view.
Add Sensors	Click to add a sensor to the selected virtual sensor.
Remove Sensors	Click to remove a sensor from the selected virtual sensor. **Note:** You cannot remove all sensors from a virtual sensor.

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 default layout of the **Monitoring** perspective; **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 a threshold related to an alarm has been defined at the Data Center Expert server.

- 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 alarm threshold has been defined at the Data Center Expert server for a sensor at a monitored device, two alarms may be listed in an alarms view for the same sensor event:
  - An alarm sent to the Data Center Expert server by a monitored device.
  - An alarm generated by the Data Center Expert server when the data it monitors for that device sensor violates the alarm threshold setting defined at the server for that sensor.
    Note: Not all SNMP devices can send alarms to the Data Center Expert server. Also, the thresholds at SNMP devices are independent from the alarm threshold settings at the Data Center Expert server.

"View Alarm Details and Comments" display

Use this display, accessed by a **View Alarm Details and Comments** right-click option in the **Active Alarms** view and **Alarm History** view, to view **Details** for any active or historical alarm, as well as **Comments**, **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 unavailable 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 each frame, 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**

Comments option

Use this option to view, add, or remove comments about the selected alarm.

You can add up to 25 comments for the selected alarm. The date and time the alarm occurred, and the username, date and time for each comment are displayed. You can click the **X** icon next to each comment to permanently remove it from the list.

Events generated by the Data Center Expert server are italicized in blue. The date and time the alarm occurred, and the name of the user that acknowledged the alarm, if applicable, are displayed. System events cannot be removed from the list.

Data Center Expert Server Administrator users can add and remove comments for any alarm.

Device Administrator users can add comments for alarms at devices in the device groups to which they have access, and can remove only their own comments.

Device Viewer users can view comments for alarms at devices in the device groups to which they have access.
Note: For a non- Data Center Expert Administrator user, including a user for which no role is selected, access privileges are determined by **Device Group Access** settings in the **Users** tab for that user, and for the user groups to which the user is assigned.

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.
Alarm Name	The name of the alarm.
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.
Custom URL	The **Custom URL** in the **Advanced** tab for the alert threshold setting associated with the alarming sensor, when defined for that threshold. **Note:** For more information, see **Alert Thresholds** under **Alert Settings** (**Device** menu).
Custom Description	The **Custom Description** in the **Advanced** tab for the alert threshold setting associated with the alarming sensor, when defined for that threshold. **Note:** For more information, see **Alert Thresholds** under **Alert Settings** (**Device** 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.

Graph option

Use this option to view a graph for an alarm associated with a sensor.

Note: This is available only for some of the alarms that list a sensor in the **Sensor** column of an alarms list; it is unavailable 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.

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.

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 **Configure Columns** icon to identify the columns that appear in the active alarms list. All available columns are displayed by default.
	Use the **Show Hidden Alarms** icon to view acknowledged alarms set as hidden, or to hide affected alarms once you have viewed them.
	Use the **Generate Custom Sensor History 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 Reports feature).

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.
Comments	The number of comments on the alarm.
Severity	Describes the severity level associated with the alarm.
Device Hostname	Identifies the hostname or IP address of the device.
Alarm Type	Identifies the type of alarm.
Location	Identifies the location of the device, when available.
Device Label	The default or custom label for the device.
Parent Device	Identifies the IP address or hostname for a NetBotz Appliance, or **<server_name> (Data Center Expert)** , for SNMP devices monitored by the Data Center Expert server.
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 alarm. **Note:** For information about the alert threshold settings, see Alert Thresholds, under Alert Settings.
Notifications Suppressed	Indicates whether notifications for the alarm were suppressed when the alarm was acknowledged.

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

- Show or hide the Alarm Details section (**Show/Hide Alarms Details** icon).
- Select which columns appear in the list (**Configure Columns** icon).
- Click a column title to sort the list in ascending or descending order based on the information in that column.
- Access the "Alarm Details" display for a selected alarm (**View Alarm Details and Comments** 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 the device associated with the selected alarm (**Custom Sensor History Report** icon).
  Note: All device sensors associated with the device will be listed, with the sensor for that alarm selected in that list.
- View all the values being reported by the device associated with the selected alarm (**View Device Sensors** option).
- Log on to the web interface of the device associated with the selected alarm, if it has one (**Launch to Device** option).
- Specify how you want to acknowledge selected alarms (**Alarm Acknowledgement** option).

- View acknowledged alarms set as hidden, or hide affected alarms once you have viewed them (**Show Hidden Alarms** icon).
- Show the selected threshold or device alarm in the **Threshold Alarm Configurations** view or the **Device Alarm Configurations** view in the **Alarm Configuration** perspective (**Find Alarm Configuration** option).
  Note: This option is not available for active alarms on NetBotz Appliances.
- Modify the settings for only the selected instance of a threshold or device alarm, or all instances of that threshold or device alarm on every device that reports it (**Edit Alarm Configuration** option).
  Note: This option is not available for active alarms on NetBotz Appliances.

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 details for the selected alarm, details that may include a graph and camera clips.

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

Note: This section reports the information available to the Data Center Expert 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.
Alarm Name	The name of the alarm.
Device	The label information for the device.
Device Location	The location of the device, when available.
Time Occurred	The time the alarm was reported.
Time Resolved	The time the alarm was resolved, or Not Yet Resolved when the alarm is still active.
Custom URL	A custom URL included in alarm notifications.
Custom Description	A custom description included in alarm notifications.
Recommended Action	Information about how to clear the alarm, when available.

"Alarm Acknowledgement" display

Use this display to specify how you want to acknowledge selected active alarms at SNMP and Modbus devices.

Type	Description

Set as Hidden	Checkmark to hide the alarm in the **Active Alarms** view of any **Data Center Expert** client logged in to the **Data Center Expert** server. **Note:** You can click the **Show Hidden Alarms** icon to view acknowledged alarms set as hidden. The information for affected alarms is italicized. You can then select any italicized alarms and uncheck the **Set as Hidden** option to display them in the view.
Suppress Future Data Center Expert Notifications	Checkmark to prevent notifications from being sent for the alarm, when the alarm actions specified in the notification policy are set to repeat. **Note:** When the alarm is resolved, Return to Normal events are sent using the alarm actions specified in the notification policy.
Add Comment	Enter additional information about acknowledging the alarm.

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 title of the view 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 text you type, 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 the 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**.
Description	Describes details for the alarm.
Comments	The number of comments on the alarm.
Clip	Uses a camera icon to identify alarms that include a surveillance clip.
Severity	Identifies the severity level associated with the alarm.
Device Hostname	Identifies the hostname or IP address of the device associated with the alarm.
Alarm Type	The type of alarm.
Location	The location of the device, when known.
Device Label	The default or custom label for the device.
Parent Device	Identifies the IP address or hostname for a NetBotz Appliance, or **<server_name> (Data Center Expert)** , for SNMP devices monitored by the Data Center Expert server.
Sensor	Identifies the sensor associated with the alarm, when an alert threshold setting is defined for the sensor 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 the information in that column.
- Select which columns appear in the list (**Configure Columns** icon).
- 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 the device associated with the selected alarm (**Generate Custom Sensor History Report** right-click option or ( ) icon).
  Note: All device sensors associated with the device will be listed, with the sensor for that alarm selected in that list.
- View all the values being reported by the sensors at the device associated with the selected alarm (**View Device Sensors** right-click option).
- Show the selected threshold or device alarm in the **Threshold Alarm Configurations** view or the **Device Alarm Configurations** view in the **Alarm Configuration** perspective (**Find Alarm Configuration** option).
- Modify the settings for only the selected instance of a threshold or device alarm, or all instances of that threshold or device alarm on every device that reports it (**Edit Alarm Configuration** option).
- Log on to the web interface of the device associated with the selected alarm, 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.

"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 the **Advanced** tab.

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 **Create Thresholds** under **Alarm Configuration**.

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

Device discovery processes

APC, MGE, NetBotz Appliances, and third-party devices are added to the list of devices the Data Center Expert 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, and added to the navigation tree in the **Thresholds** view. Additionally, you can place SNMPv1 devices, Modbus devices, and NetBotz Appliances into a device group you select, the **Unassigned** device group by default, during the discovery process.

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 250, 750, 300, 303, 310, 400, and 410 models).
- Modbus TCP

For information about discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

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

- Select **Add Devices** in the **Device** 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.

In DCE 8.2.0 and newer, the **Run discovery now** option is checked by default.

Creating a discovery process

You can create discovery processes that can discover the SNMPv1 devices, SNMPv3 devices, NetBotz Appliances, or Modbus devices on your networks. To discover NetBotz 250 and 750 series Appliances, choose SNMPv1 or SNMPv3.

1. Access the "Device Discovery" wizard.
   - Select **Add Devices** in the **Device** 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 (includes 200 and 750 series NetBotz Appliances)**
   - **SNMPv3 (includes 200 and 750 series NetBotz Appliances)**
   - **NetBotz Appliance (includes 300-500 series NetBotz Appliances)**

For information about discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

3. In the "Choose Device Group" display, select the device group where you want to place the discovered devices, and click **Next**.
4. 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.

   Modbus TCP device discovery occurs immediately after you click **Finish**, and will not appear in the **Saved Discoveries** view.

   - "SNMPv1 Discovery Settings" display:
     1. **IP Range**: the IP addresses the discovery process will search.
     2. **Read Community Name**: the community name used to read information at the SNMPv1 devices.
     3. **Write Community Name**: the community name used to control an APC SNMP v1 device or register as a trap receiver at an APC SNMPv1 device.
     4. **Port**: the port number that the SNMPv1 devices use for communication.
     5. **Timeout**: how long the Data Center Expert server will wait for a response, in seconds, when it polls an IP address before it considers the poll failed.
     6. **Retries**: how many times the Data Center Expert 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.
     7. **Register for Priority Scanning**: enables the Data Center Expert server to be defined as a trap receiver at discovered APC SNMPv1 devices.
        Note: Priority Scanning is a trap-based polling process that only occurs in response to traps from APC SNMPv1 devices or informs from APC SNMPv3 devices at which the Data Center Expert server is defined as a trap receiver. It allows the Data Center Expert server to immediately poll an APC SNMP device in response to a trap, rather than waiting to poll the device during the normal scanning interval.
     8. **Device File Transfer Settings**: accesses the "Device File Transfer Settings" display used to edit, create, or view the file transfer settings for FTP or SCP access to SNMP devices. For NetBotz 750, you must add the credentials for the root user (not superuser).
   - "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 Data Center Expert 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 Data Center Expert 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 Data Center Expert server to be defined as a trap receiver at discovered APC SNMPv3 devices.
        Note: Priority Scanning is a trap-based polling process that only occurs in response to traps from APC SNMPv1 devices or informs from APC SNMPv3 devices at which the Data Center Expert server is defined as a trap receiver. It allows the Data Center Expert server to immediately poll an APC SNMP device in response to a trap, rather than waiting to poll the device during the normal scanning interval.

9. **Device File Transfer Settings**: accesses the "Device File Transfer Settings" display used to edit, create, or view the file transfer settings for FTP or SCP access to SNMP 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.
- "Modbus Discovery Settings" display:
  1. **Single IP Address**: one IP address the discovery process will search.
  2. **Select Device Type**: lists the Modbus device types the Data Center Expert server supports.
  3. **Server Address**: identifies the server address of the Modbus device.
  4. **Port**: the port number the Modbus device uses for communication.
  5. **Timeout (seconds)**: how long the Data Center Expert server will wait for a response, in seconds, when it polls an IP address before it considers the poll failed.

5. 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.
     Note: You cannot schedule discovery for Modbus TCP devices.
   - 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, the device group in which to place the discovered SNMPv1 devices, Modbus devices, or NetBotz Appliances, 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. **Read Community Name**: the community name used to read information at the SNMPv1 devices.
     3. **Write Community Name**: the community name used to control an APC SNMP v1 device or register as a trap receiver at an APC SNMPv1 device.
     4. **Port**: the port number that the SNMPv1 devices use for communication.
     5. **Timeout**: how long the Data Center Expert server will wait for a response, in seconds, when it polls an IP address before it considers the poll failed.
     6. **Retries**: how many times the Data Center Expert 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.

7. **Register for Priority Scanning**: enables the Data Center Expert server to be defined as a trap receiver at discovered APC SNMPv1 devices. **Note:** Priority Scanning is a trap-based polling process that only occurs in response to traps from APC SNMPv1 devices or informs from APC SNMPv3 devices at which the Data Center Expert server is defined as a trap receiver. It allows the Data Center Expert server to immediately poll an APC SNMP device in response to a trap, rather than waiting to poll the device during the normal scanning interval.
8. **Device File Transfer Settings**: accesses the "Device File Transfer Settings" display used to edit, create, or view the file transfer settings for FTP or SCP access to SNMP devices.

- "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 Data Center Expert 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 Data Center Expert 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 Data Center Expert server to be defined as a trap receiver at discovered APC SNMPv3 devices. **Note:** Priority Scanning is a trap-based polling process that only occurs in response to traps from APC SNMPv1 devices or informs from APC SNMPv3 devices at which the Data Center Expert server is defined as a trap receiver. It allows the Data Center Expert server to immediately poll an APC SNMP device in response to a trap, rather than waiting to poll the device during the normal scanning interval.
  9. **Device File Transfer Settings**: accesses the "Device File Transfer Settings" display used to edit, create, or view the file transfer settings for FTP or SCP access to SNMP 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. For SNMPv1 devices, Modbus devices, or NetBotz Appliances, in the "Choose Device Group" display, edit the device group, as appropriate, and click **Next**.
5. 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**.

NetBotz 750 Appliance discovery

To discover NetBotz 750 appliances, choose the SNMPv1 or SNMPv3 discovery type. Only a Data Center Expert Server Administrator can configure the settings needed to discover NetBotz 750 appliances, and add SSL certificates if used.

1. Before you begin

When you log in to a NetBotz 750 device for the first time, you must log in as root via SSH or through a serial connection and set the root password.

See the Installation and Quick Configuration Guide for the NetBotz Rack Monitor 750 and the Security Handbook on the NetBotz 750 Rack Monitor product page: http://www.apc.com/prod_docs/results.cfm?DocType=App%20Note&Query_Type=10

Before you discover NetBotz 750 appliance in Data Center Expert, make sure you have:

- Access to the NetBotz 750 appliances you want to discover.
- The IP addresses or IP address range for the NetBotz 750 appliances you want to discover.

Only a Data Center Expert Server Administrator can configure Device File Transfer Settings, NetBotz Appliance Credentials, and add the NetBotz 750 SSL certificates in Data Center Expert.

2. Configure settings on the NetBotz 750 Appliance

On each NetBotz 750 Appliance you want to discover:

1. Log in to the NetBotz 750 web client, and enable SNMPv1 or v3 in the **Settings** > **System** > **SNMP** option. By default, SNMP is turned off on the NetBotz 750 appliance.
2. Uncheck the **Verify DCE Certificate in Trust Store**option in the **Settings** > **System** > **DCE Surveillance** option if Data Center Expert uses a self-signed certificate.

3. Add SSL Certificates to Data Center Expert and NetBotz 750 Appliance(s)

If Data Center Expert uses SSL to communicate, add SSL certificates to both Data Center Expert and each NetBotz 750 you want to discover.

Add the NetBotz 750 certificate to Data Center Expert

Add the certificate from each NetBotz 750 you want to discover in Data Center Expert. Otherwise, the cameras connected to the NetBotz 750 will not appear on the Surveillance tab.

Note: You do not need to add the NetBotz 750 SSL certificate if you intend to select No verification in the NetBotz 750 Camera Communication Settings option in Data Center Expert. This option is available after you discover the NetBotz 750.

1. Open a web browser, and go to the NetBotz 750 web client.
2. Download the certificate from the browser, and save the certificate file in Base-64 encoded X.509 format.
3. Log in to the Data Center Expert client.
4. Go to **System** > **Server Administration Settings** > **Server SSL Certificates**.
5. Click **Add**. Paste the certificate, or, click **Import Certificate** and then navigate to the NetBotz 750 certificate to import it.
6. Click **Add**.

Add the Data Center Expert SSL certificate to the NetBotz 750

Add the SSL certificate from Data Center Expert to each NetBotz 750 you want to discover. Otherwise, the NetBotz 750 cannot post camera clips and motion updates to Data Center Expert.

Note: If Data Center Expert uses a self-signed certificate, it is not necessary to upload the Data Center Expert self signed certificate to the NetBotz 750. Make sure the **Verify DCE Certificate in Trust Store**option is unchecked on each NetBotz 750 in the **Settings** > **System** > **DCE Surveillance** option.

1. Open a web browser, and go to the Data Center Expert web client.
2. Download the certificate from the browser, and save the certificate file in Base-64 encoded X.509 format.
3. Save the certificate file, and click **Finish**.
4. Log in to the NetBotz 750.
5. Go to **Settings** > **System** > **Trust Store**.
6. Click **Add**.
7. Open the certificate file in a text editor, and copy and paste the certificate into the field.
8. Click **Add**.
9. Repeat steps 4-8 for each NetBotz 750 you want to discover.

4. Configure settings on Data Center Expert

1. Click **Device** > **SNMP Device Communication Settings** > **Device File Transfer Settings** to add the root credentials (not superuser) for at least one NetBotz 750. Choose the protocol **SCP Only**. This allows Data Center Expert to download the device definition file (DDF) from the appliance.
2. Click **Device** > **NetBotz Appliance Communication Settings** > **NetBotz Appliance Credentials**. Click **Add** to specify the user credentials (not root) for the NetBotz 750 appliances you want to discover. If the credentials are different for any of NetBotz 750 appliances you want to discover, add each appliance to the list individually.

Warning and critical alarms can occur if Device File Transfer Settings and NetBotz Appliance Credentials are not configured either before you discover NetBotz 750 appliances, or, during discovery if you are a Data Center Expert Server Administrator. You can see these alarms in the Active Alarms pane in Data Center Expert.

5. Discover NetBotz 750 appliances

1. Click **Device** > **Add devices**. Select SNMPv1 or SNMPv3 depending on how your NetBotz 750 appliances communicate.
2. Specify the IP address or address range, SNMP settings, and whether you want to register for Priority scanning.
3. Add Device File Transfer Settings for at least one NetBotz 750 Appliance if you have not already done so. Click **Device File Transfer Settings**. Add the credentials for the root user (not superuser) for at least one of the NetBotz 750 appliances you are discovering. Choose the protocol **SCP Only**.
4. Add NetBotz Appliance Credentials for your NetBotz 750 Appliances if you have not already done so. Click **NetBotz Appliance Credentials**. Click **Add** to specify the information for NetBotz 750 appliances you want to discover. Enter the NetBotz 750 user credentials (not root). If the credentials are different for any of NetBotz 750 appliances you want to discover, add each appliance to the list individually.
5. Choose a group, and click Finish.

6. Configure NetBotz 750 Camera Communication Settings in Data Center Expert

If you have imported signed certificates from the NetBotz 750 Appliance, it is not necessary to modify the NetBotz 750 Camera Communication Settings.

If you imported a self signed certificate from the NetBotz 750 Appliance, and that certificate does not have a valid hostname:

1. Go to **Device** > **NetBotz Appliance Communication Settings** > **NetBotz 750 Camera Communication Settings**. Select one or more NetBotz 750 IP addresses, and click **Edit Communication Settings**.
2. Select **Verify certificate** and click OK.

7. Configure Surveillance Settings in Data Center Expert

Go to **Device** > **Surveillance Settings**. Select the NetBotz 750 cameras you want to license, check the box to **License Cameras**, and click OK. For more information, see Surveillance Settings.

"Device Discovery" wizard

Use this wizard to create, edit, and run the processes used to discover devices the Data Center Expert 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 **Device** 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, NetBotz Appliances, or Modbus TCP.

In DCE 8.2.0 and newer, the **Run discovery now** option is checked by default.

For information about discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

"Choose Discovery Type" display

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

For instructions on discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

Option	Description
SNMPv1 (includes 200 and 750 series NetBotz Appliance)	Select to discover devices that use standard SNMP communication (includes 200 and 750 NetBotz Appliances).
SNMPv3 (includes 200 and 750 series NetBotz Appliance)	Select to discover devices that use secure SNMP communication (includes 200 and 750 NetBotz Appliances).
300–500 series NetBotz Appliances (355, 450, 455, 550, 570)	Select to discover NetBotz Rack or Wall Appliances (355, 450, 455, 550, 570 models).
Modbus TCP	Select to discover devices that use Modbus TCP communication.

"SNMPv1 Discovery Settings" display

Use this display to define the settings used to discover SNMPv1 devices including NetBotz 250 and 750 Appliances.

For more information about discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

Element	Description
IP or 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	**Read Community**: define the community name to be used to read information at the SNMPv1 devices (**public**, by default). **Write Community**: define the community name to be used to control the APC devices or register as a trap receiver at the APC SNMPv1 devices (**private**, by default). **Port**: define the port number that the SNMP devices use for communication (**161**, by default). **Timeout**: define how long the Data Center Expert 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 Data Center Expert 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 Data Center Expert server registered as a trap receiver at discovered APC SNMPv1 devices. **Note:** Priority Scanning is a trap-based polling process that only occurs in response to traps from APC SNMPv1 devices or informs from APC SNMPv3 devices at which the Data Center Expert server is defined as a trap receiver. It allows the Data Center Expert server to immediately poll an APC SNMP device in response to a trap, rather than waiting to poll the device during the normal scanning interval.
Device File Transfer Settings	Click to use the display for **Device File Transfer Settings**, an **SNMP Device Communication Settings** option in the **Settings** menu, to edit, create, or view the file transfer settings used for FTP or SCP access to SNMP devices.

"SNMPv3 Discovery Settings" display

Use this display to define the settings used to discover SNMPv3 devices including NetBotz 250 and 750 Appliances.

For more information about discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

Element	Description
IP or 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**, **SHA**, **SHA-224, SHA-256, SHA-384, SHA-512**) and password used with that protocol. **Encryption Type/ Password**: select the encryption method (**None**, **DES**, **AES-128, AES-192, AES-256**) and password used with the **DES** or **AES** methods.

	Port: define the port number that the SNMP devices use for communication (**161**, by default). **Timeout**: define how long the Data Center Expert 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 Data Center Expert 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 Data Center Expert server register itself as a trap receiver at discovered APC SNMPv3 devices. **Note:** Priority Scanning is a trap-based polling process that only occurs in response to traps from APC SNMPv1 devices or informs from APC SNMPv3 devices at which the Data Center Expert server is defined as a trap receiver. It allows the Data Center Expert server to immediately poll an APC SNMP device in response to a trap, rather than waiting to poll the device during the normal scanning interval.
Device File Transfer Settings	Click to use the display for **Device File Transfer Settings**, an **SNMP Device Communication Settings** option in the **Settings** menu, to edit, create, or view the file transfer settings used for FTP or SCP access to SNMP devices.

"Device File Transfer Settings" display

Use this display to manage the File Transfer Protocol (FTP) or Secure Copy (SCP) access values for APC SNMPv1 and SNMPv3 devices.

Note: Functionally identical versions of this display are used by the "SNMPv1/SNMPv3 Device Discovery," "Apply Firmware Updates," and "APC SNMP Device Configuration" wizards, as well as by **Device File Transfer Settings**, an **SNMP Device Communication Settings** option in the **Device** menu. A change saved in one display is reflected in all.

- To use FTP for APC SNMP device access, FTP server access must be enabled at that device.
- To use SCP for APC SNMP device access, Secure Shell version 2 (SSHv2) console access must be enabled at that device.
- For NetBotz 750, you must add the credentials for the root user (not superuser).

  For more information about discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

Element	Description
List	Lists the access settings the Data Center Expert server can use for FTP or SCP access to its monitored devices. **Username**: The username used for access to a device. **Note:** By default, the Data Center Expert server can download firmware only to devices that use **apc** (lowercase) for the username and password (the actual password used for device access is identified in the "Edit Device File Transfer Settings" display). **IP or IP Range**: The IP address, or range of addresses, at which the access settings support FTP or SCP communication. **FTP Port**: The port used for FTP access to a device. **SCP Port**: The port used for SCP 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 try to access a device, after the initial attempt failed, before it stops trying to access that device (**1**, by default). **Protocol**: The protocol the transfer settings set will use to access devices (**FTP only**, **SCP only**, or **Try SCP, fall back to FTP**).
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 File Transfer Settings" display

Use this display to add or edit the settings the Data Center Expert server uses for File Transfer Protocol (FTP) or Secure Copy (SCP) access to APC SNMPv1 and SNMPv3 devices.

For more information about discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

Note: Functionally identical versions of this display can be accessed from the "Device File Transfer Settings" displays used by the "Apply Firmware Updates," "SNMPv1/SNMPv3 Device Discovery," and "APC SNMP Device Configuration" wizards, and by **Device File**

Transfer Settings, an **SNMP Device Communication Settings** option in the **Device** menu.

Element	Description
Username	Identify the name used for access to a device.
Password	Identify the password used for access to a device.
Verify Password	Retype the password.
IP or IP Range	Identify The IP address, or range of addresses, at which the access settings support FTP or SCP communication (***.*.*.***, by default).
Protocol	Identify whether the transfer settings will use FTP (**FTP only**), SCP (**SCP only**), or attempt to use SCP, but fall back to using FTP if SCP fails (**Try SCP, fall back to FTP**). **Note**: For NetBotz 750, choose **SCP only**.
FTP Port	Select the port the server will use for FTP access to devices (**21**, by default).
SCP Port	Select the port the server will use for SCP access to devices (**22**, by default).
Timeout	Identify how long the server will wait before it considers that an attempt to access a device has failed (**3000**, by default).
Retry Limit	Select the number of times the server will try to access a device, after the initial attempt failed, before it stops trying to access that device (**1**, by default).

"NetBotz Appliance Device Discovery Settings" display

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

To discover NetBotz 250 or 750 appliances, choose the SNMPv1 or SNMPv3 discovery type.

For more information about discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

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 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** **Note:** When you select this option, you must first add the certificate from the NetBotz Appliance you want to discover to the **Data Center Expert** server. You use the "Server SSL Certificate" display, a **Server Administration Settings** option in the **System** menu.
NetBotz Appliance Credentials	Click to use **NetBotz Appliance Credentials**, a **NetBotz Appliance Communication Settings** option in the **Device** menu, to manage the credentials the **Data Center Expert** server uses for communication with NetBotz Appliances.

"Modbus Discovery Settings" display

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

Modbus TCP devices with static IP addresses can be discovered on the public LAN; on Network A on the private LAN, when DHCP discovery is disabled (enabled by default); or on one segment you define on Network B on the private LAN.

Note: Modbus TCP device discovery entries are not stored in the "Saved Discoveries" list.

Element	Description
Single IP Address	Define the IP address the discovery process will search for a Modbus device.
Select Device Type	Define the device type from the list of those supported by the Data Center Expert server.
Server Address	Define the address of the device associated with the Modbus client IP address
Port	Define the port the Modbus device uses for communication (502, by default).
Timeout (seconds)	Define how long the Data Center Expert server will wait for a response, in seconds, when it polls an IP address before it considers the poll failed (**5**, by default).

"Choose Device Group" display

Use this display to select one device group into which to place the discovered devices, the Unassigned group by default.

Server Administrator users can place devices into any device group. Device Administrator users can place devices into only the device groups to which they have access.

For more information, see Device Group Access (Users tab).

"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	Run the discovery process when you exit the wizard. In DCE 8.2.0 and newer, the **Run discovery now** option is checked by default.

Saved Discoveries view

When you create a device discovery process, information about that process is listed in this view. Information about the device group selected during the SNMPv1 and NetBotz Appliance discovery process is not included.

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 Data Center Expert 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.
Import Discovery Entries	Import the SNMPv1 or NetBotz Appliance discovery entries from a local file.
Export Discovery Entries	Export the SNMPv1 or NetBotz Appliance discovery entries to a local file.

"Export Discovery Entries" display

Use this display to export information about the selected saved device discovery processes to a local file.

Note: Information about the device group selected during the SNMPv1 and NetBotz Appliance discovery process is not included.

Element	Description
Choose File	Select the location to save a copy of the device discovery properties as a *.txt file.
List	Lists the saved discovery processes, and provides the following information about each: **IP or IP Range**: The IP addresses the discovery process searched for devices. **Type**: The devices the process discovered: **SNMPv1**or **NetBotz Appliance**. **Parameters**: The network settings the discovery process used.
Export	Click to export the selected device discoveries to the local drive.

"Import Discovery Entries" display

Use this display to import saved device discoveries from a local file.

Element	Description
Choose File	Select the location to import the device discovery as a *.txt file.
List	Lists the imported discovery processes, and provides the following information about each: **IP or IP Range**: The IP addresses the discovery process searched for devices. **Type**: The devices the process discovered: **SNMPv1**or **NetBotz Appliance**. **Parameters**: The network settings the discovery process used.
Device Transfer File Settings	Accesses the display used to manage the settings the **Data Center Expert** server uses for File Transfer Protocol (FTP) or Secure Copy (SCP) access to APC SNMPv1 devices.
NetBotz Appliance Credentials	Accesses the display used to manage the list of credentials used for communication with the NetBotz Appliances.
Import	Click to import the selected device discoveries to the **Saved Discoveries** view.

Discovery Entries file format

Use this file format to import SNMPv1 and NetBotz Appliance device discovery entries to the **Saved Discoveries** view from a local *.txt file. Information about the device group selected during the discovery process is not included.

Note: You cannot import device discovery entries for SNMPv3 or Modbus devices.

Format for SNMPv1:

SNMPv1:<IP Address or Range>:<port>:<timeout>:<retries>:<trap registration (true or false)>:<read community>:<write community>

Example: SNMPv1:10.218.10-15.*:161:2:3:true:public:private

Format for NetBotz Appliance:

NetBotz Appliance:<IP Address or Range>:<port>:<security mode (HTTP or HTTPS_AVAIL_NO_VERIFY or HTTPS_REQ_NO_VERIFY or HTTPS_REQ_VERIFY)>

Example: NetBotz Appliance:10.218.10.166:80:HTTP

Device firmware and server updates

The **Updates** menu provides options you can use to update the Data Center Expert 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 Data Center Expert 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 "Select Device Updates" display, accessed from the Apply Firmware Updates option, to update firmware at the SNMP devices and NetBotz Appliances monitored by the Data Center Expert server.

1. In the **Updates** menu, select **Apply Firmware Updates**.
2. In the "Select Device Updates" display, do one of the following, depending on whether the Data Center Expert server has internet access.
   - Internet access available: click **Check Updates** to check if 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 Data Center Expert server.
   - Internet access unavailable: click **Import** to import the SNMP devices or NetBotz Appliance catalog at the Data Center Expert server.
3. In the "Device File Transfer Settings" display (SNMP devices), add new settings, or edit existing settings, as needed, and click **Finish**.

   Note: Two options in the **Device** menu allow you to manage the FTP, SCP, and global NetBotz Appliance credentials without accessing the **Apply Firmware Updates** option: **Device File Transfer Settings**, an **SNMP Device Communication Settings** option in the **Device** menu, and **NetBotz Appliance Credentials**, a **NetBotz Appliance Communication Settings** option in the **Device** menu.
4. Select the devices you want to update from the devices listed for each available firmware update, and click **Apply Updates**.

   Note: If no updates are available, click **Close**.
5. In the **Window** menu, select **Firmware Update Status**, a **Device** option.
6. In the update status view, review the progress for the selected updates.

Importing the APC updates catalog

You can download a copy of the APC device firmware update catalog (for SNMP devices and NetBotz Appliances) to your client, and then import that catalog to the Data Center Expert server, when that server does not have internet access to the APC updates server.

Note: If your DCE client does not have access to the internet, you will need to download the updates catalog to a machine that does have access, and transfer the file to your client.

1. Download the DCE Device Firmware Update Catalog from https://www.apc.com/us/en/product/SFSWCDFCF/dce-device-firmware-catalog-file/.
2. Once the updates catalog is downloaded, select **Apply Firmware Updates** in the **Updates** menu in the Data Center Expert client.
3. In the "Select Device Updates" display, click **Import**.
4. In the "Open" display, browse to the downloaded APC updates catalog, and click **Open**.
5. Go to step 4 of the Performing a firmware update task to update devices using the imported APC updates catalog.

"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
Search	Use the **Search** field to filter the list based on the text you type. **Note:** Only the Boolean operators AND, OR, and NOT are supported.
Configure Columns icon	Use the **Configure Columns** icon to identify the attribute columns that appear in the list.
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.
Update Description	Provides information about the update selected in the list.
Check Updates	Click to download any firmware updates available from the APC updates server for the Data Center Expert 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.
Device File Transfer Settings	Click to access the display used to manage the File Transfer Protocol (FTP) or Secure Copy (SCP) access values for APC SNMPv1 and SNMPv3 devices. **Note:** Functionally identical versions of this display are used by the "SNMPv1/SNMPv3

	Device Discovery" and "APC SNMP Device Configuration" wizards, as well as by **Device File Transfer Settings**, an **SNMP Device Communication Settings** option in the **Settings** menu. A change saved in one display is reflected in all.
Apply Updates	Click to perform a firmware update.

"Device File Transfer Settings" display

Use this display to manage the File Transfer Protocol (FTP) or Secure Copy (SCP) access values for APC SNMPv1 and SNMPv3 devices.

Note: Functionally identical versions of this display are used by the "SNMPv1/SNMPv3 Device Discovery" and "APC SNMP Device Configuration" wizards, as well as by **Apply Firmware Updates**, an option in the **Updates** menu, and **Device File Transfer Settings**, an **SNMP Device Communication Settings** option in the **Settings** menu. A change saved in one display is reflected in all.

- To use FTP for APC SNMP device access, FTP server access must be enabled at that device.
- To use SCP for APC SNMP device access, Secure Shell version 2 (SSHv2) console access must be enabled at that device.

Element	Description
List	Lists the access settings the Data Center Expert server can use for FTP or SCP access to its monitored devices. **Username**: The username used for access to a device. **Note:** By default, the Data Center Expert server can download firmware only to devices that use **apc** (lowercase) for the username and password (the actual password used for device access is identified in the "Edit Device File Transfer Settings" display). **IP or IP Range**: The IP address, or range of addresses, at which the access settings support FTP or SCP communication. **FTP Port**: The port used for FTP access to a device. **SCP Port**: The port used for SCP access to a device. **Timeout**: How long the server will wait before it considers that an attempt to access a device has failed.

Element	Description
	Retry Limit: How many times the server will try to access a device, after the initial attempt failed, before it stops trying to access that device (**1**, by default). **Protocol**: The protocol the transfer settings set will use to access devices (**FTP only**, **SCP only**, or **Try SCP, fall back to FTP**).
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 File Transfer Settings" display

Use this display to add or edit the settings the Data Center Expert server uses for File Transfer Protocol (FTP) or Secure Copy (SCP) access to APC SNMPv1 and SNMPv3 devices.

Note: Functionally identical versions of this display can be accessed from the "Device File Transfer Settings" displays used by the "SNMPv1/SNMPv3 Device Discovery" and "APC SNMP Device Configuration" wizards, as well as by **Device File Transfer Settings**, accessed from **Apply Firmware Updates**, an option in the **Updates** menu, and by **Device File Transfer Settings**, an **SNMP Device Communication Settings** option in the **Settings** menu.

Element	Description
Username	Identify the name used for access to a device.
Password	Identify the password used for access to a device.
Verify Password	Retype the password.
IP or IP Range	Identify The IP address, or range of addresses, at which the access settings support FTP or SCP communication (***.*.*.***, by default).
Protocol	Identify whether the transfer settings will use FTP (**FTP only**), SCP (**SCP only**), or attempt to use SCP, but fall back to using FTP if SCP fails (**Try SCP, fall back to FTP**).
FTP Port	Select the port the server will use for FTP access to devices (**21**, by default).
SCP Port	Select the port the server will use for SCP access to devices (**22**, by default).
Timeout	Identify how long the server will wait before it considers that an attempt to access a device has failed (**3000**, by default).
Retry Limit	Select the number of times the server will try to access a device, after the initial attempt failed, before it stops trying to access that device (**1**, by default).

Firmware Update Status view

An update status view is available using the **Firmware Updates** option accessed from **Device** in the **Window** menu.

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 canceled**, **Updates completed**, and **Successful updates**.
Cancel Pending Updates	Click to cancel pending device updates. **Note:** The Data Center Expert server can process device updates for up to 20 devices at a time. This button appears in the **Firmware 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 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: Firmware Update Status view (APC SNMP Devices)

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 from the server. **Recommended Action**: Make sure the access settings have not changed at the server or device, and the appropriate file transfer protocol 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 firmware.	An unknown error occurred. **Recommended Action**: Make sure the device is turned on and online, the appropriate file transfer protocol is enabled at the device, and that the "Device File Transfer Settings" display settings are correct. Correct any network connection problem.

Message	Description
	If the problem persists, contact APC Support (http://www.apc.com/support).
Failed to update the device: unable to connect.	A network or file transfer protocol communication problem exists. **Recommended Action**: Make sure the device is turned on and online, the appropriate file transfer protocol is enabled at the device, and that the "Device File Transfer Settings" display settings used to access the device include the device's correct 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 appropriate file transfer protocol 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 File Transfer Settings" display, and the appropriate file transfer protocol 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 appropriate file transfer protocol 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.

Message	Description
	Recommended Action: None
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: Firmware Update Status view (NetBotz Appliances)

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 "NetBotz Appliance Credentials" display accessed from **Server Administration** in the **Settings** menu 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 "NetBotz Appliance Credentials" display accessed from **Server Administration** in the **Settings** menu includes its correct IP address and port settings.

Message	Description
	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 "NetBotz Appliance Credentials" display accessed from **Server Administration** in the **Settings** menu 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 Data Center Expert server when a new version becomes available.

Performing a server update

You select the "Apply Server Update" option to import a server update package list file from your local machine, and install the server update.

IMPORTANT: FIPS mode requires that certificates must include the Subject Alternative Name with the fully qualified domain name (FQDN) and IP address of the monitored device or connected server. New certificates may be required.

1. Before beginning this procedure, you must have received 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 Data Center Expert 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 receive a message stating that the client and server are different versions. A link will be provided to download the updated client from the Data Center Expert 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 Data Center Expert** menu item. The display should reflect the new server version.

Device groups feature

Data Center Expert 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.
- Device groups and subgroups 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 button 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).
  - Edit 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 a specific configuration option for a selected NetBotz Appliance or Appliances (**NetBotz Appliance Configuration** options).
  Note: A **NetBotz Appliance Configuration** option is also in the **Device** menu. For information about these options, see **NetBotz Appliance Configuration** .
- Configure selected APC SNMP devices to use the same values for shared settings (**APC SNMP Device Configuration** option).
  Note: An **APC SNMP Device Configuration** option is also in the **Device** menu. For information about these options, see **APC SNMP Device Configuration** .
- Create thresholds for a selected device, or set of devices (**Create Thresholds** option).
  Note: For information about this option, see **Create Thresholds** option, under **Alarm Configuration** .
- Disable or re-enable notifications for any SNMP or Modbus device, or device group (**Enter/Exit Maintenance Mode** options).
- Access the **Custom Properties Editor** view to add, modify, or remove custom properties for selected devices or sensors (**Open Custom Properties Editor** option).
- Create a virtual sensor for a selected device group (**Create Virtual Sensor** option).
  Note: For information about this option, see Virtual Sensors view.

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, edit, or delete groups.
- Use the **Device View** to define which devices are assigned to which groups.

Managing the device groups

You can create, edit, and delete 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 name for the group or subgroup (required).
4. Enter a description for the group or subgroup.
5. Enter an address for the device group (optional), and click **Finish**.
6. Assign devices to the new group by dragging and dropping devices from the **Device View**.

7. Click **Device Group Access** to edit the user and user group monitoring and surveillance access to the device group, as needed.

Editing a device group

1. In the **Device Groups** view, right-click the group or subgroup you want to rename.
2. Click **Edit Device Group**.
3. Enter a name for the group or subgroup, or change the description or address, 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 Data Center Expert 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 Device Group Access (System menu)

Use the "Users and Device Group Access" option in this display to manage local and remote user access to the Data Center Expert server and its features and functions, and to manage the access those users have to the monitoring and surveillance data available for each device group in the **Device Groups** view.
Note: To logon to the Data Center Expert server, a user must have at least View Access for one device group that contains a minimum of one device.

The "Users and Device Group Access" display has two tabs, one with two sections.

Users and User Group Details (Users tab)

Use this section in the "Users and Device Group Access" display **Users** tab to manage the users and user groups that can access the Data Center Expert server.

Information about the users and user groups is provided in a table:

Column	Description
User or User Group Name	Lists the user groups, including default (**Device Administrators**, **Device Viewers**, **Server Administrators**, and **Unassigned Users**) and user-created groups. Users are listed under the user group to which they are assigned (local users not assigned to another group are listed under **Unassigned Users**; remote users are listed only under **Remote Users**). **Note:** This column is used in the **Device Group Access** section of the **Users** tab, as well.
Full Name	Identifies the full name for a local user only, when defined in its "User Configuration" display.
Type	Identifies each user or user group by its specific type. **Local User** **Remote User** **Local User Group** **Remote User Group** **Unassigned Users Group** **Remote Users Group**
Data Center Expert Administrator	Identifies whether a user or user group is assigned the **Data Center Expert Administrator** role, and, thus, has full

Column	Description
	access to all server features and functions (**Yes** or **No**).

You use buttons or right-click options to add new local users or local user groups, and to edit or delete users or user groups, whether local or remote.
Note: Remote users and user groups are added using the "Users and Device Group Access" display **Authentication Servers** tab.

- Add a local user using the "User Configuration" display (**Add User** button or right-click option).
  Note: You can select right-click and local device group and click **Add User to Selected Group** to add a new user directly to the selected group (this option is unavailable when a remote user group is selected).
- Add a local user group using the "User Group Configuration" display (**Add User Group** button or right-click option).
- Edit the credentials, user roles, and user group membership for a selected local user using the "User Configuration" display (**Edit** button or right-click option).
- Edit the name, user group roles, and user group members for a selected local user group using the "User Group Configuration" display (**Edit** button or right-click option).
  Note: You cannot edit the **Unassigned Users** group, a group that lists local users that are not assigned to another local user group.
- Edit the user roles for a selected remote user using the "User Configuration" display (**Edit** button or right-click option).
- Edit the user group roles for a selected remote user group using the "User Group Configuration" display (**Edit** button or right-click option).
  Note: You cannot edit the **Remote Users** group, listed in the table only when at least one authentication server has been added using the **Authentication Servers** tab.
- Delete a local or remote user or user group (**Delete** button or right-click option).
  Note: You cannot delete the **Remote Users** group, listed in the table only when at least one authentication server has been added, or the **Unassigned Users** group, which is always listed.
- Access the **Device Group Access** section of the **Users** Tab (**Device Group Access** button or right-click option).

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 and User Group Details** section of the **Users** tab, and click **Delete**.

1. In the **Users and User Group Details** section of the **Users** tab, 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. In the **User Credentials** section, define the credentials.
   b. In the **User Roles** section, select the role or roles for the user, if any.

      Note: If you select the **Data Center Expert Administrator** role, click **OK** to exit the "User Configuration" display: this role provides full access to all server, monitoring, and surveillance functions; settings in the **User Group Memberships** and **Device Group Privileges** tabs will have no affect on the user's privileges.
   c. If you want the user disabled, deselect **Enable this User**.

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

   Note: If you select a user group with **Data Center Expert Administrator** identified in its **Roles** column, selecting any other user group will have no affect on user privileges: this user group provides full access to all server, monitoring, and surveillance functions.

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 **Users and User Group Details** section of the **Users** tab, and click **Delete**.

1. In the **Users and User Group Details** section of the **Users** tab, click **Add Group** to add a local user group, or select a listed local user group and click **Edit** to access the "User Group Configuration" display.
2. In the **User Group Information** tab.
   a. Define a name for the group.
   b. Select the role or roles for the group, if any.

      Note: The **Data Center Expert Administrator** role provides full access to all server, monitoring, and surveillance functions to any user assigned to the group.
3. In the **User Group Members** tab, select the local users you want assigned to the group, if any.

Managing a remote user

Use the "User Configuration" display to edit the user role assigned to 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 and User Group Details** section of the **Users** tab and click **Delete**.

1. In the **Users and User Group Details** section of the **Users** tab, select a listed remote user and click **Edit**, to access the "User Configuration" display.

   Note: For a remote user, only the **User Roles** selections in the **User Information** tab are available.
2. In the **User Roles** section, select a role for the user, if any, and click **Apply**.

   Note: The **Data Center Expert Administrator** role provides full access to all server, monitoring, and surveillance functions.

Managing a remote user group

Use the "User Group Configuration" display to edit the user role assigned to 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 **Users and User Group Details** section of the **Users** tab and click **Delete**.

1. In the **Users and User Group Details** section of the **Users** tab, select a listed remote group and click **Edit**, to access the "User Group Configuration" display.

Note: For a remote user group, only the **User Roles** selections in the **User Group Information** tab are available.

2. In the **User Group Roles** section, select the role or roles for the group, if any, and click **Apply**.

   Note: The **Data Center Expert Administrator** role provides full access to all server, monitoring, and surveillance functions.

"User Configuration" display

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

The "User Configuration" display has two tabs; one tab has two sections.

User Credentials (User Information tab)

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

Credential	Definition
Username	Identify the name used to log on to the server.
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- **Data Center Expert Administrators**)	Identify the user's email address. **Note:** This address is used to send e-mail to a **Data Center Expert Administrator** for notifications related to the Data Center Expert server itself, and monitored NetBotz Appliances, but not for monitored SNMP or Modbus devices.
Description (optional)	Identify a role, title, or other attribute that describes the user.

User Roles or User Group Roles (User or User Group Information tab)

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

Note: For a non- **Data Center Expert Administrator** user, including a user for which no role is selected, access privileges are determined by **Device Group Access** settings in the **Users** tab for that user, and for the user groups to which the user is assigned.

Role	Description
Data Center Expert Administrator	Full access to all server, monitoring, and surveillance functions for all device groups.

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: The user will be listed under any user group in the "Users and Device Group Access display's **Users** tab to which it is assigned in its **User Group Memberships** tab.

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

"User Group Configuration" display

Use the tabs in this display to add or edit a local user group, including defining its roles and members, or to edit the roles only for a remote user group.

The "User Group Configuration" display has two tabs; one tab has two sections.

Group Name (User Group Information tab)

Use this setting to define the name for a local user group only.

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 user 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: A user selected in this tab will be listed under the user group in the "Users and Device Group Access" display's **Users** tab.

Device Group Access (Users tab)

Use this section in the "Users and Device Group Access" display's **Users** tab to manage the monitoring and surveillance access you want a user or user group to have at each device group.

Note: These settings are accessed by selecting the right-click **Device Group Access** option for any device group in the **Device Groups** view, or by clicking **Device Group Access** in the "Users and Device Group Access" display's **Users** tab.

To manage the access settings, select a listed user or user group and click **Modify Device Group Access** to access the "Device Group Access" display. However, this button is inactive for the following entries:

- The **Unassigned Users** group
- The **Remote Users** group
  Note: This users group is listed only when at least one authentication server has been added using the **Authentication Servers** tab.
- The primary **Data Center Expert** **Administrator** user (**apc**, by default).
- Any user or user group that has **Data Center Expert** **Administrator** selected for its role.
  Note: You can change this role for any user or user group except the primary **Data Center Expert** **Administrator** user (**apc**, by default).

Membership in a user group can affect a user's monitoring and surveillance access at the device groups. The settings that provide the least-restrictive access, whether it is the user's or user group's **Device Group Access** settings, define the access a user has. For example, if a user with **No Access** for surveillance at a device group belongs to a user group with **View and Tag Access** for surveillance at that device group, that user has **View and Tag Access**.

Column	Description
User or User Group Name	Lists the user groups, including default (**Device Administrators**, **Device Viewers**, **Server Administrators**, and **Unassigned Users**) and user-created groups. Users are listed under the user group to which they are assigned (local users not assigned to another group are listed under **Unassigned Users**; remote users are listed only under **Remote Users**). **Note:** This column is used in the **Users and User Group Details** section of the **Users** tab, as well.
Device Group	Reports the **Monitoring** and **Surveillance** access a selected user or user group has at the device groups. You can edit the access settings for a device group if **Modify Device Group Access** is enabled for the selected user or user group. **Note:** The **All Devices** group access settings provide a baseline for all other device groups. The other device groups will use at least the same access settings as **All Devices**, but any group can be set to use less-restrictive settings.
Monitoring	Reports the monitoring access a selected user or user group has at the device groups.
Surveillance	Reports the surveillance access a selected user or user group has at the device groups.

Monitoring access

Five selections are available for user or user group monitoring access at a selected device group.

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

Monitoring Access	Description
No Access	No monitoring access is provided.
View Access - No Camera Images	A user with this access setting for a device group can perform the following functions for the devices in that group: 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 Data Center Expert server scan a selected SNMP or Modbus device, or set of SNMP and Modbus devices, to update the available information.
View Access	A user with this access setting for a device group can perform the following functions for the devices in that group: View information about active and historical alarms. View information about device sensors. View NetBotz Appliance camera images. View clips in active and historical alarms. 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 Data Center Expert server scan a selected SNMP or Modbus device, or set of SNMP and Modbus devices, to update the available information.
View and Control Access	Users with this access setting for a device group can perform the same monitoring functions **View Access** provides, as well as the following additional functions: Change the state of a sensor in the right-click menu of the "View Device Sensors" display, when available.

Monitoring Access	Description
	Change the state of an outlet in the "Outlet Control" display, when available.
Administration Access	A user with this access setting at a device group can perform all the same monitoring functions **View Access** provides, as well as the following additional functions: Create a custom **Map View** for the device group. Configure NetBotz Appliance **Alert Thresholds** and SNMP and Modbus **Thresholds** for device sensors in that group. Configure **NetBotz Appliance Configuration** options at monitored NetBotz Appliances in that group. Configure the **Device Configuration** settings for SNMP and Modbus devices in that group. Configure the **Device File Transfer Settings**. Apply SNMP device and NetBotz Appliance firmware updates that have been downloaded to the Data Center Expert server for the group's devices. **Note:** Only a **Data Center Expert Administrator** can download the updates to the server.

Surveillance access

Five selections are available for a user or user group's surveillance access at a selected device group.

Note: Users assigned the **Data Center Expert Administrator** role, or assigned to a user group that has this role, have full monitoring 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 functions for the monitoring access associated with a device group: any **Surveillance** setting other than **No Access** for a device group requires at least **View Access** for that group's monitoring access setting.

Surveillance Access	Description
No Access	No surveillance access is provided.
View Live Feed Only (No camera clips)	A user with this access setting for a device group can perform the following functions for that group's camera devices: Access the **Camera** view for a licensed camera in the **Thumbnails** view. Change the state of a sensor in the **Camera** view, when available, when the user is also assigned View and Control monitoring access.
View Access	A user with this access 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.

Surveillance Access	Description
	Change the state of a sensor in the **Camera** view, when available, when the user is also assigned View and Control monitoring access.
View and Tag Access	A user with this access setting at a device group can perform all functions **View Access** provides, but with the added ability to tag surveillance clips.
Administration Access	A user with this access setting at a device group can perform all functions **View and Tag Access** provides, but with the added ability to configure the **Surveillance Settings** for all camera devices, and delete surveillance clips.

"Modify Device Group Access" display

Use this display to define the **Monitoring Access** and **Surveillance Access** you want a user or user group to have for the device group selected in the **Device Group Access** settings section of the **Users** tab.

The access 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 settings added (check-marked in the **Device Group Access** settings 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 setting set to **View Access**, and no device group has a higher setting selected, only the **View Access** and **No Access** settings will be available for the **All Devices** group.
  - If any device group has had its **Monitoring Access** set at **View and Control Access**, **Administration Access** will be unavailable for that monitoring access for the **All Devices** group.
    Note: If any group other than **Unassigned** has had access set at **Administration Access**, all settings for that monitoring access will be available for the **All Devices** group.
- The settings available at other groups depend on the settings defined at their parent group: 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 Access**, and **View and Tag Access** selected for its **Surveillance Access**, **No Access** is unavailable for the **Monitoring Access** at all other groups, and **No Access** and **View Access** are unavailable for the **Surveillance Access** at all other groups.

Another factor affects the access set at device groups other than **All Devices**: you can select an access that is identical to the access a group is inheriting from **All Devices**, or a parent group. Although the selected group's access settings remain unchanged, those access settings 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.

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 Data Center Expert server.

Each authentication server listed has users and user groups that can be assigned as remote users and user groups at the Data Center Expert server.

Use the "Add Authentication Server" wizard to add the authentication server to the tab and assign users and groups.

Use the "Edit Authentication Server" wizard to modify settings.

You can select an authentication server to configure the timeout for AD/LDAP up to 300 seconds, 15 seconds by default. When you increase the timeout on this tab, also increase the timeout on the desktop client login screen.

Users and user groups will be listed in the **Groups** and **Users** folders for the appropriate server or servers in the **Authentication Servers** tab and in the **Users** tab.

Note: When a remote user, or a user that belongs to a remote user group, attempts to log in to the Data Center Expert server, the username and password are sent to the authentication server associated with that user. It is that server, and not the Data Center Expert server, that authenticates the login 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 Data Center Expert 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 Data Center Expert 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 "OpenLDAP/Active Directory Server Settings" display, configure the settings, if necessary, and click **Next**.
3. In the "OpenLDAP/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 Data Center Expert console.

"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.

"OpenLDAP/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 Data Center Expert and the authentication server.

"OpenLDAP/Active Directory Bind Settings" display

Use this display to configure the settings the Data Center Expert 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 Data Center Expert server.

Reports menu

Provides options used to generate Sensor History reports and Snapshot reports, and manage the export configurations that are used to export reports on a scheduled basis.

Note: A **Manage Export Scheduling** right-click option in the **Saved Sensor Reports** section also accesses the "Manage Export Scheduling" display. For more information about the **Manage Export Scheduling** option, see Reports feature.

Reports perspective

This perspective provides access to predefined snapshot reports, and sensor history reports you create, about the devices monitored by the Data Center Expert server.

The **Reports** perspective allows you to generate, view, and export reports in HTML, CSV (comma-delimited), or PDF format, for the device groups selected.

- **Available Reports**: lists the snapshot reports, sensor history reports, and saved sensor reports available for the devices the Data Center Expert server monitors, and allows you to generate those reports for selected device groups and devices.
- **Sensor History Reports**: allows you to generate and customize sensor history reports for the devices the **Data Center Expert** server monitors. Sensor history reports can be saved in the **Saved Sensor Reports** section, and exported in graph-format, or viewed and exported in table-format or summary-format.
- **Snapshot Reports**: allows you to generate a report, containing data for the particular time at which the report is generated, for the devices the **Data Center Expert** server monitors. Snapshot reports can be viewed in graph-format only, and exported to HTML, CSV (comma-delimited), or PDF.
- **Saved Sensor Reports**: allows you to view, edit, rename, delete, and export sensor history reports you have saved.
- **Report Views**: display snapshot reports, and sensor history reports, generated for the device groups selected, and allows you to export those reports. See Snapshot Reports and Sensor History Reports for more information.

Sensor History Reports option

This option allows you to create **Sensor History Reports** for specific sensor types associated with a group selected in the **Device Group** view, as well as **Custom Sensor History Reports** (graph-format, table-format, or summary-format) for any or all sensors associated with monitored SNMP, Modbus, and NetBotz Appliance devices.

- **Custom Sensor History Reports** are created using the **Custom** option in **Generate Sensor History Report** , a right-click option and icon ( ), in the **Device Groups** view, **Active Alarms** view, **Alarm History** view, and **Device View**, and a right-click option in **Map View**. You select the date range, devices and device groups, sensor types, and sensors to include in the report. You can modify the report after it is created by selecting the **Edit Report Criteria** icon.
- **Sensor History Reports** are created for a selected device group, for the previous 24 hours, using the list of sensor types included in the right -click **Sensor History Reports** option of the **Device Groups** view, **Device View**, and **Map View**. You can modify the date range, devices and device groups, sensor types, and sensors to include in the report after the report is created by selecting the **Edit Report Criteria** icon.
  Note: You can also create Sensor History Reports in the Available Reports view of the Reports perspective.

You can create and save reports in graph-format, table-format, or summary-format, then access those reports at any time in the **Saved Reports** section of the **Reports** perspective. You can create a graph-format report, then view the data as a table by selecting the **Table Data** icon, or as a summary by selecting the **Summary Data** icon. You can export table

data or summary data reports as .csv or .txt files, and graph reports as .bmp,.jpg, or.png files.

Note: You cannot save **Snapshot Reports** in the **Saved Reports** view. You can save these reports locally as *.HTML,*.CSV (comma-delimited), or *.PDF files. For more information, see **Snapshot Reports** .

Edit Report Criteria option

Use this display to create graph-format, table-format, or summary-format reports for the device groups or devices selected when you click the **Custom** option in the right-click **Sensor History Reports** menu, or the **Custom Sensor History Report** icon in the **Device Groups**, **Alarm History**, **Active Alarms**, or **Device View**. In addition, use this display to edit the report criteria for a **Sensor History Report** or **Custom Sensor History Report** you have already created.

The devices and device groups, sensor types, and sensors listed by default in the "Report Criteria" display depend upon which view was used to access it:

- **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.

You can modify the report criteria before or after you create a report.

Note: When you click **Generate Report**, the report will not appear in the **Saved Reports** view until you use the **Save** icon to save the report.

Element	Description
Choose 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.
Choose Report Format	Select to display the report in graph (the default), summary, or table format.
Choose Devices and Device Groups	Select the devices or device groups you want to include in the report.
Choose Sensor Types	Select the sensor types you want to include in the report.
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. **Configure Columns** icon: identify the columns that appear in the display. **Sensors list**: select the device sensors you want the **report** to include. When modifying an existing report, the list includes all sensors for the devices that were selected when the report was created or last edited,

	with the following information provided for each sensor: • **Device**: device label • **Sensor**: sensor name • **Sensor Type**: 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.

"Name and Schedule Data Export" display

Use this display to export data from a report in the **Saved Reports** section by defining a name for the report, if desired, and defining how and when the report will be periodically exported.

You access this display from the **Edit Report Scheduling** right-click option in the **Saved Reports** section, or the **Edit Report Criteria** icon, accessed from the view for any saved or unsaved sensor history report. An unsaved sensor history report is saved in the **Saved Reports** section when you click OK to schedule the data export.

Element	Description
Report Name	Define or modify the name that will identify the report in the **Saved Reports** view.
Enable Export	Select to enable the report data export 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**.
Configure Columns	Choose the columns, including those created using custom property keys, and the order in which they will appear in the report.
Locale	Select to specify the locale for the report data or **Use Server Locale** (the default).
Scheduling	**Days of the week**: Select the day or days of the week for the exports. **First of the month**: Select the first of the month for the exports. **Time**: Select the time of day for the exports.
Report Interval	Select the interval between entries in a report.

Graph-format reports

This report format provides data, in the form of a graph and device sensor list, for up to 1026 device sensors.

Note: You can access a graph-format report view by clicking **Generate Report** in the **Reports** perspective, and choosing **Graph** as the report format (the default), or by selecting a report in the **Saved Reports** view.

The name (***Sensor History Report**, for an unsaved report) is identified on the tab for each report; the sensor type and time frame is identified at the top of each report.

You can select the **Trend Line** button icon to display a linear trend line when all numeric sensors included in the graph-format report use the same unit of measure. Trend lines are calculated using a linear regression model and the ordinary least squares estimation method. All the available data returned by the Data Center Expert server for the sensors selected, and the time range specified for the report, are considered in the model. The data are extended for twice the specified time range to create the trend line. For example, in a report with a time range of seven days, the linear regression is calculated over fourteen days: seven days of actual data, and seven days of prediction.

You can use the device sensor list columns, right-click menu, 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, report format, or sensors for a selected report using the "Report Criteria" display (**Edit Report Criteria** option or icon).
- Edit the report name or export properties using the "Name and Schedule Data Export" display (**Edit Report Criteria** option or icon).
- Save a copy of the report as a *.bmp (the default selection), *.jpg, or *.png file (**Export Graph** icon).
- Access the "Set Refresh Rate" display used to control how often an open graph will refresh automatically, if at all (**Refresh** icon).
  Note: The refresh settings are client-specific, and have no affect on the refresh settings used by other Data Center Expert clients.
- Display a linear trend line for twice the time period as the data, on numeric sensors only, when all numeric sensors included in the graph use the same unit of measure (**Trend Line** icon).
- Highlight the point for which data is displayed when you move the cursor over the graph (**Marker** icon).
- Click and drag the graph to view a specific area (**Pan** icon).
- View a summary-format version of a selected report (**Summary Data** icon or **Open Summary Data** option).
- View a table-format version of a selected report (**Table Data** icon or **Open Table Data** option).
- Name a report and save it in the **Saved Reports** section of the **Available Reports** view (**Save** icon).
- View the graph in more or less detail (**Zoom In** or **Zoom Out** option and icon).
  Note: You can click and drag the cursor to select a portion of the graph to view in more detail.
- Reset the graph back to its original position (**Reset Graph Position** option).

Graph section

Provides a graphic representation of the values reported by the device sensors included in a **Sensor History Report** or **Custom Sensor History Report** , over the period of time selected.

- 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 **Sensor History Report** , a single sensor's value range is labeled along the left-side of the graph.
- For **Custom Sensor History Reports** , which can cover multiple types of sensors, one sensor value range is labeled along the left-side of the graph, while any additional value ranges for the report's sensors are labeled to the right of the graph.
- A linear trend line is plotted on graph-format reports for twice the time period as the data, on numeric sensors only, when all numeric sensors included in the graph use the same unit of measure.

Sensor list section

Lists and provides information about each device sensor included in a **Sensor History Report** , including the color used to represent values for each sensor in the graph.

Column	Description
Color	The color used for the sensor values in the graph. **Note:** You can deselect the color to remove sensor values from the graph, or select (the default), to include the sensor values.
Location	The location of the sensor, if known.
Parent Device	**Data Center Expert** for SNMP and Modbus devices, or the hostname of a NetBotz Appliance for devices monitored by a NetBotz Appliance.
Monitored Device	The device label.
Sensor	The sensor type, followed by a name, if the sensor has one.
Units	The unit of measurement for numeric sensors, only.
Last Known Value	The last reported value during the time span of the report.
Minimum Value	The lowest value measured by numeric sensors only, during the time span of the report.
Maximum Value	The highest value measured by numeric sensors only, during the covered time span.
Average Value	The average value measured by numeric sensors only, during the covered time span.

"Set Refresh Rate" display

Use this display to control how often the selected graph-format **Sensor History Report** or Custom Sensor History Report will refresh automatically, if at all.

You can use any auto-refresh setting when you create a graph with less than 50,000 data points. When you create a graph with 50,000 - 199,999 data points, the graph will refresh only when you select a refresh interval of five minutes or greater. When you create a graph with 200,000 data points or more, the graph will not refresh.

Note: These settings are client-specific, and have no affect on the refresh settings used by other Data Center Expert clients.

Element	Description
Enable Graph Refresh	Enable (check-marked) or disable (default setting) the automatic refresh of the graph-format report.
Refresh Interval	Select how often the report will refresh (**5 Minutes**, by default).

"Sensor Table Data" display

This display allows you to view and save the data in a graph-format report as a table.

You click the **Table Data** icon or select the **Open Table Data** option in a graph-format **Sensor History Report** to view data as a table.

The "Sensor Table Data" display shares all the same features as a table-format **Sensor History Report** with the following exceptions:

- Sensor table data cannot be saved in the **Saved Reports** section of the **Reports** perspective.
- The report criteria for the table data cannot be modified.
- Scheduled data export is not available.

The number of sensors covered in the report, total number of data points, and the time frame are identified at the top of each table. 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.
- Select the columns, and the order in which they appear in the table, and choose whether or not to highlight alarming sensors in the table (**Edit Report Options** icon).
- Save sensor table data as a *.csv (the default selection) or *.txt file (**Save Report Data** and chevron icons).
  Note: You must use the chevron icon to select the *.txt format.
- 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> (Data Center Expert)** for SNMP and Modbus devices, or the IP address or hostname of a NetBotz Appliance for devices monitored by that appliance.
Sensor	The sensor name.
Location	The location of the sensor, if known.

Time	The date and time of the most recent sensor value change.
Value	The value measured at the identified date and time.
Unit	The unit of measurement for numeric sensors, only.
Status	The sensor status: **Alarm** (when a **Warning**, **Error**, **Critical**, or **Failure** condition exists), or no text (when no alarm condition exists). **Note:** Sensor status is reported only for sensors that have been configured at the **Data Center Expert** server, for SNMP and Modbus devices the server monitors directly, or at the NetBotz Appliances, for devices monitored by those appliances, using **Alert Thresholds**, the **NetBotz Appliance Configuration > Alert Settings** options in the **Device** menu.

"Sensor Summary Data" display

This display allows you to view and save the data in a graph-format report as a summary.

You click the **Summary Data** icon or select the **Open Summary Data** option in a graph-format **Sensor History Report** to view data as a summary.

The "Sensor Summary Data" display shares all the same features as a summary-format **Sensor History Report** with the following exceptions:

- Sensor summary data cannot be saved in the **Saved Reports** section of the **Reports** perspective.
- The report criteria for the summary data cannot be modified.
- Scheduled data export is not available.

The total number of data points are identified at the top of each table. 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 information in that column.
- Select the columns, and the order in which they appear in the table; choose whether or not to include the total for the delta value in the table; and choose whether or not to highlight alarming sensors in the table (**Edit Report Options** icon).
- Save sensor summary data as a *.csv (the default selection) or *.txt file (**Save Report Data** and chevron icons).
  Note: You must use the chevron icon to select the *.txt format.
- Browse through a multiple-page report (**Go to** arrow icons, and a box that identifies the page number).

A summary-format report shares all of the same features as a table-format report, with the following exceptions:

- A table-format report provides entries for each value change at those sensors during the reports time-frame; a summary-format report provides a single entry for each selected sensor that summarizes the values at those sensors during the reports time-frame.
- Unlike a table-format report, a summary-format report does not include a **Status** column.

Note: A summary-format report includes information about the **Last Known Value**, which has a different meaning than the **Value** reported by a table-format report.

- Only a summary report includes the following information:

Column	Description
Minimum Value	The lowest value recorded during the time-frame of the report.
Maximum Value	The highest value recorded during the time-frame of the report.
Average Value	The average of the values recorded during the time-frame of the report.
Last Known Value	The most recent value recorded before the end of the time-frame of the report.
Delta Value	The difference between the minimum and maximum values recorded during the time-frame of the report.
Total for Delta Value	The total of the delta values for the sensors in the report, included when **Show Total for Delta Value** is selected in the "Edit Report Options" display. **Note:** The Show Total for Delta Value option is available only when all sensors in the report are the same type.

Table-format reports

This report format provides data for up to 1026 sensors, in the form of table that lists all the device sensors included in a report.

You create a table-format **Sensor History Report** by selecting the **Table** report format in the "Report Criteria" display.

You can access a table-format report view of a previously generated report:

- Select the **Edit Report Criteria** icon in the report view, and the **Table** report format.
- Select the **Edit Report Criteria** right-click option in **Saved Reports** in the **Reports** perspective, and the **Table** report format.

Note: You can click the **Table Data** icon or select the **Open Table Data** option in a graph-format **Sensor History Report** to view data as a table. See "Sensor Table Data" display.

The number of sensors covered in the report, total number of data points, and the time frame are identified at the top of each table. 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, report format, or sensors for a selected report using the "Report Criteria" display (**Edit Report Criteria** icon).
- Edit the report name or export properties using the "Name and Schedule Data Export" display (**Edit Report Criteria** option or icon).

- Name a report and save it in the **Saved Reports** section of the **Available Reports** view (**Save** icon).
- Select the columns, and the order in which they appear in the table, and choose whether or not to highlight alarming sensors in the table (**Edit Report Options** icon).
- Save sensor table data as a *.csv (the default selection) or *.txt file (**Save Report Data** and chevron icons).
  Note: You must use the chevron icon to select the *.txt format.
- 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>** **(Data Center Expert)** for SNMP and Modbus devices, or the IP address or hostname of a NetBotz Appliance for devices monitored by that appliance.
Sensor	The sensor name.
Location	The location of the sensor, if known.
Time	The date and time of the most recent sensor value change.
Value	The value measured at the identified date and time.
Unit	The unit of measurement for numeric sensors, only.
Status	The sensor status: **Alarm** (when a **Warning**, **Error**, **Critical**, or **Failure** condition exists), or no text (when no alarm condition exists). **Note:** Sensor status is reported only for sensors that have been configured at the **Data Center Expert** server, for SNMP and Modbus devices the server monitors directly, or at the NetBotz Appliances, for devices monitored by those appliances, using **Alert Thresholds**, the **NetBotz Appliance Configuration > Alert Settings** options in the **Device** menu.

"Edit Report Options" display (table-format)

Use this display to choose the columns and the order in which they appear in the table-format report.

Type	Description
Highlight Alarming Sensors	Select to highlight (in red) the **Value** for sensors that have active alarm conditions when a threshold setting has been defined for that alarm at the **Data Center Expert** server, for a sensor associated with a monitored SNMP device, or at a NetBotz Appliance associated with a sensor.
Available Columns	Lists columns created using custom property keys, and any default columns not included in the report.

Add/Remove Columns	Allows you to choose the columns to include in the report.
Chosen Columns	Lists the columns to include in the report.
Move Up/Down	Allows you to specify the order in which the columns appear in the report.
Report Interval	Select the interval between entries in a report.

Summary-format reports

This report format provides data for up to 4000 sensors, in the form of a table that identifies all the device sensors included in the report, and summarizes the values measured by those sensors during the time-frame specified for the report.

You create a summary-format **Sensor History Report** by selecting the **Summary** report format in the "Report Criteria" display.

You can access a summary-format report view of a previously generated report:

- Select the **Edit Report Criteria** icon in the report view, and the **Summary** report format.
- Select the **Edit Report Criteria** right-click option in **Saved Reports** in the **Reports** perspective, and the **Summary** report format.

Note: You can click the **Summary Data** icon or select the **Open Summary Data** option in a graph-format **Sensor History Report** to view data as a summary. See "Sensor Summary Data" display.

A summary-format report shares all of the same features as a table-format report, with the following exceptions:

- A table-format report provides entries for each value change at those sensors during the reports time-frame; a summary-format report provides a single entry for each selected sensor that summaries the values at those sensors during the reports time-frame.
- Unlike a table-format report, a summary-format report does not include a **Status** column.
  Note: A summary-format report includes information about the **Last Known Value**, which has a different meaning than the **Value** reported by a table-format report.
- Only a summary report includes the following information:

Column	Description
Minimum Value	The lowest value recorded during the time-frame of the report.
Maximum Value	The highest value recorded during the time-frame of the report.
Average Value	The average of the values recorded during the time-frame of the report.
Last Known Value	The most recent value recorded before the end of the time-frame of the report.
Delta Value	The difference between the minimum and maximum values recorded during the time-frame of the report.

Column	Description
Total for Delta Value	The total of the delta values for the sensors in the report, included when **Show Total for Delta Value** is selected in the "Edit Report Options" display. **Note:** The Show Total for Delta Value option is available only when all sensors in the report are the same type.

The total number of data points covered in the report are identified at the top of each summary. You can use the search feature, 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, report format, or sensors for a selected report using the "Report Criteria" display (**Edit Report Criteria** icon).
- Edit the report name or export properties using the "Name and Schedule Data Export" display (**Edit Report Criteria** option or icon).
- Name a report and save it in the **Saved Reports** section of the **Available Reports** view (**Save** icon).
- Select the columns, and the order in which they appear in the table; choose whether or not to highlight alarming sensors in the table; and choose whether or not to include the total for the delta value in the report (**Edit Report Options** icon).
- Save sensor table data as a *.csv (the default selection) or *.txt file (**Save Report Data** and chevron icons).
  Note: You must use the chevron icon to select the *.txt format.
- Browse through a multiple-page report (**Go to** arrow icons, and a box that identifies the page number).

"Edit Report Options" display (summary-format)

Use this display to choose the columns and the order in which they appear, highlight active Critical, Error, Failure, and Warning alarms, and include the total for the delta value in the summary-format report.

Type	Description
Highlight Alarming Sensors	Select to highlight (in red) the **Value** for sensors that have active alarm conditions when a threshold setting has been defined for that alarm at the **Data Center Expert** server, for a sensor associated with a monitored SNMP device, or at a NetBotz Appliance associated with a sensor.
Show Total for Delta Value	Select to include the total for the delta value in the report, available only when all sensors in the report are the same type.
Available Columns	Lists columns created using custom property keys, and any default columns not included in the report.
Add/Remove Columns	Allows you to choose the columns to include in the report.
Chosen Columns	Lists the columns to include in the report.
Move Up/Down	Allows you to specify the order in which the columns appear in the report.

Snapshot Reports

This section provides access to predefined reports about the devices monitored by the Data Center Expert server.

The **Snapshot Reports** section allows you to generate, view, and export reports in HTML, CSV (comma-delimited), or PDF format, for the device groups selected.

Element	Description
UPS Runtime	Lists UPS systems, by IP Address, within available UPS Runtime-range categories (for example, <10 minutes).
Device Type Inventory	Lists the number of monitored devices for each device type, by model name.
Battery Age	Lists UPS systems, by IP address, within Battery Age-range categories (for example, 2-3 years).
Environmental Humidity	Lists the % Humidity, by sensor, within Humidity-range categories (for example 40-50).
Environmental Temperature	Lists the Temperature, by sensor, within Temperature-range categories (for example 60-80).
Generate Report	Allows you to choose the device groups you want to include in the report selected.

Snapshot Report View

This view displays Snapshot Reports and allows you to export it.

You can use the **Go To** arrow icons to browse through a multiple-page report, along with the box that identifies the page being viewed.

Icon	Description
	Use the chevron icon included with this **Export** icon to save the selected report as *.HTML, *.CSV, or *.PDF.

"Choose Device Groups" display

Use this display to choose the device groups you want to include in a Snapshot Report.

Element	Description
Device Group	Check-mark the groups you want to include in the report selected

	Note: All device groups, and the Select/Deselect All option, are check-marked by default.
Generate Report	Click to render the report for the device groups selected.

Button icons (report views)

The report views have icons you can use to perform various functions.

Sensor History Report graph-format icons

Icon	Description
	Use this **Edit Report Criteria** icon to edit the time frame or sensors you want a selected report to cover.
	Use this **Marker** icon to highlight the point for which data is displayed when you move the cursor over the graph.
	Use this **Pan** icon to click and drag the graph to view a specific area.
	Use this **Zoom In** icon to view the graph in more detail.
	Use this **Zoom Out** icon to view the graph in less detail.
	Use this **Summary Data** icon to view a summary-format version of a selected report.
	Use this **Table Data** icon to view a table-format version of a selected report.
	Use this **Trend Line** icon to view a linear trend line for the same time period as the data, on numeric sensors only, when all numeric sensors included in the graph use the same unit of measure.
	Use this **Refresh** icon to select how often reports will refresh.
	Use this **Save** icon to name a report and save it in the **Saved Reports** section of the **Available Reports** view. **Note:** An asterisk (*) preceding the report name indicates the report has not been saved.

Icon	Description
	Use this **Export** icon to save a copy of a report to the local drive.

Sensor History Report table-format and summary-format report icons

These report views share two icons and **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 **Edit Report Criteria** icon to edit the time frame or sensors you want a selected report to cover.
	Use this **Save** icon to name a report and save it in the **Saved Reports** section of the **Available Reports** view. **Note:** An asterisk (*) preceding the report name indicates the report has not been saved.
	Use this **Save Copy of Graph** icon for a graph-format report to save it as a *.bmp, *.jpg, or *.png file. Use this **Save Report Data** icon for a table-format or summary-format report to save a copy of the report as a .*txt or *.csv file. **Note:** You must use the chevron icon included with this **Save Report Data** icon in table-format and summary-format reports to select *.txt.
	Use this **Edit Report Criteria** icon to edit the time frame or sensors you want a selected report to cover.

Snapshot report icons

The snapshot report views have one icon and **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 **Export** icon to export a copy of the snapshot report as an *.html file. **Note:** You must use the chevron icon included with this **Export** icon to select *.csv (comma-delimited) or *.pdf

Saved Sensor Reports section

This section of the **Available Reports** view allows you to view, edit, rename, or delete saved reports.

Note: Reports are saved using the "Name and Schedule Data Export" display, accessed from the **Edit Report Criteria** icon, or by using the **Save** icon in the view for a graph-format report.
You can use the right-click options to perform the following functions:

- Edit the date range or sensors for a selected report using the "Edit Report Criteria" display (**Edit Report Criteria** option).
- Edit the name or export properties for a selected report using the "Name and Schedule Data Export" display (**Edit Report Scheduling** option).
- Modify the name of a selected report (**Rename** option).
- Delete a selected report (**Delete** option).

Manage Export Scheduling option (Reports menu)

Use this option to manage the schedule configuration settings used to export saved reports from the **Data Center Expert** server.

"Manage Export Scheduling" display

Use this display to manage the list of schedule configurations for saved reports, used for scheduled export from the **Data Center Expert** server.

Element	Description
List	Lists the export configurations for saved reports, and provides the following information about each: **Saved Sensor Report**: the name of the report scheduled for export. **Scheduled Days**: the day or days of the week for the exports. **Scheduled Time**: the time of day for the exports. **Scheduled**: whether or not the report export is enabled. **Summarized Export**: whether the export is summary-report data only. **Export Name**: the name of the export configuration. **Export Type**: the type of the export configuration.

Export Action Configuration	Click to access the display used to manage actions used to export saved reports from the Data Center Expert server.
Edit Report Criteria	Click to access the display used to modify report criteria for the selected report.
Edit Schedule	Click to access the display used to modify or schedule data export for the selected report.
Delete Report	Click to remove the saved report from the Data Center Expert server.

"Export Action Configuration" display

Use this display, accessed by the **Manage Export Scheduling** option in the **Reports** menu, to manage a list of export configurations used for the scheduled export of saved reports from the **Data Center Expert** server.

Element	Description
List	Lists the saved export action configurations, and provides the following information about each: **Export Name**: the name defined for the export action. **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 action.
Edit Export	Click to use the "Edit Export" display to edit the settings of a selected export action configuration.
Remove Export	Click to delete a selected export action configuration.

Managing the export action configurations

You can add new export action configurations, or edit existing configurations, using the "Export Action Configuration" display, accessed from the **Manage Export Scheduling** option of the **Reports** menu.

Note: To remove an export action configuration, select it in the list and click **Remove Export**.

Adding a new export action configuration

1. Select **Export Action Configuration**, accessed from the **Manage Export Scheduling** option in the **Reports** menu. Alternatively, click the **Edit Report Scheduling** option in the **Saved Sensor Reports** section of the **Reports** perspective, or click the **Edit Report Criteria** icon in a graph-format report, to access the **Name and Schedule Data Export** option.
2. In the "Export Action Configuration" display, click **Add Export** to access the "Add Export" wizard. Alternatively, in the "Name and Schedule Data Export" display, click **Add Export** to access the "Add Export" wizard.
3. In the "Choose Export Type" display, select the type of export action configuration you want to add.
4. In the settings display for the selected export type, define the settings.

   Note: Each export type uses 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 action configuration

1. Select **Export Action Configuration**, accessed from the **Manage Export Scheduling** option in the **Reports** menu.
2. In the "Export Action Configuration" display, select a listed export, 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 action configuration you want to add, and to define the settings for that configuration.

Note: When you click **Edit Export** in the "Export Action Configuration" display, you access the 'Edit Export" display, the same display, except in name, that was used to add the export action configuration.

"Choose Export Type" display

Use this display to select the type of export you want to add.

Option	Description
E-mail Export	Click to add e-mail settings.
FTP Export	Click to add FTP settings.
HTTP Export	Click to add HTTP settings.
NFS Export	Click to add NFS settings.

Windows Export	Click to add Windows settings.

"E-mail Export Settings" display

Use this display to add or edit an export action configuration that exports a report's data to specified e-mail addresses.

Note: The SMTP server the Data Center Expert 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.

"FTP Export Settings" display

Use this display to add or edit an export action 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 Data Center Expert 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.

"HTTP Export Settings" display

Use this display to add or edit an export action 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.
Server Requires Authentication	Activate the **Username**, **Password**, and **Verify Password** settings used for authenticated HTTP server access.
Username	Identify the name needed to post data to the HTTP server at the specified **Target URL**.
Password	Identify the password needed to post data to the HTTP 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.

"NFS Export Settings" display

Use this display to add or edit an export action configuration that exports a report's data to a specified UNIX server that uses the Network File System (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 receive 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.
Protocol	Select the transport protocol: UDP or TCP.
Version	Select the NFS version: v2.0, v3.0, v4.0, or v4.1.
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).

"Windows Export Settings" display

Use this display to add or edit an export action 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.
Security	Specify the NT LAN Manager authentication level: NTLM, NTMLi, NTLMv2, NTLMv2i, NTLMSSP, or NTLMSSPi.
Test Export	Click to test the export settings. **Note:** Verify the test data actually was saved in the proper folder on the Windows server.

Alarm Configuration Overview

The Alarm Configuration perspective provides options used to configure how the Data Center Expert server reports alarms and threshold violations, and manages alarm actions, for monitored SNMP and Modbus devices.

By default, four views appear in the **Alarm Configuration** perspective. These views, along with **Manage Alarm Actions**, an **Alarm Configuration** menu option, allow you to perform threshold and device alarm configuration and notification functions for monitored SNMP and Modbus devices.

- **Navigation** view: contains the navigation tree, listing device groups and the monitored devices associated with them. This view allows you to do the following:
  - Select a device group or device in the navigation tree to view the list of thresholds or device alarms that can be configured or added to a notification policy.
  - Select a device group or device in the navigation tree and create thresholds for that selection.
  - Edit thresholds.
  - View device sensors and current sensor data for the selected device.
  - Enter and exit maintenance mode to prevent and re-enable alarm notifications for the device groups or devices selected.
  - Add and remove thresholds from a notification policy.
  - Select a device group or device in the navigation tree and edit the configuration for all the device alarms for the selection.
  - Select a device group or device in the navigation tree and change the notification policy associated with that device group or device.
    Note: A device can be associated with only one notification policy at a time.
  - Modify the default labels in the navigation tree.
- **Notification Policies** view: displays the default notification policy, user-created notification policies, and the notification policy details. This view allows you to do the following:
  - Create, modify, and delete notification policies.
  - Double-click a notification policy to view the actions, thresholds, and devices associated with it.

  Note: The **Default** notification policy can be edited and renamed, but it cannot be deleted.
  Note: At device discovery, alarms for SNMP and Modbus devices monitored by the Data Center Expert server are added to the **Default** notification policy. You can change the notification policy associated with a device from **Change Device Alarm Notification Policy**, a right-click option in the **Navigation** view.
- **Threshold Alarm Configuration** view: displays the list of thresholds that can be configured or added to a notification policy. By default, a communication link status threshold is displayed for every device monitored by the **Data Center Expert** server. This view allows you to do the following:
  - Modify and delete thresholds.
    Note: You cannot delete communication link status thresholds.
  - Add and remove thresholds from notification policies.
  - Display the notification policies associated with the selected thresholds.
  - Find the device associated with the selected threshold in the **Navigation** view.
- **Device Alarm Configuration** view: displays the list of device alarms that can be configured or added to a notification policy. This view allows you to do the following:
  - Enable or disable an alarm, modify the severity and recommended action, and add a custom description.

- Find the device associated with the selected alarm in the **Navigation** view.
- Expand the list when there is more than one device alarm in the selection.

Creating alarm notifications

Use the Alarm Configuration perspective to define the alarm notifications you want available to the Data Center Expert server for monitored SNMP and Modbus devices.

You must do the following before the Data Center Expert server can generate alarm notifications:

- Create at least one alarm action.
- Add at least one alarm action to the **Default** notification policy.

You can do the following to specify how the Data Center Expert server generates additional alarm notifications:

- Create thresholds for sensor types supported by each device.
- Create new notification policies.
- Add at least one alarm action to each notification policy you created.
- Add thresholds, devices, and additional alarm actions, to the **Default** notification policy, or notification policies you created.
- Add SNMP and Modbus devices to notification policies you created.
- Modify thresholds or device alarm configurations, if necessary.

You can create and configure thresholds, alarm actions, and notification policies, or modify device alarm configurations, at any time, in any order. For example, you can create alarm actions first, create thresholds, then add selected actions, thresholds, and devices, as needed, to the **Default** notification policy. Alternatively, you can create new notification policies first, then create actions or thresholds, and add them to any notification policy.

Alarm Configuration menu

Provides options used to configure how the Data Center Expert server reports alarm conditions.

"Search" field

Use the **Search** field to filter the list based on text you type.

You can broaden or narrow your search using the Boolean operators AND, OR and NOT. For example, you can search for UPS AND On Battery; PDU NOT Phase 1; Humidity OR Temperature; Humidity OR Temperature NOT UPS.

Only items that contain the text you specify in the **Search** field are displayed. When the results of a search are displayed, the background of the search field is shaded. When you clear the search field, the background shading is removed and all items are displayed.

Note: Search fields support the Boolean operators AND, OR, and NOT only.

Navigation View

This view in the **Alarm Configuration** perspective shows the device groups and devices for which thresholds and device alarms can be configured on SNMP and Modbus devices.

You can select a device group or device in the **Navigation** view to display the thresholds or device alarms that can be configured or added to a notification policy for that selection. Thresholds are displayed in the **Threshold Alarm Configuration** view; device alarms are displayed in the **Device Alarm Configuration** view. The number of thresholds or device alarms associated with each device group or device is shown next it, in parentheses.

You can use the **Search** fields to filter the list based on text you enter in the Navigation, Threshold Alarm Configuration, and Device Alarm Configuration views; only items that contain the text you type are listed.

When the results of a search are displayed, the background of the search field is shaded. When you clear the search field, the background shading is removed and all items are displayed.
Note: You can hold the Ctrl key down to select multiple items.

You can use the right-click options and the button icons at the top of the view to do the following:

- Create thresholds for any sensor value reported for any device group or device (**Create Thresholds** option).
- Edit the thresholds for the device group or device selected (**Edit Thresholds** option).
- Access the "View Device Sensors" display to see current sensor data for the selected device (**View Device Sensors** option).
- Prevent alarm notifications from occurring for the device groups or devices selected (**Enter Maintenance Mode** option).
- Re-enable alarm notifications for the device groups or devices selected (**Exit Maintenance Mode** option).
- Add the thresholds for the selected device group or device to a specified notification policy (**Add Thresholds to Notification Policy** option).
- Remove the thresholds for the selected device group or device from a specified notification policy (**Remove Thresholds from Notification Policy** option).
- Enable or disable, modify the severity and recommended action, and add a custom description on one or more alarms for the device group or device selected (**Edit Device Alarm Configuration** option).
- Change the notification policy associated with the device alarms in the device group or device selected (**Change Device Alarm Notification Policy** option).
  Note: All device alarms for all devices are added to the **Default** notification policy at device discovery.
- Access the "Configure Navigation Tree Labels" display to select up to three labels to specify how monitored devices appear in the navigation tree (**Configure Navigation Tree Labels** icon ( )).

Button icons (Navigation view)

In addition to standard minimize and maximize icons, one icon is available to perform specific **Navigation** view functions.

Icon	Description
	Use this **Configure Navigation Tree Labels** icon to identify up to three labels that appear in the navigation tree. The device type and hostname are displayed by default.

"Configure Navigation Tree Labels" display

Use this display to select up to three labels to specify how monitored devices appear in the navigation tree. This affects the navigation tree in the **Navigation** view and the **Choose Thresholds** display in the **Notification Policies** view.
Note: The device type and hostname are displayed by default.

Label	Description
Groups	The names of any device groups a device belongs to, including **Unassigned**.
Type	The type of device.
Model	The device model, if known. For example, **Symmetra PX**, for an APC/MGE UPS.
Hostname	The hostname, or IP address, if no hostname is defined, for a monitored SNMP or Modbus device.
Serial Number	The serial number assigned to a device, if known.
IP Address	The IP address used by a monitored SNMP or Modbus device.
Location	The location associated with a device, if known.
Application Version	The application or firmware version number for a device, if known. For example, **v3.5.8**, for a Smart-UPS 3000 RM device.
Label	The label of the device.
Maintenance Mode	Indicates whether notifications have been disabled for the device.
<Custom Property Key Name>	All custom property keys, identified by name.
Contact Name	The name of the contact associated with the device.

Create Thresholds option

The Data Center Expert allows you to create thresholds for any sensor reported by a device.

In addition to the alarms available for each device, you can create thresholds for the Data Center Expert server. Two basic types of thresholds are available: those that use numeric settings, and those that use state settings.

Note: You can create a threshold for a virtual sensor using the **Create Threshold** option for the selected virtual sensor. You cannot create a virtual sensor for state sensors. See Virtual Sensors view for more information.

- Numeric thresholds:
  - **Air Flow**
  - **Audio**
  - **Current (Amps)**
  - **Dew Point**
  - **Energy (kWh)**
  - **Humidity**
  - **Other Numeric Sensors**
  - **Power (VA)**
  - **Power (kVA)**
  - **Power (Watts)**
  - **Power (Kilowatts)**
  - **Temperature**
  - **Voltage**
- State thresholds:
  - **Door**
  - **Dry Contact**
  - **Motion Sensor**
  - **Other State Sensors**

Both types of thresholds allow you to do the following:

- Create thresholds at one time for multiple sensors of the same type (for example, all are **Humidity** sensors, or all are **Door** sensors).
- Specify the severity and return-to-normal parameters for any defined threshold.
- Provide a custom URL and custom description for any defined threshold.
- Configure Threshold Scheduling to specify when any defined threshold is active.
- Add any defined threshold to one or more Data Center Expert notification policies.

Five menus provide access to create alarm thresholds:

- **Create Thresholds** , an option in the **Alarm Configuration** menu.
- Right-click menu **Create Thresholds** in the navigation tree in the **Navigation** view.
- Right-click menu **Create Thresholds** in the **Device Groups** view in the **Monitoring** perspective.
- Right-click menu **Create Thresholds** in the **Device View** in the **Monitoring** perspective.
- Right-click menu **Create Thresholds** in the **Map View** in the **Monitoring** perspective.

Each threshold option allows you to search the sensors monitored by the Data Center Expert server that match the selection. You can add a threshold to one of those sensors, or add thresholds with the same settings to any number of those sensors simultaneously.

Using the right-click menus to add thresholds to one or more sensors allows you to focus threshold management to the sensors at a single device, or at a set of devices.

Creating numeric and state thresholds

All numeric and state thresholds use the same basic procedure and displays to create threshold settings.

Note: The same displays are used to create thresholds when you select the **Create Thresholds** option in any of the following:

- The **Alarm Configuration** menu.
- The right-click menu in the navigation tree in the **Navigation** view of the **Alarm Configuration** perspective.
- The right-click menu in the **Device Groups**, **Device View**, or **Map View** of the **Monitoring** perspective.

Threshold settings for all monitored devices are available when you use the **Alarm Configuration** menu options. Threshold settings for only the device group or device selected are available when you use the right-click menu in the **Navigation** view, **Device Groups**, **Device View**, or **Map View**.

1. Select the sensor type on which you want to add a threshold from the **Create Thresholds** option in the **Alarm Configuration** menu. Alternatively, select a device group or device in the **Alarm Configuration** or **Monitoring** perspective views, and right-click to select the **Create Thresholds** option.
2. In the "Select Threshold Type" display, select the threshold type you want to add, and click **Next**.
3. In the "Select Sensors" display, select the sensor or sensors for which you want to add thresholds, and click **Next**.
4. In the "Create Threshold" display, define the settings, and, if desired, configure when the Data Center Expert server will generate notifications if the threshold becomes active using the **Threshold Scheduling** button, and click **Next**.
5. In the "Select Notification Policies" display, select the notification policies to which you want to add the alarm threshold, and click **Finish** to exit the wizard.

Thresholds and supported devices

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

For a full SNMP support device or Modbus device monitored by the Data Center Expert server, all threshold options except **Dew Point** can be used to define threshold settings the Data Center Expert server will monitor for that device. These thresholds are created using the **Create Thresholds** option.

Full SNMP support and Modbus devices:

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

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

- Set the threshold settings that the Data Center Expert server will monitor for these devices.
- Select the notification policies the Data Center Expert server will use for alarm notifications related to these devices.

NetBotz Appliances:

When you create alert thresholds for a NetBotz Appliance, its sensor pods, camera pods, and monitored SNMP devices (using **Alert Settings**, a **NetBotz Appliance Configuration** option in the **Device** menu), the threshold settings are set at the NetBotz Appliance. It is the NetBotz appliance that stores the settings and sends the alerts to the Data Center Expert 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.

Basic and model ID SNMP support devices:

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

Numeric alarm thresholds

Numeric alarm 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:

- 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 **Dew Point** can be used to define threshold settings the Data Center Expert 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.
Audio	**Relative number (0 - 100)**	Settings for sensors that measure the volume of sound.
Current (Amps)	**Amps (0.0 - 100.0)**	Settings for sensors that measure current as total amperage (amps).
Dew Point	**°F (-40.0 - 122.0)/ °C (-40.0 - 50.0)**	Settings for sensors that measure dew point as degrees Fahrenheit (°F) or Celsius (°C).
Energy (kWh)	**kWh**	Settings for sensors that measure energy consumption as kilowatt hours (kWh).
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 **Thresholds** options.
Power (VA)	**VA** and **kVA**	Settings for sensors that measure power as total Volt-amperes (VA) or kiloVolt-amperes (kVA). **Note:** Sensors that measure power as a percentage of VA will be displayed under the

		Other Numeric Sensors option.
Power (Watts)	**W** and **kW**	Settings for sensors that measure power as total watts (W) or kilowatts (kW).
Temperature	**°F (-40.0 - 122.0)/ °C (-40.0 - 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 value is below the **Minimum** setting for longer than the delay in the **Time Allowed Below Minimum** setting.
Above Value for Time Threshold	An alarm occurs if the sensor value is above the **Maximum** setting for longer than the delay in the **Time Allowed Above Maximum** setting.
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 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 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 Data Center Expert server.

Note: You can configure multiple sensors discovered for the **Other Numeric Sensors** option, when the sensors you select can all use the same threshold settings. For example,

battery and UPS age sensors use the same units of measure, and can be configured at the same time, as can utility, input, and output voltage sensors.

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 alarm 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 **Thresholds** options.

State threshold types:

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

State Mismatch for Time Threshold	An alarm occurs when the sensor state does not match the **Normal State** setting for longer than the time defined by the **Time Allowed in Alarm 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 Data Center Expert server.

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

Note: You can configure multiple sensors discovered for the **Other State Sensors** option, when the sensors you select use the same alarm states settings. For example, all sensors that use **On** and **Off** states can be configured at the same time, as can all sensors that use **Up** and **Down**.

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

"Select Threshold Type" display

This display allows you to select the type of threshold for which you want to create an alarm.

You use this display to choose the type of threshold you want to create on any available sensors for the device group or device you select. The types of thresholds available depend on the type of sensor you select.

Note: Once you access this display, you must select a threshold type and click **Next** or click **Cancel** to exit the wizard.

"Select Sensors" display

Use this display to select the sensors on which you want to create an alarm threshold.

When you access this display from the **Alarm Configuration** menu **Create Thresholds** option, all the sensors monitored by the Data Center Expert server for the selected threshold type are listed.

When you access this display from the right-click menu in the **Navigation** view of the **Alarm Configuration** perspective, only the sensors for the selected device group or device are listed.

You can select the **Configure Columns** icon to identify the columns that appear in the display. You can click the column headers to sort the list in ascending or descending order.

Column	Description
Sensor	Identifies the sensors that can be configured for the threshold selected.
Current Reading	The most recent value reported by the sensor.
Hostname	Identifies a device by its hostname, or IP address when no hostname is defined.
Unit of Measure	Defines the unit of measure for numeric sensors only.
Device Type	Identifies a device by its type, or by **SNMP Device**, if the Data Center Expert server cannot determine the device type.
Device Model	Identifies a device by its model number, when known.
Device Label	Identifies a device by its label, or IP address.
Parent Device	**<server_name> (Data Center Expert)** for devices monitored by the Data Center Expert server.
<Custom Property Key Name>	A custom property key, identified by name.

"Create Sensor Threshold" display

Use this display to configure the settings for the identified threshold.

In addition to the settings provided, the display also identifies the name of the sensor (**Sensor Name**), the type of 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**). You can use the **Threshold Scheduling** button to access the **Threshold Schedule** display to configure when the threshold alarm action will be active.
Note: When more than one sensor is selected, the name of the sensor is identified in the display as <Multiple>, and value currently read by the sensor is identified as <Multiple Values>.

Threshold settings :

Element	Description
Threshold value	Define the criteria for the threshold. **Note:** The available value fields will depend on the type of numerical or state threshold selected.
Enabled	Select to enable the threshold, if it is disabled. **Note:** Thresholds are enabled by default.
Severity	Select the severity you want associated with the threshold: **Information**, **Warning**, **Error**, **Critical**, or **Failure**.
Return-to-Normal Requires User Input	Select to clear a threshold violation only when a user with **Administrator** privileges marks the alarm condition as resolved.
Return-to-Normal Delay	Define a delay, in seconds, that will occur after a threshold 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.
Custom Description	Provide a description you want included in a threshold's alarm notifications.
Custom URL	Identify an Internet address you want included in an alarm notification for the threshold.

"Select Notification Policies" display

This display allows you to select the notification policies to which to add the selected threshold.

You can add the threshold to one or more existing notification policies, or none.
Note: The **Default** notification policy is selected by default and can be deselected.

Edit Thresholds option

The Data Center Expert allows you to edit threshold settings for any sensor reported for any device.

You select a device group or device in the navigation tree of the **Navigation** view in the **Alarm Configuration** perspective to view the thresholds for that selection.

Three basic types of thresholds are available: those that use numeric settings, those that use state settings, and those that monitor communication link status.

- Numeric thresholds:
  - **Air Flow**
  - **Audio**
  - **Current (Amps)**
  - **Dew Point**
  - **Energy (kWh)**
  - **Humidity**
  - **Other Numeric Sensors**
  - **Power (VA)**
  - **Power (kVA)**
  - **Power (Watts)**
  - **Power (kWatts)**
  - **Temperature**

    - **Voltage**
- State thresholds:
    - **Door**
    - **Dry Contact**
    - **Motion Sensor**
    - **Other State Sensors**
- Communication threshold
    - **Communication status**

All types of thresholds allow you to do the following:

- Edit thresholds at one time for multiple sensors of the same type (for example, all are **Humidity** sensors, or all are **Door** sensors) at the devices monitored by the Data Center Expert server.
- Specify the severity and return-to-normal parameters for any defined threshold.
- Provide a custom description for any defined threshold.
- Configure **Threshold Scheduling** to specify when any defined threshold is active.

Three menus provide access the **Edit Thresholds** option:

- Right-click menu **Edit Thresholds** in the navigation tree in the **Navigation** view: each option allows you to simultaneously edit the thresholds for one or more sensors that match that option, for the selected device group or device.
- Right-click menu **Edit Thresholds** in the **Threshold Alarm Configuration** view: allows you to edit only the threshold selected, or when multiple thresholds are selected, each option allows you to simultaneously edit the thresholds for all the sensors that match that option.
- Right-click menu **Edit Alarm Configuration** in the **Active Alarms** view of the **Monitoring** perspective: allows you to edit only the threshold selected.

Note: You can use the **Filter Thresholds** icon ( ) to modify the **Threshold Alarm Configuration** view to prevent communication link status, user-created thresholds, thresholds with 'Enabled' set to 'No', and thresholds of any severity from appearing in the view.

"Edit thresholds" display

Use this display to configure the settings for the identified thresholds.

In addition to the settings provided, the display also identifies the number of sensors to be modified, the name of the sensor (**Sensor Name**), the type of 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**).
Note: When more than one sensor is selected, the name of the sensor is identified in the display as <Multiple>, and value currently read by the sensor is identified as <Multiple Values>.

Threshold settings :

Element	Description
Threshold value	Define the criteria for the threshold. **Note:** The available value fields will depend on the type of numerical or state threshold selected.
Enabled	Select to enable the threshold, if it is disabled. **Note:** Thresholds are enabled by default.

Severity	Select the severity you want associated with the threshold: **Information**, **Warning**, **Error**, **Critical**, or **Failure**.
Return-to-Normal Delay	Define a delay, in seconds, that will occur after a threshold 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 **Yes** to clear a threshold violation only when a user with **Administrator** privileges marks the alarm condition as resolved.
Custom Description	Provide a description you want included in a threshold's alarm notifications.
Custom URL	Identify an Internet address you want included in an alarm notification for the threshold.

"Threshold Schedule" display

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

Note: This display is used to schedule when a threshold will be enabled and disabled, using the threshold's settings display.
Two menus in the **Alarm Configuration** perspective provide access to the Threshold Schedule display:

- The threshold settings display in the **Create Thresholds** option.
- The threshold settings display in the **Edit Threshold** option.

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 alarm threshold 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.

"Edit Thresholds" display

Use this display to edit existing thresholds for the selected device.

The display lists all the settings currently defined for each option.

Element	Description
Threshold Types	Select the threshold type you want to view in the display.
Search	Filter the list based on text you enter in this box; only existing thresholds that contain the text you type are listed. You can broaden or narrow your search using the Boolean operators AND, OR and NOT only.

	When the results of a search are displayed, the background of the search field is shaded. When you clear the search field, the background shading is removed and all items are displayed.
List	Check-mark the previously defined thresholds that you want to edit or delete. The following information is provided for the listed threshold. **Threshold**: the sensors that can be configured for the threshold selected. **Current Value**: the most recent value reported by the sensor. **Parameters**: the settings defined for the threshold. **Alarmed State**: whether the threshold is in an alarm state. **Hostname**: the hostname, or IP address when no hostname is defined. **Unit of Measure**: the unit of measure. **Name**: the name of the threshold. **Severity**: the severity of the threshold. **Label** : the device label, or IP address when no label is defined. **Device Model** : the model, when known. **IP Address**: The IP address of the device. **Device Type**: the type of device. **Notification Policy**: the policy or policies with which the threshold is associated.
Edit	Click to edit a selected threshold.

View Device Sensors option

This option shows the current sensor data for the selected device or active alarm.

You can select a device or active alarm to view the most recent sensor data available for that selection. By default, data for all sensor types are displayed when data for more than one sensor type is available. For some devices, you can select one sensor set for which to display current data.

Use the **Search** field to filter the list of sensors based on the text you type. You can broaden or narrow your search using the Boolean operators AND, OR and NOT. Only items that contain the text you specify in the **Search** field are displayed. When the results of a search are displayed, the background of the search field is shaded. When you clear the search field, the background shading is removed and all items are displayed.

Use the **Configure Columns** icon to show or hide sensor columns and custom properties.

Five menus provide access to the "View Device Sensors" display:

- Right-click menu **View Device Sensors** in the **Device View** and **Map View** of the **Monitoring** perspective.
- Right-click menu **View Device Sensors** in the **Active Alarms** view in the **Monitoring** perspective: view the most recent sensor data available for the device on which the selected alarm occurred.
  Note: Camera clips are not displayed when more than one active alarm is selected.
- Right-click menu **View Device Sensors** in the navigation tree in the **Navigation** view of the **Alarm Configuration** perspective.
- Right-click menu **View Device Sensors** in the **Alarm History** view, accessed from the **Window** menu.

Enter/Exit Maintenance Mode options

Schedule when you want to disable or re-enable notifications for any device or device group. This option is available to users with Device Administration or View and Control access on the Data Center Expert server.

You use the **Enter Maintenance Mode** option to disable notifications for the selected devices or device group on a date and time you specify, and re-enable notifications on a date and time you choose, or never.

You can choose **Never** re-enable notifications if you do not want to get notifications for the selected devices, or you prefer to re-enable notifications manually.

You can use the **Exit Maintenance Mode** option re-enable notifications now or at a time you choose.

Note: The date and time you choose to enter and exit maintenance mode is the local time of the Data Center Expert client.

The **Maintenance Mode Schedules** window automatically opens when you create a schedule and displays all the schedules you create. You can modify a schedule to specify the time to disable or re-enable notifications at any time.

Right-click a schedule to:

- **View Devices** in a schedule and remove selected devices from the schedule if needed.
- **Edit Maintenance Mode Schedule and Comment** to change the date and time to enter or exit maintenance mode, or to modify the comment.
- **Delete** the schedule. When you delete a schedule, the maintenance mode settings are also disabled and deleted.

When notifications are disabled:

- The **Active Alarm** and **Alarm History** views report the date and time the notifications were disabled and when they were enabled again.

  Notifications also appear in the web client event log.
- The information for affected devices is italicized, and the regular status icons are replaced, in the Device View, Map View, and view in the Alarm Configuration perspective.
- You can click a device to view its status in the **Active Alarms** view. All alarm conditions are reported while notifications are disabled.

User Access

Users with Device Administration access can perform all actions on schedules created by all users, and view the usernames of all schedule owners.

Users with Device View and Control access can see all the schedules created in the **Maintenance Mode Schedules** window.

Users with Device View access can only see schedules in the **Maintenance Mode Schedules** window if they have access to devices listed in that schedule. The usernames of the schedule owners are not visible. View and Control users can see only the devices they have access to in any schedule, and can only modify the schedules they create.

Schedule ownership

The user who creates a schedule is the owner of that schedule. Access permission to a schedule is based on the owner.

Administration users can add devices to any schedule regardless of ownership.

If an Administration user adds devices to a schedule owned by a View and Control user, the View and Control user can only see those devices if they have access to them. Otherwise, a message is displayed.

A schedule owner can remove any device from the schedule regardless of whether they have control access to it.

Add Thresholds to Notification Policy option

This option allows you to add thresholds for the selected device group, device, or thresholds to an existing policy used by the Data Center Expert server to generate alarm notifications.

In the **Alarm Configuration** perspective, you can select a device group, device, or threshold and add the thresholds for that selection to an existing notification policy. All the thresholds for that selection will be added to the selected notification policy.
Note: You can view thresholds after they have been added to the notification policy, and choose which thresholds to include or exclude. You can add alarm actions and configure options for those actions.

Two menus in the **Alarm Configuration** perspective provide access to the **Add Thresholds to Notification Policy** option:

- Right-click menu **Add Thresholds to Notification Policy** in the **Navigation** view.
- Right-click menu **Add Thresholds to Notification Policy** in the **Threshold Alarm Configuration** view.

Remove Thresholds from Notification Policy option

This option allows you to remove thresholds for the selected device group or device from a policy used by the Data Center Expert server to generate alarm notifications.

In the **Alarm Configuration** perspective, you can select device groups, devices, or thresholds and remove the thresholds for that selection from an existing notification policy. When one or more device groups or devices are selected, all the thresholds for that selection will be removed from the selected notification policy.

Two menus in the **Alarm Configuration** perspective provide access to the **Remove Thresholds from Notification Policy** option:

- Right-click menu **Remove Thresholds from Notification Policy** in the **Navigation** view.
- Right-click menu **Remove Thresholds from Notification Policy** in the **Threshold Alarm Configuration** view.

Show Notification Policy option

This option allows you to view the names of the notification policies to which the selected threshold is added.

In the Threshold Alarms Configuration view in the **Alarm Configuration** perspective, you can select a threshold and view the notification policies to which it is added.
Note: When more than one threshold is selected, every notification policy to which those thresholds are added is shown.

The right-click menu in the **Threshold Alarm Configuration** view provides access to the **Show Notification Policy** option.

Find Device in Navigation Tree option

This option allows you to select a threshold and locate the device associated with it in the **Navigation** view.

In the **Alarm Configuration** perspective, with a device group selected in the **Navigation** view, you can select a threshold in the list and locate the device associated with it.

The right-click menu in the **Threshold Alarm Configuration** view provides access to the **Find Device in Navigation Tree** option.

Threshold Alarm Configuration view

This view in the **Alarm Configuration** perspective shows user-created threshold alarms, and communication link status alarms, and that can be configured for the device groups and devices selected in the **Navigation** view.

You can select a device group or device in the **Navigation** view to display the thresholds in the **Threshold Alarm Configuration** view that can be configured or added to a notification policy for that selection. The number of thresholds associated with each device group or device is shown next to the threshold type or threshold, in parentheses.

You can use the **Search** fields to filter the list based on text you enter in the Navigation or Threshold Alarm Configuration views; only items that contain the text you type are listed.

When the results of a search are displayed, the background of the search field is shaded. When you clear the search field, the background shading is removed and all items are displayed.
Note: You can hold the Ctrl key down to select multiple items.

You can use the right-click options and the button icons at the top of the view to do the following:

- Edit the thresholds for the device group or device selected (**Edit Thresholds** option).
- Remove one or more thresholds from the list (**Delete Thresholds** option).
- Create a new notification policy and add one or more thresholds for the selected device group or device (**Add Thresholds to New Notification Policy** option).
- Add one or more thresholds for the selected device group or device to an existing notification policy (**Add Thresholds to Notification Policy** option).
- Remove one or more thresholds from a notification policy for the selected device group or device (**Remove Thresholds from Notification Policy** option).

- Show the notification policy to which a threshold is assigned (**Show Notification Policy** option).
- Locate a device in the navigation tree from the thresholds list (**Find Device in Navigation Tree** option).
- Access the "Configure Columns" display to select the attribute columns that appear in the list (**Configure Columns** icon ( )).
- Enable filters that hide various threshold types and attributes. (**Filter Thresholds** icon ( )).

Modifying thresholds

All thresholds use the same basic procedure and displays to modify threshold settings.

Note: The same displays are used to modify the threshold settings regardless of whether you select:

- **Edit Threshold**, a right-click option in the **Alarm Configuration** perspective.
- **Edit Alarm Configuration**, a right-click option in the **Active Alarms** view in the **Monitoring** perspective.

Modifying thresholds in the Alarm Configuration perspective

1. In the **Alarm Configuration** perspective, select a device group, device, or threshold, right-click to select **Edit Thresholds**, and select the threshold type you want to modify from those defined for the selection.

   Note: If you selected **Other Numeric Sensors** or **Other State Sensors** to modify multiple thresholds simultaneously, the unit of measure for all selected thresholds must be the same.
2. In the "Edit Thresholds" display, define the threshold settings, and click **OK**.

Modifying thresholds in the Active Alarms view

1. In the **Active Alarms** view in the **Monitoring** perspective, select an alarm, and right-click to select **Edit Alarm Configuration**.
2. Select **This Instance** to modify the threshold on the device reporting the selected alarm only, or select **All Instances** to simultaneously modify the threshold on every device on which it is defined, regardless of whether those devices are currently reporting an alarm.
3. Click **OK**.

Delete Thresholds option

This option allows you to delete thresholds for any sensor on any device.

You select a device group or device in the **Navigation** view of the **Alarm Configuration** perspective to view the thresholds for that selection in the **Threshold Alarms Configuration** view. You can then select any thresholds, with the exception of communication link status thresholds, and delete them from the thresholds list. The thresholds will also be deleted from any notification policy to which they were added.
Note: You can filter the list to view only certain thresholds (**Filter Thresholds** icon).

You access the **Delete Thresholds** option from the right-click menu in the **Threshold Alarms Configuration** view. When one threshold is selected, only that threshold is deleted. When multiple thresholds are selected, they are deleted simultaneously.
Note: Only user-created alarm thresholds can be deleted. Communication link status thresholds are never deleted, regardless of whether they are included in the selection.

Button icons (Threshold Alarm Configuration view)

In addition to standard minimize and maximize icons, two icons are available to perform specific **Threshold Alarm Configuration** view functions.

Icon	Description
	Use this **Configure Columns** icon to identify the attribute columns that appear in the **Threshold Alarm Configuration** view.
	Use this **Filter Thresholds** icon to enable filters that prevent communication link status and user-created thresholds, thresholds with 'Enabled' set to 'No', and thresholds of any severity, from appearing in the list.

"Configure Threshold Attribute Columns" display

Use this display to identify the columns that appear in the **Threshold Alarm Configuration** view.

Section	Description
Threshold Attribute Columns	Lists all possible threshold attribute columns that can appear in the view. **Threshold**: Identifies the threshold. **Severity**: The severity associated with the threshold. **Label**: The label of the device **Hostname**: The hostname, or IP address, if no hostname is defined. **Enabled**: Whether or not the threshold is enabled. **Device Model**: The device model, if known. For example, Symmetra PX, for an APC/ MGE UPS. **Device Type**: The type of device

	Name: The name of the threshold. **IP Address**: The IP address of the device. **Notification Policy**: The name of the notification policy or policies to which the alarm is added. **Sensor**: Identifies the sensor associated with the alarm. **Sensor Type**: The type of sensor. **Parameters**: The settings defined on the sensor.

"Filter Thresholds" display

Use this display to select the types of thresholds to exclude from the **Thresholds** view.

Device Alarm Configuration view

This view in the **Alarm Configuration** perspective shows device alarms that can be configured for the device groups and devices selected in the Navigation view.

You select a device group or device in the **Navigation** view to display the device alarms that can be configured for that selection in the **Device Alarm Configuration** view. The device alarms associated with each device group or device are displayed by alarm type, then by alarm name, then by device. The number of device alarms associated with each device group or device is shown next to the alarm type or alarm, in parentheses.

You can select one or more device alarm types, alarm names, or alarm by device and modify the alarm configuration. You can disable or enable alarms, modify the severity, add a custom description, or modify the recommended action.
Note: For additional alarm configuration, you can access the web interface for the device.

All device alarms for all devices are added to the **Default** notification policy at device discovery. You use the **Change Device Alarm Notification Policy** option in the right-click menu of the **Navigation** view to change the notification policy associated with a device.

You can use the "Edit Notification Policy" display, accessed from the **Edit** option in the **Notification Policies** view, to add and remove a device group or device from a notification policy. All the device alarms available for the selected device group or device are added or removed simultaneously.

You can use the **Search** fields to filter the list based on text you enter in the Navigation or Device Alarm Configuration views; only items that contain the text you type are listed.

When the results of a search are displayed, the background of the search field is shaded. When you clear the search field, the background shading is removed and all items are displayed.
Note: You can hold the Ctrl key down to select multiple items.

You can use the right-click options and the button icons at the top of the view to do the following:

- Enable or disable, modify the severity and recommended action, and add a custom description on one or more alarms for the device group or device selected (**Edit Device Alarm Configuration** option).

- Locate a device in the Navigation view from the device alarm list (**Find Device in Navigation Tree** option).
- Show all the device alarms for the alarm type selected (**Expand Selection** option).
- Access the "Configure Columns" display to select the attribute columns that appear in the list (**Configure Columns** icon ( )).
- Enable filters that hide various device alarm attributes. (**Filter Device Alarms** icon ( )).

Modifying device alarms

All device alarms use the same basic procedure and displays to modify the device alarm configuration.

Note: The same display is used to modify the device alarm configuration regardless of whether you select:

- **Edit Device Alarm Configuration**, a right-click option in the **Navigation** view in the **Alarm Configuration** perspective.
- **Edit Device Alarm Configuration**, a right-click option in the **Device Alarm Configuration** view in the **Alarm Configuration** perspective.
- **Edit Alarm Configuration**, a right-click option in the **Active Alarms** view in the **Monitoring** perspective.

Modifying device alarms in the Alarm Configuration perspective

1. Select a device group or device in the **Navigation** view of the perspective, or select a device alarm type, alarm name, or alarm by device in the **Device Alarm Configuration** view of the **Alarm Configuration** perspective. Right-click to select **Edit Alarm Configuration**.
2. In the "Edit Device Alarm Configuration" display, define the alarm settings, and click **OK**.

Modifying device alarms in the Active Alarms view

1. In the **Active Alarms** view in the **Monitoring** perspective, select an alarm, and right-click to select **Edit Alarm Configuration**.
2. Select **This Instance** to modify the device alarm configuration on the device reporting the selected alarm only, or select **All Instances** to simultaneously modify the configuration on every device for which that alarm is defined, regardless of whether those devices are currently reporting an alarm.
3. Click **OK**.

"Edit Device Alarm Configuration" display

This display allows you to specify how device alarms reported by monitored SNMP or Modbus devices are displayed in Data Center Expert. You can modify severity and recommended action, add a custom description, and disable or reenable device alarms for the device groups, devices, or device alarms selected.

You access the display from the right-click menu in the **Device Alarm Configuration** view or the **Navigation** view in the **Alarm Configuration** perspective.

When you access the display from the **Navigation** view, all the device alarms associated with the device groups or devices selected are configured simultaneously.

When you access the display from the **Device Alarm Configuration** view, you can specify which device alarms associated with the device groups or devices you selected in the **Navigation** view to configure. You can expand the selection to view and configure device alarms by alarm type, alarm name, or by one or more devices reporting that alarm.
Note: With the exception of the **Enabled** option, device alarm settings you modify do not apply to active alarms. The modified settings will apply the next time the alarm is triggered.

Element	Description
Enabled	Select to enable the device alarm, if it is disabled. **Note:** Device alarms are enabled by default.
Severity	Select the severity you want associated with the device alarm: **Information**, **Warning**, **Error**, **Critical**, or **Failure**.
Description	The alarm description provided by the device. You cannot modify this description.
Custom Description	Provide a description you want included in the device alarm notifications.
Recommended Action	The recommended action provided by the device. You can modify the recommended action to include instructions you want in the device alarm notifications.
Reset to default	Reset the recommended action to default, if it has been modified.

Button icons (Device Alarm Configuration view)

In addition to standard minimize and maximize icons, two icons are available to perform specific **Device Alarm Configuration** view functions.

Icon	Description
	Use this **Configure Columns** icon to identify the attribute columns that appear in the **Device Alarm Configuration** view.
	Use this **Filter Device Alarms** icon to enable filters that prevent device alarms with 'Enabled' set to 'No', and device alarms of any severity, from appearing in the list.

"Filter Device Alarms" display

Use this display to select the types of device alarms to exclude from the **Device Alarm Configuration** view.

"Configure Device Alarm Attribute Columns" display

Use this display to identify the columns that appear in the **Device Alarm Configuration** view.

Section	Description
Device Alarm Attribute Columns	Lists all possible device alarm attribute columns that can appear in the view. **Device Alarm**: Identifies the device alarm. **Severity**: The severity associated with the device alarm. **Label**: The label of the device. **Hostname**: The hostname, or IP address, if no hostname is defined. **Enabled**: Whether or not the device alarm is enabled. **Device Model**: The device model, if known. For example, Symmetra PX, for an APC/ MGE UPS. **Device Type**: The type of device. **IP Address**: The IP address of the device. **Notification Policy**: The name of the notification policy or policies to which the alarm is added. **Device Definition File**: The file the **Data Center Expert** server uses to access information about the environmental, power, and cooling alarms at supported SNMP and Modbus devices.

Notification Policies View

This view in the **Alarm Configuration** perspective shows the default and user-created notification policies.

You can create your own custom notification policies for the Data Center Expert server, and edit existing policies used to generate alarm notifications. A **Default** notification policy exists for the Data Center Expert server. This default notification policy cannot be deleted, but it can be edited and renamed.

Note: A notification policy must include at least one threshold or device and one alarm action before it can be used to generate alarm notifications.

You can use the button icons and the right-click options at the top of the view to perform the following functions:

- Create a new notification policy, and add one or more alarm actions, and one or more thresholds and devices, for the selected device group or device (**Create** option and icon).
- Edit the thresholds, devices, and alarm actions for the selected notification policy (**Edit** option and icon).
- Delete the selected notification policy (**Delete** option and icon).
- Add, edit, delete, and test alarm actions for the selected notification policy using the "Manage Alarm Actions" display (**Manage Alarm Actions**).

Button icons (Notification Policies view)

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

Icon	Description
	Use the **Create Notification Policy** icon to create a new notification policy. **Note:** A notification policy must include at least one threshold or device and one alarm action before it can be used to generate alarm notifications.
	Use the **Edit Notification Policy** icon to choose thresholds or devices to add or remove, and to add, edit, or remove alarm actions in the notification policy selected.
	Use the **Delete Notification Policy** icon to delete the notification policy selected.
	Use the **Manage Alarm Actions** icon to add, edit, delete, or test alarm actions for the notification policy selected.

Create Notification Policy option

This option allows you to create a policy used by the Data Center Expert server to generate alarm notifications.

In the **Notification Policies** view of the **Alarm Configuration** perspective, you can create a new notification policy, and choose the thresholds, and SNMP and Modbus devices, to include in the new policy; view the thresholds and devices you have added, and add alarm actions and configure options for those actions.
Note: A notification policy must include at least one threshold or device and one alarm action before it can be used to generate alarm notifications.

The right-click menu **Create** in the **Notification Policy Name** list, and the **Create Notification Policy** icon ( ) in the **Notification Policies** view, provide access to the "Create New Notification Policy" display.

Creating a New Notification Policy

In the **Alarm Configuration** perspective, you can create a new notification policy in the **Notification Policies** view. You select any existing notification policy, or use the **Create Notification Policy** icon , to create a new notification policy.

A notification policy must include at least one threshold or device, and one alarm action before it can be used to generate alarm notifications. No thresholds or actions are included by default in a new notification policy.

1. Select the **Create Notification Policy** icon or right-click option in the **Notification Policies** view.
2. In the "Create New Notification Policy" display, identify a policy name, choose the thresholds, devices, and actions to add to the notification policy.
   a. Click **Add** to configure the alarm actions to add to the notification policy. Click **Manage Actions** to create alarm actions, or modify or remove existing alarm actions on the Data Center Expert server. Check-mark one or more actions to configure their notification options, check-mark the actions you want to add to the notification policy, and click **OK** .
   b. On the Thresholds tab, click **Choose Thresholds** to identify the thresholds you want to add to the notification policy. In the "Choose Thresholds" display, you select a device group or device, select the thresholds you want to add to the notification policy, and click the **Add Selected Thresholds** button. Use the **Remove Selected Thresholds** to refine the list. Click **OK** to exit the display.

      Note: You can modify thresholds in the **Threshold Alarm Configuration** view in the **Alarm Configuration** perspective.
   c. On the Devices tab, click **Choose Devices** to identify the devices you want to add to the notification policy. In the "Choose Devices" display, you select a device group or device you want to add to the notification policy, and click **OK**.

      Note: All device alarms reported by the device or device group selected will be added to the notification policy. You can modify the alarm configuration for alarm types or individual device alarms in the **Device Alarm Configuration** view in the **Alarm Configuration** perspective.
3. Modify the alarm actions, thresholds, or devices you have added to the notification policy, if necessary, or click **OK** to exit the display.

"Create New Notification Policy/Edit Notification Policy" display

Use this display to create a new notification policy or edit an existing notification policy used by the Data Center Expert server to generate alarm notifications.

A **Default** notification policy exists for the Data Center Expert server. This default notification policy cannot be deleted, but it can be edited and renamed.
Note: A notification policy must include at least one threshold or device and one alarm action before it can be used to generate alarm notifications.

Three menus and one button icon in the **Alarm Configuration** perspective provide access to the **Create New Notification Policy** display:

- Right-click menu **Create** in the **Notification Policy Name** pane of the **Notification Policies** view.
- Button icon **Create Notification Policy** in the **Notification Policies** view.
- Right-click menu **Add Thresholds to Notification Policy** in the **Navigation** view.
- Right-click menu **Add Thresholds to Notification Policy** in the **Threshold Alarm Configuration** view.

One menu and one button icon in the **Notification Policies** view provide access to the **Edit Notification Policy** display:

- Right-click menu **Edit** in the **Notification Policy Name** pane.
- Button icon **Edit Notification Policy** ( ).

Element	Description
Policy Name	Identify the name of the notification policy.
Actions	Displays the actions and action options included in the notification policy. You can click on any column head (**Action**, **Delay (min), Repeat**, or **Interval (min)**) to sort the list.
Add	Click to add actions to the notification policy. **Note:** To add alarm actions, use the "Manage Alarm Actions" display, accessed by the **Manage Actions** button.
Edit	Click to edit the options for the selected alarm action. **Note:** To edit alarm actions, use the "Manage Alarm Actions" display, accessed by the **Manage Actions** button.
Remove	Click to delete an action from the notification policy. **Note:** The action is deleted from the notification policy only, and remains on the Data Center Expert server for future use. To delete alarm actions from the Data Center Expert server, use the "Manage Alarm Actions" display, accessed by the **Manage Actions** button in the Add and Edit Alarm Action displays, or the **Manage Alarm Actions** option in the **Alarm Configuration** menu.
Thresholds	Displays the thresholds included in the notification policy.
Choose Thresholds	Click to select thresholds to include in the notification policy.
Devices	Displays the devices included in the notification policy.
Choose Devices	Click to select devices to include in the notification policy

"Add or Edit Alarm Action" display

This display allows you to create or modify alarm actions for the notification policy selected.

Element	Description
List	The alarm actions on the Data Center Expert server.
Manage Actions	Accesses the "Manage Alarm Actions" display to create, modify, or delete alarms from the Data Center Expert server.
Options	**Delay (minutes)**: Define how long the Data Center Expert server will wait to generate a notification after it becomes aware of an alarm. **Repeat (number of times)**: Specify how often the notification policy will repeat the alarm action. **Repeat Until Alarm Clears**: Select to repeat the notification until the alarm condition is resolved. **Interval (minutes)**: Define how long the notification policy will wait before it repeats the alarm action. **Include graph (if supported)**: Select to include graphs in the notification, available for threshold alarms only.

"Choose Thresholds" display

This display allows you to select the thresholds that will be part of a new or existing notification policy.

You select a device group or device in the navigation tree to display the thresholds that can be added to the notification policy for the selection.

You can add all the thresholds, or choose only those thresholds you want to add to the notification policy.
Note: You can hold the Ctrl key down to select multiple items in both the navigation tree and the thresholds list.

The number of thresholds in the notification policy is displayed. You must click **OK** in the "Choose Thresholds" display, and the "Create or Edit Notification Policy" display to apply your changes.

You can use the search feature, table columns, and button icons to do the following:

- Type text in the **Search** field to filter the navigation tree or the thresholds list. You can broaden or narrow your search using the Boolean operators AND, OR and NOT. Only items that contain the text you specify in the **Search** field are displayed. When the results of a search are displayed, the background of the search field is shaded. When you clear the **Search** field, the background shading is removed and all items are displayed.
  Note: **Search** fields support the Boolean operators AND, OR, and NOT only.
- Access the "Configure Navigation Tree Labels" display to select up to three labels to specify how monitored devices appear in the navigation tree (**Configure Navigation Tree Labels** icon).

Note: Changes to the navigation tree labels in this display affect the navigation tree in the **Navigation** view.

- Access the Configure Columns display to select the attribute columns that appear in the list. (**Configure columns** icon).
  Note: Changes to the columns in this display affect the columns in the **Thresholds** view.
- Enable filters to specify the threshold attributes that appear in the list (**Filter Thresholds** icon).
- Click a column title to sort the list in ascending or descending order based on that column's information.

The **Add Selected Thresholds** and **Remove Selected Thresholds** buttons are used to add thresholds to or remove thresholds from the notification policy. When you add thresholds to the notification policy, a 'plus-sign' icon ( ) indicates which thresholds were added. When you remove a threshold from the notification policy, the icon is removed.
Note: When you remove thresholds from the notification policy, the thresholds remain in the list for the device group or device, and can be readded, if desired.

"Choose Devices" display

This display allows you to select the devices that will be part of a new or existing notification policy.

You checkmark the device groups or devices in the navigation tree to add all the alarms reported by the devices for that selection to the notification policy. You can then modify the configurations for individual device alarms in the **Device Alarm Configuration** view.
Note: All the devices monitored by the Data Center Expert server are added to the **Default** notification policy at device discovery.

Note: You must click **OK** in the "Choose Devices" display, and the "Create or Edit Notification Policy" display to apply your changes.

You can use the search feature to do the following:

- Type text in the **Search** field to filter the navigation tree or the thresholds list. You can broaden or narrow your search using the Boolean operators AND, OR and NOT. Only items that contain the text you specify in the **Search** field are displayed. When the results of a search are displayed, the background of the search field is shaded. When you clear the **Search** field, the background shading is removed and all items are displayed.
  Note: **Search** fields support the Boolean operators AND, OR, and NOT only.

Edit Notification Policy option

This option allows you to edit a notification policy used by the Data Center Expert server to generate alarm notifications.

In the **Notification Policies** view of the **Alarm Configuration** perspective, you can select a notification policy, and change the policy name, choose the thresholds and devices to include in the notification policy; and add, edit, and remove alarm actions.
Note: A notification policy must include at least one threshold or device and one alarm action before it can be used to generate alarm notifications.

The right-click menu **Edit** in the **Notification Policy Name** list, and the **Edit Notification Policy** icon of the **Notification Policies** view, provide access to the "Edit Notification Policy" display.

Delete Notification Policy option

This option in the Alarm Configuration perspective allows you to delete a notification policy used by the Data Center Expert server to generate alarm notifications.

The right-click menu **Delete** in the **Notification Policy Name** list, and the **Delete Notification Policy** icon ( ) of the **Notification Policies** view, allow you to delete the selected notification policies.

Note: The **Default** notification policy cannot be deleted.

Manage Alarm Actions option (Alarm Configuration menu)

This option allows you to create, modify, delete, and test the alarm actions that can be included in the notification policies the Data Center Expert server uses to generate alarm notifications.

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

- A threshold violation at a sensor the Data Center Expert server monitors.
- An alarm at a monitored SNMP or Modbus device.

You can create multiple versions of an alarm action, each with unique settings, for example, assigning different severities that apply to the alarm action.

Once alarm actions have been created, you must add at least one action, and one alarm or threshold, to at least one notification policy to generate alarm notifications.
Note: Device alarms for every device the Data Center Expert server monitors are added to the **Default** notification policy at discovery. You must manually add alarm actions to this policy before the Data Center Expert server can use it to generate alarm notifications.

Two displays, "Add Alarm Action" and "Edit Alarm Action" in the **Notification Policies** view, also provide access to the **Manage Alarm Actions** display.

"Manage Alarm Actions" display

Use this display to create, modify, delete and test alarm actions that can be included in policies used by the Data Center Expert server to generate alarm notifications.

Type	Description
List	Displays the alarm actions currently configured on the Data Center Expert server. You can click any column head (**Action** or **Action Type**) to sort the list.
Create	Click to create a new alarm action.
Edit	Click to edit the selected alarm action.
Delete	Click to delete the selected alarm action from the Data Center Expert server.
Test	Click to test the selected alarm action.

Manage Alarm Actions

You use the "Alarm Action" wizard to create alarm actions that can be included in the notification policies used by the Data Center Expert server for alarm notifications.

Creating an alarm action

You must create at least one alarm action, and add it to a notification policy, before your Data Center Expert server can generate alarm notifications.

All alarm actions are created using the same basic procedure.

1. Select **Manage Alarm Actions** in the **Alarm Configuration** menu.
2. Click **Create** to access the Alarm Action wizard.
3. In the "Choose Alarm Action Type" display, select the type of alarm action you want to create, and click **Next**.
4. In the "Configure Alarm Action" display for the selected action, define the settings you want the action to use, and click **Finish** to exit the wizard.

   Note: For information about the settings for the action you are creating, see the help section for that action and its settings display.

Modifying an alarm action

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

All alarm actions are modified using the same basic procedure.

1. Select **Manage Alarm Actions** in the **Alarm Configuration** menu.
2. Select the alarm action you want to modify, and click **Edit** to access the configuration display for that action.
3. Define the settings you want the action to use, and click **Finish** to exit the wizard.

   Note: For information about the settings for the action you are creating, see the help section for that action and its settings display.

Deleting an alarm action

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

All alarm actions are deleted using the same basic procedure.

1. Select **Manage Alarm Actions** in the **Alarm Configuration** menu.
2. Select the alarm action you want to remove, and click **Delete** .
3. Click **Finish** to exit the wizard.

   Note: Deleting an alarm action in the Manage Alarm Actions display removes the action from the Data Center Expert server.

Testing an alarm action

You can test alarm actions to ensure that your Data Center Expert server can generate alarm notifications.

All alarm actions are tested using the same basic procedure.

1. Select **Manage Alarm Actions** in the **Alarm Configuration** menu.
2. Select the action you want to test, click **Test**, and then click **OK**.

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.

"Choose Alarm Action Type" display

Use this display to select the type of action you want to create.

Alert Action	Description
Send E-mail	Sends a message that uses the standard e-mail format.
Send Short Message E-mail	Sends a message that uses the short-message e-mail format.
Send Data to FTP Server	Sends data to an FTP server.
Send HTTP POST	Sends an HTTP POST.
Send SNMPv1 Trap	Sends an SNMPv1 trap.
Send SNMPv3 Inform	Sends an SNMPv3 inform.

"Alarm Action" displays

Each type of alarm action has its own configuration display.

Common alarm action settings

All alarm action types share a name field, severity selections, and an "Alarm Action Scheduling" display.

Alarm action severity settings

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

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

- An alarm action named "send_user1_sms” is created, and defined to send User1 an SMS e-mail for critical events only.
- The “send_user1_sms” action is added to a notification policy called “sms messaging.”
- The "sms messaging" notification policy includes various thresholds and device alarms. The alarms 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 thresholds and device alarms defined as critical.

You must select at least one severity.

Severity	Description

Information	Typically used to set up an alarm 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 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 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.

"Alarm Action Schedule" 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 alarm action will be enabled and disabled, using the action's 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 alarm action 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.

"Send E-mail" display

Use this display to define the settings for a **Send E-mail** alarm action on the Data Center Expert server.

A name field, severity selections, and the "Alarm Action Scheduling" display that all alarm action types share, are also available.
Note: Make sure the Data Center Expert server's SMTP settings 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.
Server E-mail Settings	Select to define the SMTP settings on the Data Center Expert server.
Locale	Select to specify the locale to be used when sending email messages or **Use Server Locale** (the default).

Advanced Options tab

Provides elements that further define what an e-mail can include, as well as an **Alarm Action Scheduling** button that allows you to select when an alarm 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 or alarm condition returns to normal.
Minimize Header Usage	Select to minimize the size of the e-mail headers.

"Send Short Message E-mail" display

Use this display to define the settings for a **Send Short Message E-mail** alarm action on the Data Center Expert server.

A name field, severity selections, and the "Alarm Action Scheduling" display that all alarm action types share, are also available.
Note: Make sure the Data Center Expert server's SMTP settings 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.
Subject	Enter a subject for the message; macros can be used.
Message	Enter a message; macros can be used.
Server E-mail Settings	Select to define the SMTP settings on the Data Center Expert server.
Locale	Select to specify the locale for email messages or **Use Server Locale** (the default).

Advanced tab

Provides elements that further define what an e-mail can include, as well as an **Alarm Action Scheduling** button that allows you to select when an alarm 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 or alarm condition 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 Data to FTP Server" display

Use this display to define the settings for a **Send Data to FTP Server** alarm action on the Data Center Expert server.

A name field, severity selections, and the "Alarm Action Scheduling" display that all alarm 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. Alarm data will be stored in a file with this name, followed by the *.nbalert.xml file extension. **Note:** This **Base Filename** field accepts macros.

"Send HTTP POST" display

Use this display to define the settings for a **Send HTTP POST** alarm action on the Data Center Expert server.

A name field, severity selections, and the "Alarm Action Scheduling" display that all alarm 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.

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 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 **Alarm Action Scheduling** button that allows you to select when an alarm action is enabled (all time periods are enabled, by default).

Setting	Description
SSL Verify Options	Select **No verification**, **Verify certificate**, or **Verify certificate and hostname** for HTTP POSTs.

"Send SNMPv1 Trap" display

Use this display to define the settings for a **Send SNMPv1 Trap** alarm action on the Data Center Expert server.

A name field, severity selections, and the "Alarm Action Scheduling" display that all alarm 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.
Locale	Select to specify the locale to be used when sending SNMP traps or **Use Server Locale** (the default).

"Send SNMPv3 Inform" display

Use this display to define the settings for a **Send SNMPv3 Inform** alarm action on the Data Center Expert server.

A name field, severity selections, and the "Alarm Action Scheduling" display that all alarm 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 informs will be sent.
Authentication User ID	Identify the user identification to be used when sending SNMPv3 informs to the target NMS.
Authentication Protocol	Select **SHA-1** or **MD5** as the protocol 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.
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.
Inform Port Number	Identify the number of the port that the target NMS identified in the **Primary** tab uses to receive SNMPv3 informs.
Locale	Select to specify the locale to be used when sending SNMP v3 informs or **Use Server Locale** (the default).

Macros for alarm action settings

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

Location macros

One location macro is available for use when defining alarm action settings for SNMP and Modbus devices monitored by the Data Center Expert server.

Macro	Definition	Example
${LOCATION}	The location for a Data Center Expert SNMP or Modbus device.	Test Lab

Identification macros

Identification macros are available for use when defining alarm action settings for SNMP and Modbus devices monitored by the Data Center Expert server.

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.	device.apc.com
${MODEL}	The model of the device.	Symmetra 80K
${SERVERIP}	The dotted-decimal IP address of the **Data Center Expert** server.	192.168.2.10
${SERVERHOSTNAME}	The hostname of the **Data Center Expert** server.	isxc.apc.com
${SERVERMODEL}	The model of the **Data Center Expert** server.	**Data Center Expert**
${TIMESTAMP}	The current UTC time (seconds since 1/1/1970).	998885130
${DATE}	The current date (year-month-day).	2010-03-27
${YEAR}	The current year.	2010
${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

Alarm macros

Alarm macros are available for use when defining alarm action settings on the Data Center Expert server.

Macro	Definition	Example
${ALERTTYPE}	The type of alarm.	HIGHERR
${ALERTTYPENAME}	The ${ALERTTYPE} value, displayed in the language appropriate for the Data Center Expert server locale.	Value Too High
${SENSORTYPE}	The type of sensor generating the alarm.	TEMP
${SENSORVAL}	The value reported by the sensor that is generating the alarm.	60
${SENSORVAL_NOLABEL}	The value reported by the sensor generating the alarm, excluding special characters.	81.2 rather than 81.2 ° F
${ALERTTIME}	The date and time at which the alarm notification was generated.	Apr 2, 2009 13:01:45
${ALERTSEV}	The severity value reported by the sensor that is generating the alarm (such as ERR, WARN, INFO). If the alarm state has returned to normal, the severity value will be followed by "-RTN" (for example WARN-RTN).	ERR, WARN-RTN
${ALERTSEVNAME}	The ${ALERTSEV} value, displayed in the language appropriate for the Data Center Expert server locale.	ERROR, WARN (returned to normal)
${SENSORNAME}	The name of the sensor associated with the alarm.	Bldg. 3 Door
${NOTIFPOLICY}	The name of the notification policy that was used to generate the alarm.	Default, Policy #1
${ALERTTITLE}	The alarm title.	Replacement Battery Needed
${ALERTDESC}	The description, and recommended action, if any, for the alarm.	At least one faulty battery exists. Recommended Action: Replace all faulty batteries. You can use the APC Selectors (http://www.apc.com/go/direct/index.cfm?tag=selectors) page to order new batteries.
${ISACTIVE?yes?no}	Specifies custom active vs. return to normal text. The strings “yes” and “no” can be replaced with user-specified	“active” and “cleared”

	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.	
${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 alarm condition was initially detected.	13:01:45
${RESOLVE_TIME}	The time at which the alarm condition returned to normal.	13:07:13
${SENSORLUID}	The locally unique ID of the sensor generating the alarm.	TEMP1
${SENSORGUID}	The globally unique ID of the sensor generating the alarm.	B000113_TEMP1
${EVENTID}	The unique 16 character identifier shared by all messages generated as a result of a single alarm notification event. For example, if an appliance generates an alarm notification when the internal temperature sensor threshold is exceeded, and then generates a "return to normal" message when the temperature drops below the high threshold, both of these messages will have the same Event ID number. However, if the temperature rises again and a second threshold exceeded alarm is generated, the second alarm will have a new Event ID.	3E4512C0FE03440F
${DEVICELABEL}	The label of value of the device that either contains the sensor that reported the alarm or to which the sensor is connected.	My Device
${ALERTPOD}	The label of value of the pod that either contains the sensor that reported the alarm or to which the sensor is connected.	My Pod
${ALERTPODSERIAL}	The serial number of the pod that either contains the sensor that reported the alarm or to which the sensor is connected.	NB007100730114
${ALERTPORT}	The label value for the external sensor port to which the	Ext1

	external sensor that reported the alarm is connected.	
${CURRENT_ALERT_NUM}	The number of times the alarm action has been repeated, from 0 up to the Repeats value for the alarm action.	0, 1, 2
${RESOLVEUSERID}	The user ID that is responsible for manually resolving an alarm (when this option applies).	joeuser
${RESOLVECOMMENT}	The text entered into the user-specified description field whenever an alarm 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”

Alert Settings option

Provides options used to configure how NetBotz Appliances report alarm conditions.

NetBotz Appliance Alert Notifications overview

The NetBotz Appliances monitored by the Data Center Expert server each generate their own alert notifications in response to alert threshold violations that occur at the devices they monitor.

The NetBotz appliance stores its threshold settings and sends alert notifications to the Data Center Expert server. The **Alert Settings** options in the **NetBotz Appliance Configuration** option of the **Device** 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 NetBotz Appliance 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 NetBotz Appliance can generate alert notifications.
- **Alert Thresholds**: Used to define threshold settings that the 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 for monitored NetBotz Appliances.

The alert notifications can alert you, or other members of your organization, when a sensor threshold violation, or other alarm condition, occurs at a monitored NetBotz Appliance.
Note: A default alert profile exists for notifications associated with each NetBotz Appliance.

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 can use the "Alert Actions" wizard to create, modify, or delete the alert actions used in alert profiles as part of the alert notifications used only by monitored NetBotz Appliances.

Creating an alert action

You must create at least one alert action before your NetBotz Appliance can generate alert notifications.

All alert actions are created using the same basic procedure.

1. Select **Alert Actions** in the **Alert Settings** option in the **NetBotz Appliance Configuration** option in the **Device** 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 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 **Alert Settings** option in the **NetBotz Appliance Configuration** option in the **Device** 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 **Alert Settings** option in the **NetBotz Appliance Configuration** option in the **Device** 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 Settings** in the **NetBotz Appliance Configuration** option of the **Device** menu, is used to manage the alert actions for NetBotz Appliances.

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: Each NetBotz Appliance is the parent device for its camera pods, sensor pods, and other devices it monitors.

Parent Device	Description
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 "Alert Action 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 to indicate a condition exists that may require attention to make sure it does not deteriorate into a critical state.
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 to indicate an operational failure requires immediate attention.
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.

"Alert Action 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 surveillance activity on a camera can also be scheduled directly on the NetBotz Appliance, and in the Data Center Expert client **Surveillance** perspective. The camera will not capture data when either the Data Center Expert 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 a NetBotz Appliance.

A name field, severity selections, and the "Alert Action Scheduling" display that all alert action types share, are also available.
Note: Make sure the SMTP settings for the monitored NetBotz Appliances are 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 the NetBotz Appliance 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 **Alert Action Scheduling** button that allows you to select when an alert action is enabled (all time periods are enabled, by default).

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 "Alert Action 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 a NetBotz Appliance.

A name field, severity selections, and the "Alert Action 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 a NetBotz Appliance.

A name field, severity selections, and the "Alert Action 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 **Alert Action 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 a NetBotz Appliance.

A name field, severity selections, and the "Alert Action Scheduling" display that all alert action types share, are also available.
Note: Make sure the SMTP settings for the monitored NetBotz Appliances are 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 NetBotz Appliance 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 **Alert Action 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 a NetBotz Appliance.

A name field, severity selections, and the "Alert Action 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 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 **Alert Action Scheduling** button that allows you to select when an alert action is enabled (all time periods are enabled, by default).

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.

	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 Data to FTP Server** alert action on a NetBotz Appliance.

A name field, severity selections, and the "Alert Action 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 **Alert Action Scheduling** button that allows you to select when an alert action is enabled (all time periods are enabled, by default).

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. **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 "Alert Action 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 **Alert Action 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 "Alert Action 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 "Alert Action 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:

Identification macros are available for use when defining alert action settings for NetBotz Appliances.

Macro	Definition	Example
${SERIAL}	The serial number of the device.	5A0902V00025
${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).	2009-03-27
${YEAR}	The current year.	2009
${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:

Location macros are available for use when defining alert action settings for NetBotz Appliances.

Macro	Definition	Example
${LOCATION}	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 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, 2009 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 drops below the high threshold, both of these messages will have the same Event ID number. However, if the temperature rises again and a second threshold exceeded alert is generated, the second alert will have a new Event ID.	3E4512C0FE03440F
${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 NetBotz Appliances use to generate alert notifications.

A default alert profile exists 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 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. This is completely separate from the alarm actions, thresholds, and notification policies that are created on the Data Center Expert server in the Alarm Configuration perspective, and stored on the Data Center Expert server.

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

Alarm type	Profile
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 by the NetBotz Appliance 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.
- 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 **Alert Settings** option in the **NetBotz Appliance Configuration** option in the **Device** menu.
2. In the "Select Parent Device" display, highlight the parent device (the individual NetBotz Appliance) associated with the profile you want to configure, and click **Next**.

   Note: Only one parent device can be selected: 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, the alert threshold 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: 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
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, the alert threshold 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 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 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 the NetBotz Appliance 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**.
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 Data Center Expert allows you to create alert threshold settings for any sensor value reported for monitored NetBotz Appliances.

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

- Numeric thresholds:
  - **Air Flow**
  - **Audio**
  - **Current (Amps)**
  - **Dew Point**
  - **Humidity**
  - **Other Numeric Sensors**
  - **Power (VA)**
  - **Power (Watts)**
  - **Temperature**
  - **Voltage**
- State thresholds:
  - **Door**
  - **Door (Handle)**
  - **Door (Lock)**
  - **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 monitored by the Data Center Expert server.
- 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.

The **Alert Settings** menu in the **NetBotz Appliance Configuration** option of the **Device** menu provides access to the alert thresholds. Each **Alert Threshold** option allows you to search some or all of the NetBotz Appliances monitored by the Data Center Expert 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.

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.

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 Data Center Expert 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.

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.

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.
Audio	**Relative number (0 - 100)**	Settings for sensors that measure the volume of sound.
Current (Amps)	**Amps (0.0 - 100.0)**	Settings for sensors that measure current as total amperage (amps).
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 Data Center Expert server.

Note: You can configure multiple sensors discovered for the **Other Numeric Sensors** option, when the sensors you select can all use the same threshold settings. For example, battery and UPS age sensors, can be configured to use the same thresholds, as can utility, input, and output voltage sensors.

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.

State threshold options

Threshold	Value	Description

Door	**Open** or **Closed**	Settings for sensors that determine whether a door is open or closed.
Door (Handle)	**Up** or **Down**	Settings for sensors that determine whether a door handle is up or down.
Door (Lock)	**Locked** or **Unlocked**	Settings for sensors that determine whether a door lock is locked or unlocked.
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.

State threshold types for rack access

Setting	Description
Door Forced Entry Threshold	An alert occurs when the door is open while the handle is down and the lock is locked, enabled by default. **Note:** When the “Allow handle down while door open” option is selected, returning the handle to the down position while the door is open will not generate an alert.
Handle Forced Entry Threshold	An alert occurs when the handle is up while the lock is locked, enabled by default.
Unscheduled Access Threshold	An alert occurs when unscheduled rack access is attempted using a card, key, or remote command, enabled by default.

	Note: If any of the other “Unscheduled” access thresholds are used (Card, Key, or Remote), this threshold should be removed from the lock sensor.
Unscheduled Remote Access Threshold	An alert occurs when unscheduled rack access is attempted using a remote command issued from the NetBotz Appliance or the Data Center Expert console. **Note:** To allow remote access without generating an alert, you must modify the threshold schedule, disable the threshold for the desired time frame, and disable the default "Unscheduled Access Threshold". An unlock event will still be generated in the NetBotz Appliance event log.
Unscheduled Card Access Threshold	An alert occurs when unscheduled rack access is attempted using a card, or a door is opened with a card, and left open past that card’s access schedule.
Unscheduled Key Access Threshold	An alert occurs when unscheduled rack access is attempted using a key. **Note:** To allow key access without generating an alert (for example, during normal work hours), you must modify the threshold schedule, disable the threshold for the desired time frame, and disable the default “Unscheduled Access Threshold”. A key unlock event will still be generated in the NetBotz Appliance event log.

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 Data Center Expert server.

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

Note: You can configure multiple sensors discovered for the **Other State Sensors** option, when the sensors you select use the same alert states settings. For example, all sensors that use **On** and **Off** states can be configured to use the same thresholds, as can all sensors that use **Up** and **Down**.

Active/Inactive: • Button • Temperature Override Status **Open/Closed**: • Input Contact • Output Relay • Bypass	**Fault/No Fault**: • Contact • Input State **Connected/ Disconnected**: • Speakers • External Microphone	**Multiple Statuses:**: • Online • Device Status • Battery Status • UPS Status • Communication Status

On/Off: • Switch • Outlet • Alarm Device • Test Relay **Other Settings**: • Ethernet Link • UPS Input Voltage (line neutral) • Current Output Phase	**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	• 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 **NetBotz Appliance Configuration** option in the **Device** 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 **Device** menu options.

1. Select the sensor type you want to manage from the **NetBotz Appliance Configuration** option in the **Device** menu or **Device View** right-click menu.
   - For a **Device** 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 **Alert Settings** option in the **NetBotz Appliance Configuration** option in the **Device** 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 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 monitored by the Data Center Expert server.
Hostname	Identifies a device by its hostname or IP address, when no hostname is defined.
Type	Identifies a device by its 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**: 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.
Add	Click to add an alert threshold for the selected sensor.
Edit	Click to edit a selected alert threshold.
Remove Selected	Click to delete a selected alert threshold from the list.

"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 the device is monitored 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.
Threshold Scheduling	Allows you to define the specific periods of time, for each day of the week, during which an associated threshold will be disabled.
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.
Custom URL	Identify an Internet address you want included in an alert notification for the alert threshold.
Custom 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.

"Threshold Schedule" display:

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

The **Advanced** tab of each threshold's "Configure Settings" display, accessed from the **Alert Threshold** options in **NetBotz Appliance Configuration > Alert Settings** provides access to the "Threshold Schedule" 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 alarm threshold 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.

Network Management System Integration option

This option allows you to specify trap receivers (Network Management System consoles) to which the Data Center Expert server will send SNMPv1 traps and SNMPv3 informs.

This option accesses settings used to enable the Data Center Expert server to send SNMPv1 traps and SNMPv3 informs to defined Network Management System consoles for alarms that occur at monitored SNMP devices and NetBotz Appliances, and the devices associated with those appliances.

Note: For information about the SNMPv1 traps and SNMPv3 informs that the Data Center Expert server can send, see the latest version of the APC PowerNet MIB available for download at https://www.apc.com/us/en/tools/download/ .

"Network Management System Integration" display

Use this display to manage the trap receivers (Network Management System consoles) to which you want the Data Center Expert server to send SNMPv1 traps and SNMPv3 informs for alarms that occur at the monitored SNMP, Modbus, and NetBotz Appliances, and the devices associated with those appliances.

Note: For information about the SNMPv1 traps and SNMPv3 informs that the Data Center Expert server can send, see the latest version of the APC PowerNet MIB available for download at https://www.apc.com/us/en/tools/download/ .

Element	Description
Enable All Traps	Select (check-mark) to allow the Data Center Expert server to send SNMPv1 traps or SNMPv3 informs to the listed receivers.
List	Use to manage the receivers to which SNMPv1 traps or SNMPv3 informs can be sent. **Trap Receiver**: IP address of the Network Management System console. **Port**: Port at the receiver to which SNMPv1 traps or SNMPv3 informs are sent. **Type**: Type of SNMP communications to be used (**SNMPv1** or **SNMPv3**). **Severities**: Severity levels for which SNMPv1 traps or SNMPv3 informs will be sent: **Failure**, **Error**, **Critical**, **Warning**, and **Information**. **Note:** At least one severity level must be selected. For information about what each severity level indicates, see Alarm action severity settings.

Element	Description
Add	Click to access the "Add Trap Receiver" wizard.
Remove	Click to delete a selected trap receiver from the list.
Edit	Click to access the "Edit Trap Receiver" wizard for a selected trap receiver.
Send Test Trap	Click to send a test trap or inform to a selected trap receiver. **Note:** The Data Center Expert server cannot determine if a trap or inform was received. You must verify its receipt at the trap receiver. For information about what can cause a trap test to fail, see Test trap failures.

"Add (or Edit) Trap Receiver" display

Use this display to select the **Trap Type** you want to send to a new (**Add**) or existing (**Edit**) trap receiver: **SNMPv1 Trap** or **SNMPv3 Inform**.

"SNMPv1 Trap Settings" display

Use this display to define the SNMPv1 settings for a new trap receiver, or to edit the SNMPv1 settings for an existing trap receiver.

Element	Description
IP Address	Identify the IP address of the Network Management System console.
Port	Select the port number the Network Management System console uses to receive SNMPv1 traps.
Read Community Name	Identify the read community string that will be used when sending SNMPv1 traps to the Network Management System console.
Severities	Select (check-mark) at least one severity for which you want the Data Center Expert server to send SNMPv1 traps to the Network Management System console when that severity level is reported by a monitored SNMP device, NetBotz Appliance, or devices associated with those appliances. **Note:** For information about what each severity level indicates, see Alarm action severity settings.

"SNMPv3 Inform Settings" display

Use this display to define the SNMPv3 settings for a new trap receiver, or to edit the SNMPv3 settings for an existing trap receiver.

Element	Description
IP Address	Identify the IP address of the Network Management System console.
Port	Select the port number the Network Management System console uses to receive SNMPv3 informs.
Username	Identify the user identification to be used when sending SNMPv3 informs to the Network Management System console.
Authentication Type/Password	Select **SHA-1** or **MD5** as the authentication protocol used for the SNMPv3 informs, and type in the password for the selected protocol. **Note:** No password is needed for **None**, the default selection.
Encryption Type/Password	Select **DES** or **AES-128** as the encryption protocol used for the SNMPv3 informs, and type in the password for the selected protocol. **Note:** No password is needed for **None**, the default selection.
Severities	Select (check-mark) at least one severity for which you want the Data Center Expert server to send SNMPv3 informs to the Network Management System console when that severity level is reported by a monitored SNMP device, NetBotz Appliance, or devices associated with those appliances. **Note:** For information about what each severity level indicates, see Alarm action severity settings.

Test trap failures

A Network Management System listed as a trap receiver in the "Network Management System Integration" display can fail to receive a test trap if there are problems with the settings used, or with the network.

Note: If the problem persists, contact APC Support (http://www.apc.com/support).

Problem	Recommended Actions
Settings	Make sure the "SNMPv1 Trap Settings" display or "SNMPv3 Inform Settings" display settings associated with the target Network Management console are properly defined. Make sure the SNMP settings have not changed at the target Network Management System console, and that the appropriate SNMP service is enabled at that console.
Network	Make sure the device was not turned off or disconnected from the network when the test trap was sent.

Problem	Recommended Actions
	Correct any network connection problem.

SNMP Device Communication Settings (Device menu)

Provides options used to configure the settings the Data Center Expert server uses for FTP and SNMP communication with its monitored SNMP devices.

Device File Transfer Settings option

Use this option to access the "Device File Transfer Settings" display used to manage the settings the Data Center Expert server uses for File Transfer Protocol (FTP) or Secure Copy (SCP) access to APC SNMPv1 and SNMPv3 devices.

"Device File Transfer Settings" display

Use this display to manage the File Transfer Protocol (FTP) or Secure Copy (SCP) access values for APC SNMPv1 and SNMPv3 devices.

Note: Functionally identical versions of this display are used by the "SNMPv1/SNMPv3 Device Discovery," "Apply Firmware Updates," and "APC SNMP Device Configuration" wizard, as well as by **Device File Transfer Settings**, an **SNMP Device Communication Settings** option in the **Device** menu. A change saved in one display is reflected in all.

- To use FTP for APC SNMP device access, FTP server access must be enabled at that device.
- To use SCP for APC SNMP device access, Secure Shell version 2 (SSHv2) console access must be enabled at that device.

Element	Description
List	Lists the access settings the Data Center Expert server can use for FTP or SCP access to its monitored devices. **Username**: The username used for access to a device. **Note:** By default, the Data Center Expert server can download firmware only to devices that use **apc** (lowercase) for the username and password (the actual password used for device access is identified in the "Edit Device File Transfer Settings" display). **IP or IP Range**: The IP address, or range of addresses, at which the access settings support FTP or SCP communication.

Element	Description
	FTP Port: The port used for FTP access to a device. **SCP Port**: The port used for SCP 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 try to access a device, after the initial attempt failed, before it stops trying to access that device (**1**, by default). **Protocol**: The protocol the transfer settings set will use to access devices (**FTP only**, **SCP only**, or **Try SCP, fall back to FTP**).
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 File Transfer Settings" display

Use this display to add or edit the settings the Data Center Expert server uses for File Transfer Protocol (FTP) or Secure Copy (SCP) access to APC SNMPv1 and SNMPv3 devices.

Note: Functionally identical versions of this display can be accessed from the "Device File Transfer Settings" displays used by the "Apply Firmware Updates," "SNMPv1/SNMPv3 Device Discovery," and "APC SNMP Device Configuration" wizards, and by **Device File Transfer Settings**, an **SNMP Device Communication Settings** option in the **Device** menu.

Element	Description
Username	Identify the name used for access to a device.
Password	Identify the password used for access to a device.
Verify Password	Retype the password.
IP or IP Range	Identify The IP address, or range of addresses, at which the access settings support FTP or SCP communication (***.*.*.***, by default).
Protocol	Identify whether the transfer settings will use FTP (**FTP only**), SCP (**SCP only**), or attempt to use SCP, but fall back to using FTP if SCP fails (**Try SCP, fall back to FTP**).
FTP Port	Select the port the server will use for FTP access to devices (**21**, by default).
SCP Port	Select the port the server will use for SCP access to devices (**22**, by default).

Timeout	Identify how long the server will wait before it considers that an attempt to access a device has failed (**3000**, by default).
Retry Limit	Select the number of times the server will try to access a device, after the initial attempt failed, before it stops trying to access that device (**1**, by default).

Device Scan Settings option

Use this option to manage the settings the Data Center Expert server uses for SNMPv1 and SNMPv3 communication with its monitored SNMP devices, as well as alarm 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**
- **Notification Policy** : The notification policy the Data Center Expert server associates with alarms at an APC SNMP device.
- **Location**: The location of the device, if known.
- **Protocol**: **SNMPv1** or **SNMPv3**.
- **Port**, **Scan interval**, **Timeout**, and **Retries**: SNMP communication settings.
- **Last Scan Time**: The date and time when the Data Center Expert server last scanned a device for status information.

You can edit the **Notification Policy**, **Port**, **Timeout**, and **Retries** settings and other settings not identified in the list, select one or more of the listed devices and click **Edit Device Scan Settings**. The following editable settings are not identified in the list.

- **Scan Interval (minutes)**
- **Priority Scanning**
  Note: Priority Scanning is a trap-based polling process that only occurs in response to traps from APC SNMPv1 devices or informs from APC SNMPv3 devices at which the Data Center Expert server is defined as a trap receiver.
- **SNMP Settings**: Select the protocol the DCE server uses to communicate with the selected device(s). Rebooting the DCE server is not required.

  IMPORTANT: You must also change the communication protocol on each device.
- **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 Scan Settings" display.

"Edit Device Scan Settings" display

Use this display to edit notification policy and SNMP communication settings the Data Center Expert server uses with its monitored SNMP devices.

The display includes elements that are shared by 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 SNMP device. **Note:** No **Hostname** is provided when multiple devices are selected.
Scan Interval (minutes)	Select how much time will pass between Data Center Expert server scans of a selected SNMP 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:** Setting the scan interval below the default value of five minutes can adversely affect performance when the Data Center Expert server is managing a large number of devices.
Port	The number of the port used for SNMP communications with a selected SNMP device.
Timeout (seconds)	Select how long the Data Center Expert server will wait for a response before it considers an attempt to communicate with a selected SNMP device has failed: from **1** through **60** seconds.
Retries	Define how many times the Data Center Expert server will attempt to communicate with a selected SNMP 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 Data Center Expert 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 for an APC SNMPv1 device, the server will poll the device as soon as it receives a trap from that device. As a non-trap receiver, the server reports device alarms during normal scan intervals only. **Note:** Priority scanning is a trap-based polling process that only occurs in response to traps from APC SNMPv1 devices or informs from APC SNMPv3 devices.
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 Data Center Expert server as a trap receiver at a selected APC SNMPv3 device. This allows for faster reporting of errors at that device by the server. As a trap receiver for an APC SNMPv3 device, the server will poll the device as soon as it receives an inform from that device. As a non-trap receiver, the server reports device alarms during normal scan intervals only. **Note:** Priority Scanning is a trap-based polling process that only occurs in response to traps from APC SNMPv1 devices or informs from APC SNMPv3 devices.
User	Identify the username the server uses for secure communication with a selected SNMPv3 device.
Authentication Protocol	Change the protocol (**MD5** or **SHA-1**), 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 Data Center Expert 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 Data Center Expert 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 SNMP devices supported by the Data Center Expert server. The new or updated DDFs can be uploaded to the Data Center Expert server from a local file, or from the APC website.

1. Select **Device Definition Files**, an **SNMP Device Communication Settings** option in the **Device** menu.
2. Select the **Device Definition Files** option in the "SNMP Device Communication 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 files 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 Scan Settings option

Use this option to define the global scan settings that the Data Center Expert server will use for its communication with its monitored SNMP devices.

Element	Description
Scan Interval	Select how much time will pass between Data Center Expert server scans for status information at a monitored SNMP device, when the **Device Settings** option in the "SNMP Device Communication Settings display" has **Default** selected for that device's **Scan Interval (minutes)** setting. **Note:** Setting the scan interval below the default value of five minutes can adversely affect performance when the Data Center Expert server is managing a large number of devices.

Scan Interval Offset	The next device scan time is based on the **Scan end time** plus the **Scan interval (minutes)** by default. Data will be displayed in sensor history at intervals that equal the amount of time the scan takes plus the scan interval. This helps optimize network traffic, particularly when monitoring large numbers of devices. To display data at the configured interval, select **From scan start time**.

Supplemental OIDs option

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

Once a supplemental OID has been added, the Data Center Expert 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 the **Other Numeric Sensors** threshold option to configure alert threshold settings for an SNMP device that has the type of numeric 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 numeric 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**.

Modbus Device Communication Settings (Device menu)

Provides options used to configure settings the Data Center Expert server uses for communication with its monitored Modbus devices.

Modbus Device Definition Files option

Use this option to manage the Device Definition Files (DDFs) that the Data Center Expert server uses to access information about the sensors at supported Modbus devices.

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

Element	Description
Device Definition Files	Lists the DDFs already installed at the Data Center Expert server.
Remove	Click to delete a selected DDF from the list. You cannot delete a DDF that is preinstalled on the Data Center Expert server. **Note:** Deleting a DDF will affect what sensors at 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, or stored on a local computer.

"Add/Update Definitions" wizard

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

"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.

Device Scan Settings option

Use this option to manage the settings the Data Center Expert server uses to communicate with its monitored Modbus devices, as well as alarm settings the server associates with those devices.

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

- **Server Address**
- **Device Type**
- **Notification Policy** : the notification policy the Data Center Expert server associates with alarms at a Modbus device.
- **Location**: the location of the device, if known.
- **Port**
- **Timeout**
- **Retries**
- **Last Scan Time**

You can edit the **Notification Policy**, **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 Scan Settings**. The following editable settings are not identified in the list.

- **Scan Interval (minutes)**

"Edit Device Scan Settings" display

Use this display to edit notification policy and communication settings the Data Center Expert server uses with its monitored Modbus devices.

Shared Element	Description
Hostname	When only one device is selected, identifies the hostname or IP address of that Modbus device. **Note:** No **Hostname** is provided when multiple devices are selected.
Server Address	Select the server address you want associated with the selected Modbus device. **Note:** When more than one device is selected, the server address cannot be configured.
Device Definition File	The device definition file (DDF) associated with the device. **Note:** The DDF associated with a Modbus device cannot be modified.
Scan Interval (minutes)	Select how much time will pass between Data Center Expert server scans of a selected Modbus device for status information: from **1** through **60** minutes, and **Default**, the minutes for which is defined by the **Global Scan Settings** option's **Scan Interval** setting. **Note:** Setting the scan interval below the default value of five minutes can adversely affect performance when the Data Center Expert server is managing a large number of devices.
Port	The number of the port used for Modbus communications with a selected Modbus device.
Timeout (seconds)	Select how long the Data Center Expert server will wait for a response before it considers an attempt to communicate with a selected Modbus device has failed.
Retries	The number of times the Data Center Expert server will try to communicate with the device after the timeout has expired before considering communication has failed.

Global Scan Settings option

Use this option to define the global scan settings that the Data Center Expert server will use for its communication with its monitored Modbus devices.

Element	Description
Scan Interval (minutes)	Select how much time will pass between Data Center Expert server scans for status information at a monitored Modbus device, when the "Device Scan Settings" display in the **Modbus Device Communication Settings** option has **Default** selected for that device's **Scan Interval (minutes)** setting. **Note:** Setting the scan interval below the default value of five minutes can adversely affect performance when the Data Center Expert server is managing a large number of devices.
Scan Interval Offset	The next device scan time is based on the **Scan end time** plus the **Scan interval (minutes)** by default. Data will be displayed in sensor history at intervals that equal the amount of time the scan takes plus the scan interval. This helps optimize network traffic, particularly when monitoring large numbers of devices. To display data at the configured interval, select **From scan start time**.

Adding or updating device definition files (DDFs)

Use the "Add/Update Definitions" wizard to add or update the DDFs available for the Modbus devices supported by the Data Center Expert server. The new or updated DDFs can be uploaded to the Data Center Expert server from a local file, or downloaded from the APC website.

1. Select **Device Definition Files**, a **Modbus Device Communication Settings** option in the **Device** menu.
2. Select the **Device Definition Files** option in the "Modbus 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 files 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.

NetBotz Appliance Communication Settings (Device menu)

Provides options used to configure settings the Data Center Expert server uses for communication with its monitored NetBotz Appliances.

NetBotz Appliance Credentials option

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

For information about discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

Note: The "Apply Firmware Updates" display relies on the elements in this option to update NetBotz Appliances.

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 NetBotz Appliance Credentials" display

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

This display is accessed from the **NetBotz Appliance Credentials** option in the **NetBotz Appliance Communication Settings** option of the **Device** menu.

For NetBotz 750, enter user credentials (not root). If the credentials are different for any of NetBotz 750 appliances you want to discover, add each appliance to the list individually.

For more information about discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

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

Define how often the Data Center Expert server polls for sensor and alarm data and device status on monitored NetBotz Appliances, or 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.

The Data Center Expert server polls NetBotz 750 Appliance cameras every 10 minutes by default.

NetBotz 750 Camera Communication Settings

Configure settings to communicate with the cameras connected to the selected NetBotz 750 Appliances.

Before you discover a NetBotz 750 Appliance, add the certificate from the NetBotz 750 to Data Center Expert. Otherwise, you cannot see its connected cameras on the Surveillance tab. You must also add the certificate from Data Center Expert to the NetBotz 750. Otherwise, camera clips and motion updates cannot be posted to Data Center Expert.

For more information about discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

Element	Description
List	**IP address**: IP address of the NetBotz 750 Appliance

	Location: Location of the NetBotz 750 Appliance **Use SSL**: Whether the NetBotz 750 Appliance requires SSL to communicate with its connected cameras. **Verify options**: The level of verification required for communication between Data Center Expert and the cameras connected to the NetBotz 750 Appliance. **Port**: The SSL port used by the NetBotz 750 Appliance, 443 by default. **Last Scan Time**: Date and time of the last communication with the NetBotz 750 Appliance.

Edit Communication Settings display

When you select the **Verify certificate** option, you can use a self signed certificate from Data Center Expert to add to the NetBotz 750. You must also uncheck the box on the NetBotz 750 on the **Settings** > **System** > **DCE Surveillance** page.

When you select the **Verify certificate and hostname** option, you must use a certificate signed by a certificate authority and DNS must enabled on Data Center Expert and the NetBotz 750.

Element	Description
Use SSL	Check to require Data Center Expert to use SSL to communicate with the cameras connected to the selected NetBotz 750 Appliance, checked by default.
Port	The SSL port used to communicate with the cameras connected to the NetBotz 750 Appliance, 443 by default.
Verify SSL Options	**No verification**: Verification of the SSL certificate is not required to communicate with the cameras connected to the NetBotz 750 Appliance. Selected by default. **Verify certificate**: Either a signed or a self-signed SSL certificate from the selected NetBotz 750 must be verified to communicate with the cameras connected to the appliance. **Verify certificate and hostname**: A signed SSL certificate and the DNS hostname of the NetBotz 750 must be verified to communicate with the cameras connected to the selected appliance.

	Note: You add the NetBotz 750 SSL certificate to Data Center Expert in the **System** > **Server Administration Settings** > **Server SSL Certificate** option.

NetBotz Appliance Configuration (Device menu)

The configuration settings at the monitored NetBotz Appliances can be defined using the **NetBotz Appliance Configuration** options. **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.

The Data Center Expert server can notify users when the Data Center Expert server alarm thresholds are triggered for its monitored devices. Additionally, the **Alert Settings** options in the **NetBotz Appliance Configuration** option define how the monitored NetBotz Appliances can each generate their own alert notifications in response to alert threshold violations that occur at the devices they monitor.

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. To configure **Rack Access Settings** at multiple appliances, you must select the NetBotz Appliances, then select that **NetBotz Appliance Configuration** option.

Note: With the exception of the **Alert Settings** and **Post Alert Data Settings** options, 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**, **Rack Access Settings**, and the **Alert Settings** options.

Note: For information about the **Alert Settings** and **Rack Access Settings** options, use the related links to the help for these options.

For information about discovering NetBotz 750 Appliances, see NetBotz 750 Appliance discovery .

1. In the **Device** 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 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 Data Center Expert 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: If an invalid password is used during an attempt to restore a NetBotz Appliance that is in Post-only mode, the status will go to **Completed**, with no restore or error occurring.

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

Backup/Restore option

Use this option to store a configuration backup file in the Data Center Expert 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.
   Note: If you use an invalid password during an attempt to restore a NetBotz Appliance in Post-only Mode, the restore will not occur, and no error will be reported. You will need to repeat the restore procedure using the valid password.
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 on 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 **Device** 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 **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.
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 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.
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

Create masks that will cause motion in image areas to be ignored (**Motion Mask**), or regions of the image from being seen (**Blockout Mask**) for the selected camera during alarm and surveillance activities. Only the options supported by the selected camera are shown.

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), 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 must change (as determined by the **Sensitivity** value) before the changed image is considered movement. A lower **Area of Motion** value indicates a smaller area and therefore a smaller amount of movement is required to flag a change.
Sensitivity	Use this setting to specify how much change in a portion of the image will be tolerated before the changed image is considered movement. A lower **Sensitivity** value indicates less tolerance for change between images. More subtle movements will be marked as a change.
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:

Configure a selected camera so that specified areas of the image cannot be seen. The selected camera must be monitored by a NetBotz Appliance that has the Premium Software Module. This option is not available for NetBotz 750 cameras.

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.

Motion mask

Configure the NetBotz 750 camera's motion sensor to ignore movement that is detected in specified regions of the image capture.

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.

Note: 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 in the NetBotz 750 web interface, the **Motion Mask** tab will show only the cropped area.

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 **Restore Defaults**. 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.
Sensitivity	Use this setting to specify how much change in a portion of the image will be tolerated before the changed image is considered movement. A lower **Sensitivity** value indicates less tolerance for change between images. More subtle movements will be marked as a change.

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 Data Center Expert 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 the configuration display in this option 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, certain Pelco cameras, 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, certain Pelco cameras, 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, certain Pelco cameras, 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 Data Center Expert server to send their alert data.

When a NetBotz Appliance is discovered by Data Center Expert, the hostname of the Data Center Expert is added to the NetBotz Appliance. This enabled the Data Center Expert 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 Data Center Expert server.

Note: This display also can be accessed when using **Network Settings**, a **Server Administration Settings** option in the **System** 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 Data Center Expert Hostname	The **Hostname** defined in the **Network Settings** option's **Public (LAN1)** tab.
Current Data Center Expert 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. **Note:** If any of the NetBotz Appliances you want the Data Center Expert server to monitor have no DNS service available, select to use the server's IP address. Otherwise, those appliances will be unable to post data to the server, and status will only be available in response to polling.

Rack Access Settings

Use this option, accessed from the **NetBotz Appliance Configuration** option, to configure access to rack doors monitored by NetBotz Appliances that monitor Rack Access Pod 170 devices.

To configure **Rack Access Settings**, you must be a Data Center Expert Administrator, or a Device Administrator for the selected device group or the device group that contains the selected NetBotz Appliance.

When no Rack Access Pod 170 devices are monitored by the selected NetBotz Appliance, the "Rack Access Settings" display is not available.

The "NetBotz Appliance Rack Access Settings" display appears the first time you access the **Rack Access Settings** option for a selected NetBotz Appliance. This display allows you to specify the supported card type and auto lock timeout for the selected appliance. You can access the display again, if needed, from the **NetBotz Appliance Settings** link in the "Rack Access Settings" display. When the card type has already been specified, you can modify the **Auto Lock Timeout** only. To modify the supported card type, you must first remove all the cards associated with the appliance.

The **Show Unregistered Cards** link is displayed when one or more rack access cards swiped at a Rack Access Pod 170 device have not been registered to the associated

NetBotz Appliance. You access the "Unregistered Cards" display from the link to select the rack access cards you want to register, or remove cards you do not want to register from the list.

You can add up to 200 rack access cards to the list for the device group, or NetBotz Appliance or Appliances selected. You identify the Card ID #, the user name, a description, and whether the card requires an authorization card swipe from another card to access the door. You can modify the settings for each card, remove cards from the list one at a time, or copy the scheduled access of one card to another.
Note: When you remove cards from the list, you must press **Apply** or **OK** to save the changes.

You select a card in the left pane to display its card ID #, user name, description, and authorization requirement, if any, above the right pane. The right pane allows you to select the doors on which to enable or disable access for that card, 24 hours a day, 7 days a week by default. You can select a NetBotz Appliance, a Rack Access Pod 170, or a door, and press **Edit Access** to modify the weekly access schedule.
Note: When you enable or disable door access, you must press **Apply** or **OK** to save the changes.

You must configure door access for one card at a time. You can then copy the scheduled access of one card to another.

Four menus provide access to the **Rack Access Settings**:

- **NetBotz Appliance Configuration** option, accessed from the **Device** menu.
- Right-click menu **NetBotz Appliance Configuration** in the **Device View** and **Map View** of the **Monitoring** perspective.
- Right-click menu in the **Device Groups** view.

When you access the "Rack Access Settings" display from the right-click menu **NetBotz Appliance Configuration** in the **Device View** and **Map View** of the **Monitoring** perspective, the NetBotz Appliance you selected, and its associated Rack Access Pod 170 devices, are displayed in the right pane.

When you access the "Rack Access Settings" display from the **NetBotz Appliance Configuration** option, accessed from the **Device** menu, the device groups that contain NetBotz Appliances monitoring Rack Access Pod 170 devices, and their associated appliances and devices, are displayed in the right pane.

When you access the "Rack Access Settings" display from the right-click menu **NetBotz Appliance Configuration** in the **Device Groups** view of the **Monitoring** perspective, the device group you selected that contains NetBotz Appliances monitoring Rack Access Pod 170 devices, and its associated appliances and devices, are displayed in the right pane.

"Rack Access Settings" display

Use this display to add cards and assign users to those cards, and configure access to rack doors monitored by the Rack Access Pod 170 devices associated with the selected device group, or NetBotz Appliance or Appliances.

You use the left pane in this display to add up to 200 rack access cards for the selected device group, or NetBotz Appliance or Appliances, and assign users to those cards. You then select a card in the left pane, and select a device group, NetBotz Appliance, Rack Access Pod 170, or door in the right pane to enable, disable, or schedule the rack access for that card.

When no HID cards proximity cards have been registered for the selected NetBotz Appliance, the "NetBotz Appliance Settings" display appears when you access the **Rack Access Settings** option. This display allows you to specify the supported card type and auto lock timeout for the selected appliance.

You can access the "NetBotz Appliance Settings" display from the **NetBotz Appliance Settings** link to modify the **Auto Lock Timeout** only. To modify the supported card type, you must first remove all the cards associated with the appliance.

When one or more rack access cards swiped at a Rack Access Pod 170 device have not been registered to the associated NetBotz Appliance, the **Show Unregistered Cards** link is displayed. You can access the "Unregistered Cards" display from the link to select the rack access cards you want to register, or remove cards you do not want to register from the list.

Left pane:

Element	Description
List	**Card ID#**: The identification number assigned to the card. **User name**: The user name assigned to the card.
Add	Select to add a rack access card to the list.
Edit	Select to modify the username, description, or authorization level for the selected card.
Remove	Select to remove a card from the list. **Note:** You must press **Apply** or **OK** to save the changes.
Copy	Select to copy the scheduled access of the selected card to one or more additional cards.

Right pane:

Element	Description
Card ID#	Displays the card ID # selected in the table at left, the associated user name, description, and whether a swipe from an additional card is required to authorize rack access. **Note:** The additional card must not require an authorization card swipe.
List	**Door**: Select a device group, NetBotz Appliance, or Rack Access Pod 170 device, or check mark one or more doors to schedule access for the card selected. **Scheduled Access**: Icons for each door indicate whether access is scheduled 24 hours a day, 7 days a week (full green icon), some of the time (half green icon), or disabled (white icon).
Enable	Select to schedule door access 24 hours a day, 7 days a week for the selected device group,

	NetBotz Appliance, Rack Access Pod 170 device, or door.
Disable	Select to disable door access 24 hours a day, 7 days a week for the selected device group, NetBotz Appliance, Rack Access Pod 170 device, or door.
Edit Access	Select to modify weekly door access for the selected device group, NetBotz Appliance, Rack Access Pod 170 device, or door.

You can use the right-click options in the right pane to do the following:

- Enable or disable rack access 24 hours a day, 7 days a week for the selected device group, NetBotz Appliance, Rack Access Pod 170 device, or door (**Enable** or **Disable** option).
- Schedule weekly rack access for the selected device group, NetBotz Appliance, Rack Access Pod 170 device, or door (**Edit** option).
- Expand or collapse the list for the selected device group, NetBotz Appliance, or Rack Access Pod 170 device (**Expand** or **Collapse** option).
- Select every door for every NetBotz Appliance in the list (**Select All Doors** option).
- Select every Door 1 door for the selection (**Select All Door 1 Doors** option).
- Select every Door 2 door for the selection (**Select All Door 2 Doors** option).

Note: To lock and unlock the doors, you use the **Rack Access Control** option, available in the right-click menu of the **Device View** or **Map View** for the selected controllable NetBotz Appliance or NetBotz Rack Access Device.

"NetBotz Appliance Rack Access Settings" display

Use this display to identify the HID proximity card type used for the selected NetBotz Appliance, and specify the auto lock timeout. All cards registered to the NetBotz Appliance must use the same card type.

The "NetBotz Appliance Rack Access Settings" display appears the first time you access the **Rack Access Settings** option for a selected NetBotz Appliance. You can specify one of four supported HID proximity card types:

- H10301 - Standard 26-bit
- H10302 - 37-bit without a facility code
- H10304 - 37-bit with a facility code
- CORP1000 - Corporate 1000

You can access the display again, if needed, from the **NetBotz Appliance Settings** link in the "Rack Access Settings" display. You can modify the **Auto Lock Timeout** only. To modify the supported card type, you must first remove all the cards associated with the appliance.

The **Auto Lock Timeout** determines how long the device will wait (10 - 60 seconds) until it automatically locks the rack door after a card, a key, or a remote command is used to unlock it. If the door is open or the handle is up after the timeout expires, the device will issue the lock command until the door is closed and the handle is down.

Additionally, the **Auto Lock Timeout** limits the time the device will wait for a second authorizing card swipe after a rack access card that requires authorization is swiped.

Element	Description

Card Type	The type of HID proximity card registered to the NetBotz Appliance selected. You can specify the card type once only.
Auto Lock Timeout	Specify the time the device will wait until it automatically locks the rack door after a card, a key, or a remote command is used to unlock it (10 - 60 seconds).

"Unregistered Cards" display

Use this display to register one or more rack access cards swiped at a Rack Access Pod 170 device, and not registered to the associated NetBotz Appliance.

Note: You access this display from the "Rack Access Settings" display **Show Unregistered Cards** link, available only when a rack access card swiped at device for the selection has not been registered.

Element	Description
List	**Card ID#**: The identification number assigned to the card. **Timestamp**: The date and time the rack access card was swiped.
Register	Select to register the selected rack access cards.
Remove	Select to remove the selected unregistered rack access cards from the list.
Remove All	Select to remove all unregistered rack access cards from the list.

"Add Rack Access Card" display

Use this display to add a rack access card, and specify its authorization level.

Element	Description
Card ID #	Identify the number assigned to the card, in the format shown.
User Name	Identify the user name assigned to the card
Description	Provide a description for the card, if desired.
Requires Authorization Card Swipe	Specify whether a swipe from an additional card is required to authorize rack access.

"Edit Rack Access Card" display

Use this display to modify the settings, with the exception of the card ID #, for a rack access card.

Element	Description

Card ID #	The number assigned to the rack access card cannot be modified. **Note:** You can use the "Add Rack Access Card" display to add another card and copy settings to it.
User Name	Modify the user name assigned to the card.
Description	Modify the description.
Requires Authorization Card Swipe	Specify whether a swipe from an additional card is required to authorize rack access.

"Copy Rack Access Card" display

Use this display to copy the weekly access schedule from the selected rack access card to one or more cards.

Element	Description
Source Card	The Card ID # and user name of the card from which the weekly access schedule will be copied.
Include Authorization Card Swipe Attribute	Check-mark to require a swipe from an additional card to authorize rack access.
List	Check-mark one or more rack access cards on which to copy the weekly access schedule.

"Schedule Access" display

Use this display to define the specific periods of time, for each day of the week, during which rack access will be enabled or disabled for the card selected, and the device group, NetBotz Appliance, Rack Access Pod 170 device, or door selected, in the "Rack Access 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 rack access 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.
- Enable or disable all cells (**Enable All** or **Disable All** button icons).
- Double-click or right-click a disabled cell to schedule access for the day selected (**New Schedule** option).
- Double-click or right-click an enabled cell to modify scheduled access for the day selected (**Edit Schedule** option).
- Right-click an enabled cell to disable scheduled access for the day selected (**Remove Schedule** option).

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 the 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 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 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 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.

APC SNMP Device Configuration (Device menu)

Use this option to configure settings at one or more monitored APC SNMP devices.

Note: You cannot use this option to configure settings for non-APC SNMP devices, NetBotz Appliances and their monitored devices, and some older APC SNMP devices.

The following "Configuration Type" display options, and the Configuration Status view, are used by the APC SNMP Device Configuration wizard:

- **Standard device configuration settings**: Select one or more monitored APC SNMP devices and configure them to use settings shared with a selected APC SNMP device, or settings saved as a template.
- **User configuration (APC OS versions 6.0.0 and higher**, **excluding v6.0.6 through v6.1.1)**: Modify user management options on devices with firmware v6.0.0 and higher, excluding v6.0.6 and v6.1.1.

The "Configuration Type" display is not available when there are no monitored devices with firmware v6.0.0 and higher.

You must upload a .csf file directly to the device to configure users on devices with firmware v6.0.6 or v6.1.1.

File transfer using SCP fails on devices with firmware v6.x earlier than v6.3.3. For best results, set the protocol to **FTP Only** in the "Device File Transfer Settings" display before you select the v6.x devices you want to update.

Note: FTP file transfer may fail on v6.x devices with touch screens.

See the Data Center Expert documentation on http://dcimsupport.apc.com for the most recent information on APC SNMP Device Configuration.

"Configuration Type" display

Use this display to select the type of device configuration you want to perform.

There are two types of APC SNMP device configuration available when at least one monitored APC SNMP device has firmware v6.0.0 and higher, excluding v6.0.6 - v6.1.1.

Note: You must upload a .csf file directly to the device to configure users on devices with firmware v6.0.6 or v6.1.1.

File transfer using SCP fails on devices with v6.x firmware earlier than v6.3.3. For best results, set the protocol to **FTP Only** in the "Device File Transfer Settings" display before you select the v6.x devices you want to update.

Note: FTP file transfer may fail on v6.x devices with touch screens.

See the Data Center Expert documentation on http://dcimsupport.apc.com for the most recent information on APC SNMP Device Configuration.

Element	Description

Standard device configuration settings	Select a monitored device or a template to configure the devices you select.
User Configuration for firmware v6.0.0 and higher (excluding v6.0.6 and v6.1.1)	Configure the user management actions for the devices with NMC firmware v6.0.0 and higher, excluding v6.0.6 and v6.1.1. Use this option to modify the existing user configuration on devices in this firmware range.

"Select Destination Devices" display

Use this display to select the APC SNMP devices on which you want to modify the user configuration.

Element	Description
Filter	Filter the table to list only entries that include the text you type, exactly as typed.
List	Select the APC SNMP devices on which you want to configure user management options to modify the existing user configuration. All APC SNMP devices monitored by the Data Center Expert server with firmware v6.0.0 and higher, excluding v6.0.6 and v6.1.1, are listed.
Device File Transfer Settings	Click to access the "Device File Transfer Settings" display used to manage the File Transfer Protocol (FTP) or Secure Copy (SCP) access values for APC SNMPv1 and SNMPv3 devices.

See the Data Center Expert documentation on http://dcimsupport.apc.com for the most recent information on APC SNMP Device Configuration.

"User Configuration" display

Use this display to select user management actions to modify the existing user configuration on the selected devices.

Configuration changes are sent to the device one command at a time. It can take up to 30 seconds per user after the "Device Configuration Status" display reports the configuration is complete to apply all the options.

Configure the following user management actions, or delete a selected action:

Create/Modify User: Configure the settings for the user you want to create or modify. You must configure this action individually for each user.

Modify Super User: Modify the settings for the 'apc' super user. The current password for the super user is required.

Modify Default User Settings: Modify the default settings used when a new user is created.

Delete Existing User: Specify the username for the user you want to delete. You cannot delete the only Administrator for the device.

Remove Action: Click to remove the selected action.

Element	Description
Action	The name of the user management action
Command	The parameters to configure on the selected devices.

See the Data Center Expert documentation on http://dcimsupport.apc.com for the most recent information on APC SNMP Device Configuration.

"Create/Modify User" display

Use this display to configure the settings for a new user or the user you want to modify.

Once you specify the username and password, check the box to configure each option.

When you modify a user that already exists on any destination device, all the settings you select, including the password, will be overwritten.

Element	Description
Username	The name of the user.
Password/Confirm Password	Specify the password for a new user or enter a new password for an existing user if you want to change it. The password is case-sensitive, with a 64 byte maximum (64 ASCII characters, fewer for multi-byte languages).
Role	Specify the user role: Administrator, Device, Network only, or Read only
Description	Additional notes to decribe the user.
Date Format	The date format to display in the device user interface.
Language	The language to display in the device user interface. **Note:** This setting will not take affect if the language you choose is not installed on the device.
Units	The units, Metric (the default) or US Customary, to display in the device user interface.
Session Timeout (mins)	The amount of time before the user is logged out due to inactivity, 1-60 minutes. The default is 3 minutes.
Serial Remote Authentication Override	Specify whether the user can login serially and override a logged in user, even when the device authentication method is set to RADIUS.
Event Log Color Coding	Specify whether text in the event log is color-coded based on event severity.
Log Export Format	The format of the event log when exported: **Tab** (the default) or **CSV**.

Enable User	Specify whether the user has access to login in to the device.
Advanced Options	Enter command line parameters to configure additional user options. For example, to configure the role Outlet, enter -pe "Outlet" in this field. For more information, see the Command Line Interface manual for your device at http://apc.com.

"Modify Super User" display

Use this display to change the settings for the super user.

Once you specify the username and password, check the box to configure each option.

Element	Description
Username	The name of the super user. This field cannot be changed for the super user.
Current Password/Confirm Current Password	The password for the super user is required.
New Password/Confirm New Password	Enter a new password for the super user if you want to change it. Otherwise, leave the field blank. The password is case-senstitive, with a 64 byte maximum (64 ASCII characters, fewer for multi-byte languages).
Description	Additional notes to decribe the user.
Date Format	The date format to display in the device user interface.
Language	The language to display in the device user interface. **Note:** This setting will not take affect if the language you choose is not installed on the device.
Units	The temperature units, Metric(the default) or US Customary, to display in the device user interface.
Session Timeout (mins)	The amount of time before the user is logged out due to inactivity, 1-60 minutes. The default is 3 minutes.
Serial Remote Authentication Override	Specify whether the user can login serially and override a logged in user, even when the device authentication method is set to RADIUS.
Event Log Color Coding	Specify whether text in the event log is color-coded based on event severity.
Log Export Format	The format of the event log when exported: **Tab** (the default) or **CSV**.
Enable User	Specify whether the user has access to login in to the device.
Advanced Options	Enter command line parameters to configure additional user options. For example, to configure the role Outlet, enter -pe "Outlet" in this field. For more information, see the Command

	Line Interface manual for your device at http://apc.com.

"Modify Default User" display

Use this display to modify the default settings used when a Super User or Administrator for the device creates a new user.

Element	Description
Enable User	Specify whether the user has access to login in to the device.
Role	Specify the user role: Administrator, Device, Network only, or Read only
Description	Additional notes to decribe the user.
Session Timeout (mins)	The amount of time (in minutes) before the user is logged out due to inactivity, 0-60 minutes. The default is 3 minutes.
Login Attempts	The number of incorrect logon attempts a user is allowed before the system disables the account 0-99. The default, 0 attempts, allows unlimited attempts.
Event Log Color Coding	Specify whether text in the event log is color-coded based on event severity.
Log Export Format	The format of the event log when exported: **Tab** (the default) or **CSV**.
Units	The units, Metric (the default) or US Customary, to display in the device user interface.
Date Format	The date format to display in the device user interface.
Language	The language to display in the device user interface. **Note:** This setting will not take affect if the language you choose is not installed on the device.
Require Strong Passwords	Specify whether new passwords created for users require additional rules: at least 8 characters long, with one lowercase character, one uppercase character, one number, and one symbol.
Require Password Change (days)	Select the duration (in days) after which the user is required to change the password, 0-365. The default, 0 days, disables this option.
Advanced Options	Enter command line parameters to configure additional user options. For example, to configure the role Outlet, enter -pe "Outlet" in this field. For more information, see the user manual for your device at http://apc.com.

"Select a Configuration Action" display

Use this "APC SNMP Device Configuration" wizard display to select the action you want to perform.

Configure Devices action

Allows you to use a monitored APC SNMP device's settings to configure and apply those same settings at other monitored APC SNMP devices.

Note: You can use this action to configure the settings for a single APC SNMP device, by selecting it as both the source and destination device, and editing the settings you want to change at that device.

1. Select **Configure Devices** and click **Next**.
2. Use the "Select Configuration Source" display to select the APC SNMP device you want to use as the configuration source, and click **Next**.
3. Use the "Select Destination Devices" display to select the APC SNMP devices you want to configure using settings from the selected source APC SNMP device, and click **Next**.
4. Use the "Configure Device Settings" display to select, and edit, as needed, the source APC SNMP device settings to be used to configure the same settings at the APC SNMP devices selected in the "Select Destination Devices" display, and click **Finish** to initiate the configuration activity.
5. Review the process of the configuration activity in the **Configuration Status** view.

Create a Template action

Allows you to use a monitored APC SNMP device's settings to create a template that can be used to configure monitored APC SNMP devices.

1. Select **Create a Template**, and click **Next**.
2. Use the "Select Configuration Source" display to select the APC SNMP device you want to use as the template source, and click **Next**.
3. Use the "Configure Device Settings" display to select, and edit, as needed, the settings you want to store in the template, and click **Next**.
4. Use the "Save Configuration Template" display to name the template, and to save it when you click **Finish**.

Edit a Template action

Allows you to rename, delete, or edit the settings for an existing template that can be used to configure the monitored APC SNMP devices.

1. Select **Edit a Template**, and click **Next**.
2. Use the "Select Configuration Source" display to select a listed template and do the following, as needed:
   - Click **Rename**, to change its name.
   - Click **Delete**, to delete it from the list.
   - Click **Next**, to use the "Configure Device Settings" display to select, and edit, as needed, the settings you want to store in the template.
     Note: When you click Next in the "Configure Device Settings" display, the "Save Configuration Template" display allows you to save the edited settings as the selected template, or to save the settings as a new template.

Configure Devices from a Template action

Allows you to use a previously saved template to configure monitored APC SNMP devices.

1. Select **Configure Devices from a Template**, and click **Next**.

2. Use the "Select Configuration Source" display to select the template you want to use as the configuration source, and click **Next**.
3. Use the "Select Destination Devices" display to select the APC SNMP devices you want to configure using the selected template, and click **Next**.
4. Use the "Configure Device Settings" display to select, and edit, as needed, the source template settings to be used to configure the same settings at the APC SNMP devices selected in the "Select Destination Devices" display, and click **Finish** to initiate the configuration activity.
5. Review the process of the configuration activity in the **Configuration Status** view.

"Select Configuration Source" display

Use this "APC SNMP Device Configuration" wizard display to select the APC SNMP device, or configuration template, you want to use as the source of your configuration activity.

The action selected in the "Select a Configuration Action" display affects what elements are available in the "Select Configuration Source" display.

Display for Configure Devices or Create a Template actions

Use this version of the "Select Configuration Source" display to select the APC SNMP device you want to use to configure other APC SNMP devices (Configure Devices action) or to create a template (Create a Template action).

Element	Description
Filter	Filter the table to list only entries that include the text you type, exactly as typed.
List	Select the APC SNMP device you want to use to create the new template, or to configure other APC SNMP devices directly from its settings. All APC SNMP devices monitored by the Data Center Expert server are listed. **Note:** In addition to standard identification information (**Hostname**, **Type**, **Model**, **Location**, and **IP Address**), the list also identifies when the settings for a device were last retrieved by the Data Center Expert server (**Last Retrieved** column), if at all (**Not Retrieved**).
Device File Transfer Settings	Click to access the "Device File Transfer Settings" display used to manage the File Transfer Protocol (FTP) or Secure Copy (SCP) access values for APC SNMPv1 and SNMPv3 devices.

Element	Description
Retrieve Device Settings	Click to force the Data Center Expert server to retrieve the most recent settings for a selected device. **Tip:** You must retrieve the settings for a device that reports **Not Retrieved** as its **Last Retrieved** status before you can use that device. **Note:** If a pop-up status message appears, you can click Status messages: Configuration Status view, a related information link provided below, for information about that message.
Next	Click to access the "Select Destination Devices" display (**Configure Devices** action), or the "Configure Device Settings" display (**Create a Template** action).
Back	Click to return to the "Select a Configuration Action" display.

Display for Edit a Template action

Use this version of the "Select Configuration Source" display to rename, delete, or edit the settings for an existing configuration template.

Element	Description
Filter	Filter the table to list only entries that include the text you type, exactly as typed.
List	Select the template you want to rename, delete, or edit.
Rename	Click to rename a selected template.
Delete	Click to delete a selected template.
Next	Click to edit a selected template using the "Configure Device Settings" display.
Back	Click to return to the "Select a Configuration Action" display.
Finish	Click to save your **Rename** or **Delete** changes, and exit the "APC SNMP Device Configuration" wizard. **Note:** Only enabled when you finish renaming or deleting at least one listed template.

Display for Configure Devices from a Template action

Use this version of the "Select Configuration Source" display to select the template you want to use to configure monitored APC SNMP devices.

Element	Description
Filter	Filter the table to list only entries that include the text you type, exactly as typed.
List	Select the template you want to use.
Next	Click to select the APC SNMP devices you want to configure using the "Select Destination Devices" display.
Back	Click to return to the "Select a Configuration Action" display.

"Select Destination Devices" display

Use this "APC SNMP Device Configuration" wizard display to select the APC SNMP devices you want to configure using another APC SNMP device (**Configure Devices** action) or a selected configuration template (**Configure Devices from a Template** action).

Note: Which configuration action was used to access this display has no affect on how the display is used.

Element	Description
Filter	Filter the table to list only entries that include the text you type, exactly as typed.
List	Select (check-mark) the devices you want to configure from the list of all APC SNMP devices monitored by the Data Center Expert server. You can select devices that are all the same model (Smart-UPS 750), all the same type (UPS), or any set of devices (Symmetra 80K, Integrated EMU, and APC Rack Manager, for example). **Note:** In addition to standard identification information (**Hostname**, **Type**, **Model**, **Location**, and **IP Address**), the list also identifies when the settings for a device were last retrieved by the Data Center Expert server (**Last Retrieved** column), if at all (**Not Retrieved**).
Device File Transfer Settings	Click to access the "Device File Transfer Settings" display used to manage the File Transfer Protocol (FTP) or Secure Copy (SCP) access values for APC SNMPv1 and SNMPv3 devices.
Retrieve Device Settings	Click to force the Data Center Expert server to retrieve the most recent settings for the

Element	Description
	device that is highlighted (actively selected) in the list. **Tip:** You must retrieve the settings for any device that reports **Not Retrieved** as its **Last Retrieved** status before you can configure that device using the selected configuration source (APC SNMP device or template). However, when multiple devices of the same model and firmware, are listed as **Not Retrieved**, retrieving the settings for one of those devices updates the **Last Retrieved** status for all of those devices: the Data Center Expert server recognizes that identical devices (same model and firmware version) have identical available settings. **Note:** If a pop-up status message appears, you can click Status messages: Configuration Status view, a related information link provided below, for information about that message.
Next	Click to access the "Configure Device Settings" display.
Back	Click to return to the "Select Configuration Source" display.

"Configure Device Settings" display

Use this "APC SNMP Device Configuration" wizard display to select, edit, and apply the settings for the configuration source selected in the "Select Configuration Source" display, at the APC SNMP devices selected in the "Select Destination Devices" display.

Typically, this display lists only the configuration source settings that can be used at all the selected destination devices: the **Show Shared Settings Only** is selected (check-marked). If you disable **Show Shared Settings Only**, all the configuration source settings are listed and identified as follows:
Note: If no source settings can be used at all of the selected destination devices, **Show Shared Settings Only** is disabled, by default.

- Black text identifies a settings category that has only settings that can be shared with all the destination devices, as well as individual settings that can be shared.
- Brown text identifies a settings category that has at least one setting that cannot be shared with all the destination devices, as well as individual settings that cannot be shared.
- Red text identifies a selected settings category that has at least one setting that has no value defined, as well as individual settings that have no value defined.
  Note: If no setting is selected, or a setting that cannot be shared with all the destination devices, or that currently has no value defined, is selected, you will be unable to initiate the configuration activity (**Finish** will be disabled).

Element	Description
List	Use to select the settings that have the configuration source values you want to share with the selected devices.
Edit	Click to edit the value for a selected setting. **Note:** If you select a setting that has no value currently defined, you must edit that setting to define a value before you can share it with the selected devices.
Back	Click to return to the "Select Destination Devices" display.
Finish	Click to apply the selected settings at the destination devices, and exit the "APC SNMP Device Configuration" wizard. **Note:** The status of the configuration activity will be reported in the **Configuration Status** view.

"Save Configuration Template" display

Use this "APC SNMP Device Configuration" wizard display to save edited settings for an existing (**Edit a Template** action) or new template (**Create a Template** action).

Element	Description
Configuration Name	Edit the template's name (**Edit a Template** action), if desired, or type in a new name (**Create a Template** action).
Filter	Filter the table to list only entries that include the text you type, exactly as typed.
List	Select a listed template to save the edited settings to that template rather than to the template you selected to edit (**Edit a Template** action) or to a new template (**Create a Template** action).
Back	Click to return to the "Configure Device Settings" display.
Finish	Click to save your changes, and exit the "APC SNMP Device Configuration" wizard. **Note:** When creating a new template, **Finish** is disabled until you provide some information in the **Configuration Name** text box .

"Device File Transfer Settings" display

Use this display to manage the File Transfer Protocol (FTP) or Secure Copy (SCP) access values for APC SNMPv1 and SNMPv3 devices.

Note: Functionally identical versions of this display are used by the "SNMPv1/SNMPv3 Device Discovery," "Apply Firmware Updates," and "APC SNMP Device Configuration" wizards, as well as by **Device File Transfer Settings**, an **SNMP Device Communication Settings** option in the **Device** menu. A change saved in one display is reflected in all.

- To use FTP for APC SNMP device access, FTP server access must be enabled at that device.
- To use SCP for APC SNMP device access, Secure Shell version 2 (SSHv2) console access must be enabled at that device.

Element	Description
List	Lists the access settings the Data Center Expert server can use for FTP or SCP access to its monitored devices. **Username**: The username used for access to a device. **Note:** By default, the Data Center Expert server can download firmware only to devices that use **apc** (lowercase) for the username and password (the actual password used for device access is identified in the "Edit Device File Transfer Settings" display). **IP or IP Range**: The IP address, or range of addresses, at which the access settings support FTP or SCP communication. **FTP Port**: The port used for FTP access to a device. **SCP Port**: The port used for SCP 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 try to access a device, after the initial attempt failed, before it stops trying to access that device (**1**, by default). **Protocol**: The protocol the transfer settings set will use to access devices (**FTP only**, **SCP only**, or **Try SCP, fall back to FTP**).
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 File Transfer Settings" display

Use this display to add or edit the settings the Data Center Expert server uses for File Transfer Protocol (FTP) or Secure Copy (SCP) access to APC SNMPv1 and SNMPv3 devices.

Note: Functionally identical versions of this display can be accessed from the "Device File Transfer Settings" displays used by the "Apply Firmware Updates," "SNMPv1/SNMPv3 Device Discovery," and "APC SNMP Device Configuration" wizards, and by **Device File Transfer Settings**, an **SNMP Device Communication Settings** option in the **Device** menu.

Element	Description
Username	Identify the name used for access to a device.
Password	Identify the password used for access to a device.
Verify Password	Retype the password.
IP or IP Range	Identify The IP address, or range of addresses, at which the access settings support FTP or SCP communication (***.*.*.***, by default).
Protocol	Identify whether the transfer settings will use FTP (**FTP only**), SCP (**SCP only**), or attempt to use SCP, but fall back to using FTP if SCP fails (**Try SCP, fall back to FTP**).
FTP Port	Select the port the server will use for FTP access to devices (**21**, by default).
SCP Port	Select the port the server will use for SCP access to devices (**22**, by default).
Timeout	Identify how long the server will wait before it considers that an attempt to access a device has failed (**3000**, by default).
Retry Limit	Select the number of times the server will try to access a device, after the initial attempt failed, before it stops trying to access that device (**1**, by default).

Device Configuration Status view

This view provides information about the status of an ongoing APC SNMP device configuration process, or the results of the most recently completed process, if any.

Note: For information about the **Status** reported for a device, see Status messages: Device Configuration Status view.

Element	Description
Filter	Filter the table to list only entries that include the text you type, exactly as typed.
List	Identifies each device that was included in the configuration process, by **Hostname**, **Model**, **Location**, **Status**, and **Time Completed**.
Configuration Progress	Reports the **In Progress**, **Completed**, and **Successful** status for the configuration process.
Configuration Results	Click to access the "Configuration Results" display for a selected device that reports a date and time (**Time Completed**), and other than **Configuration successful** for its **Status**. **Note:** This button is disabled for any device that was configured successfully, or for which the configuration is ongoing.

Status messages: Device Configuration Status view

The following error messages can be reported as the **Status** for a device while the configuration process is either ongoing, or completed.

Note: No information is provided for the three progress messages (**Retrieving configuration**, **Transferring configuration**, and **Waiting for configuration to load**), or for the **Configuration successful** message.

Message	Description
Incomplete configuration	The configuration finished, but not all settings were applied successfully. Either the destination device doesn't support the applied setting, or the configuration process failed to overwrite an existing setting value. **Recommended Action**: This can occur when different types of devices are selected for the source and destination devices (for example, a Rack PDU and Smart-UPS). Select devices that match, and try again. This can also occur when an applied value does not fall into the allowed values range/ list (such as a string that exceeds the maximum length, **False** rather than **Enabled**, etc.). **Note:** You can select the device and click **Configuration Results** to access the "Configuration Results" display and review the settings that failed to be configured.

Message	Description
Failed: Unable to connect	A network or file transfer protocol communication problem exists. **Recommended Action**: Make sure the device is turned on and online, the appropriate file transfer protocol is enabled at the device, and that the "Device File Transfer Settings" display settings used to access the device include the device's correct port number. Correct any network connection problem. **Note:** If the problem persists, contact APC Support (http://www.apc.com/support).
Failed: Unable to log on	The Data Center Expert server does not have the appropriate file transfer protocol 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 File Transfer Settings" display, and the appropriate file transfer protocol 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. **Note:** If the problem persists, contact APC Support (http://www.apc.com/support).
Failed: Unable to transfer configuration	A problem occurred, after the server logged on to the device successfully, that prevented the server from transferring the configuration. **Recommended Action**: Make sure the access settings have not changed at the server or device, and the appropriate file transfer protocol 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. **Note:** If the problem persists, contact APC Support (http://www.apc.com/support).
Failed: Unable to retrieve configuration	A problem occurred, after the Data Center Expert server transferred the configuration to the device successfully, that prevented the server from verifying that the

Message	Description
	configuration was successful by retrieving a copy of the configuration from the device. **Recommended Action**: Make sure the access settings have not changed at the server or device, and the appropriate file transfer protocol 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. **Note:** If the problem persists, contact APC Support (http://www.apc.com/support).
Failed: Connection timed out	A network or file transfer protocol communication problem prevented the Data Center Expert server from logging on before the **Timeout** identified in the "Device File Transfer Settings" display expired. **Recommended Action**: Make sure the device is turned on and online, and the appropriate file transfer protocol is enabled at the device. Also, make sure the "Device File Transfer Settings" display includes the correct access settings needed to access the device, and that the **Timeout** value is appropriate for the network traffic requirements. Correct any network connection problem. **Note:** If the problem persists, contact APC Support (http://www.apc.com/support).

"Configuration Results" display

This display provides information about the settings that failed to update for a selected device during a configuration process.

Note: For information about the **Status** reported for the selected device, see Status messages: Configuration Status view.

Element	Description
Section Name	Identifies the section that includes a setting that failed to be configured to use the source settings. For example, **SystemModem**, **EventLog**, and **DataLog** are three of the sections under the **Advanced Settings** category.

Element	Description
Key Name	Identifies the name of the setting that failed to be configured to use the source settings.
Expected Value	Identifies the value expected to be reported for the setting following the configuration process.
Actual Value	Identifies the value actually reported by the device following the configuration process. **Note:** The setting may not be shared by the source and destination (**Not Supported** reported for the **Expected Value**), the two devices may allow different values, or the set may have failed for an unknown reason. You can use **Launch to Device**, a right-click option in the **Device View** and **Map View**, to access the device to review its event log to see if it contains information about the error, or to review the user interface at the device to see the available settings, allowed values.

Changing the protocol used to monitor APC SNMP devices

You can change the protocol the Data Center Expert server uses to monitor APC devices discovered as SNMPv1 to SNMPv3.

Note: You can change the protocol only on APC SNMPv1 devices that support SNMPv3. For information about whether an APC SNMP device supports SNMPv3, consult the device documentation.
Before you begin, it is recommended you view and confirm the devices you want to convert from SNMPv1 to SNMPv3 in the "Device Scan Settings" display, accessed from the **SNMP Device Communication Settings** option in the **Device** menu.

1. Select the **APC SNMP Device Configuration** option in the **Device** menu.
2. Select **Configure Devices**.
3. Select the APC SNMPv3 device you want to use as the source.
4. Click **Retrieve Device Settings**.
5. Click **Next** to select the devices you want to convert to SNMPv3.

   To ensure only the devices you want to convert to SNMPv3 are selected, you can checkmark **Select/Deselect All** to clear the list, then checkmark the devices to include.
6. Expand **SNMPv1 Settings** and checkmark the **Access** option.
7. Double-click the **Access** option under **SNMPv1 Settings**, or select the **Access** option and click **Edit**, to change its setting to **Disabled**, if necessary.
8. Uncheck **Authentication** options 1 - 4, if necessary.
9. Expand the **SNMPv3 Settings** option.
10. Double-click the **Access** option under **SNMPv3 Settings**, or select the **Access** option and click **Edit**, to change its setting to **Enabled**, if necessary.
11. Expand the Authentication options 1 - 4 you want to use, select the **Access** option under each option, and click **Edit**, to change its setting to **Enabled**, if necessary.
12. Checkmark other available options to change their settings, if necessary.

The security settings on some target devices might require setting user passwords, authentication phrases, and encryption phrases manually at the device user interface.

13. Click **Finish**.

You can monitor progress applying the settings to the selected devices in the **Device Configuration Status** view, accessed from the **Device** option in the **Window** menu.

Surveillance Settings (Device menu)

Use this option's display to configure how the Data Center Expert server affects, and responds to, its monitored NetBotz Appliance cameras in all device groups.

Note: For more information about 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.

Manage Custom Property Keys (Device menu)

This option allows you to create, modify, and delete user-created property keys for devices or sensors.

You use this option to access the display used to add, modify, and delete user-created property keys for devices or sensors. Once a custom property key is created, a new column appears, with the custom property key as the column heading, in the **Device View**, **Custom Properties Editor** view, and the **View Device Sensors** display.
Note: You access the **View Device Sensors** display from the right-click option in the **Device View** and **Map View**.

This display allows you to manage custom property keys only. To identify the value associated with a custom property key, you use the **Add Custom Property** display in the right-click menu of the **Device View**, **Map View**, or **Custom Properties Editor** view. Until you identify a value for a property key, the fields in that property key column will be blank.

You can use the **Configure Columns** icon to show or hide custom property columns in either the **Device View** or the **View Device Sensors** display.

The **Manage Custom Property Keys** option in the **Device** menu, and the **Manage Custom Property Keys** icon in the **Custom Properties Editor** view, provide access to the **Manage Custom Property Keys** display.

"Manage Custom Property Keys" Display

Use this display to create, modify, or remove custom property keys.

Note: This display allows you to manage custom property keys only. To identify the value associated with a custom property key, you use the **Add Custom Property** display, accessed from the right-click menu of the **Device View**, **Map View**, or **Custom Properties Editor** view.

You can choose to display a new custom property key as a column in the Device View, or select it later in the Configure Columns display.

Element	Description
Add	Specify the name of the custom property key. **Note:** The property key cannot be blank.
Edit	Modify the name of the selected property key.
Remove	Remove one or more selected property keys.

Building Management Settings (System menu)

Provides access to a separately-licensed feature you can use to configure the Data Center Expert server's MODBUS TCP Output Module support for your Building Management System (BMS).

Note: Port 502 is used to connect a BMS to the MODBUS TCP Output Module support at the Data Center Expert server.
Three displays are used to configure MODBUS TCP Output Module support:

- **Building Management Settings**, used to select the devices on which to enable Modbus support, and assign the server addresses.
- **Modify Device Settings**, used to configure the server address for the selected device, and map sensors to registers.
- **Copy Register Map**, used to select the devices to which you want to copy a register map.

Note: Until you purchase and add the MODBUS TCP Output Module license to the Data Center Expert server using **License Keys**, a **Server Administration Settings** option in the **System** menu, you cannot configure the Building Management System support.

"Building Management Settings" display

Use this display to manage the server addresses assigned to monitored devices, and to access the "Modify Device Settings" display used to map the registers assigned to sensors at a selected device.

Note: Until the MODBUS TCP Output Module license is purchased and added to the Data Center Expert server using **License Keys**, a **Server Administration Settings** option in the **System** menu, the "Building Management Settings" display provides only an **Add License Key** button you can click to access the **License Keys** option. For more information about the MODBUS TCP Output Module support, see Data Center Expert v7.2.0 Addendum: Building Management System Integration, available at the APC Application Notes web page for the Data Center Expert product: https://www.se.com/vn/en/download/document/SPD_JRUK-7R4L9N_EN/

You can assign unique server addresses for up to 247 monitored devices; you can modify the settings for one device at a time, including the **Register** values for any or all of its sensors.

Element	Description
Filter	Filter the table to list only entries that include the text you type, exactly as typed.
List	Select one or more devices, to generate or remove server identifications (**Server Address**), or select a single device, to modify the device settings for its sensors. You can click on any column head (**Server Address**, **Hostname**, **Parent Device**,

Element	Description
	Location, **Device Type**, or **Model**) to sort the list. **Note:** All monitored devices are listed, unless filtered, but only a maximum of 247 devices can have server addresses assigned.
Select/Deselect All	Select (check-mark) or deselect all devices.
Modify Device Settings	Click to access the "Modify Device Settings" display for a selected device. **Note:** Disabled when more than one device is selected.
Generate Server ID's	Click to assign a **Server Address** to a selected device or devices. **Note:** Any device with an existing **Server Address** assignment will be unaffected.
Remove Server ID's	Click to unassign a **Server Address** for a selected device or devices.

"Modify Device Settings" display

Use this display to manage the register addresses assigned to the sensors at a selected device, including importing or exporting register map settings as an external *.csv file, and copying the register map settings to other devices.

Element	Description
Filter	Filter the table to list only entries that include the text you type, exactly as typed.
Select Device Server Address	Select a new server address for the device, if needed. **Note:** Only server addresses, from **1** through **247**, which are not mapped to another device are listed; **No Server Mapping** is selected when the device has no server address assigned, and can be used to change the device's server address to unmapped.
List	Select a sensor or sensors, to map **Register** values for those sensors or remove them from the list, or select a single sensor, to modify its **Register** value. You can click on any column head (**Register**, **Sensor**, **Units**, or **Details**) to sort the list. **Note:** All sensors for the selected device are listed, unless filtered.

Element	Description
Select/Deselect All	Select (check-mark) or deselect all sensors.
Modify Register	Click to edit or delete the **Register** value for a selected sensor. **Note:** Disabled when more than one sensor is selected.
Remove Registers	Click to remove the **Register** value for a selected sensor or set of sensors.
Generate Register Map	Click to map a **Register** value for the selected sensor or set of sensors. You can use any value between 31000 to 39999 for a single sensor; for a set of sensors, you can use any value that is at least 31000 for the start of the **Register** value range, as long as that value allows for mapping all of the sensors within the maximum range of 39999. If you select a single sensor, whether that sensor is mapped already, its value will map to the new value unless that value is assigned to another register. In that case, the next highest available value will be used. For example, if you define 31009 as the value, 31009 through 31058 are assigned to other sensors, 31059 will be assigned to the sensor. **Note:** To map a sensor to a value that is assigned to another register, you must either change or remove that value at the other register. If you select multiple sensors, the sensors are mapped sequentially from the sensor at the top of the list through to the sensor at the end of the list, except as follows: • Any values assigned to unselected sensors will be skipped. • If the starting value is assigned to an unselected sensor, the mapping will start at the next highest available value. For example, if you select 31005, and 31005 through 31050 are already assigned, 31051 will be the first **Register** value assigned.
Import Register Map	Click to apply the contents of a *.csv file for a previously saved register map to the list.
Export Register Map	Click to save a copy of the register map, as configured, as a *.csv file. **Note:** Do not edit the .csv file for an exported register map. Any errors made during editing can affect the MODBUS TCP

Element	Description
	Output Module support when that file is imported.
Copy Register Map	Click to copy the register map, as configured, to one or more devices using the "Copy Register Map to Device" display.

"Copy Register Map to Devices" display

Use this display to copy the register map settings from the source selected in the "Modify Device Settings" display to one or more of the devices monitored by the Data Center Expert server.

Note: Only register map settings that match settings at a selected device will be copied to that device.

Element	Description
Search	Filter the table to list only entries that include the text you type, exactly as typed.
List	Select the device or devices to which you want to copy register map settings from the source selected in the "Modify Device Settings" display. You can click on any column head (**Server Address**, **Hostname**, **Device Type**, **Model**, or **Location**) to sort the list. **Note:** All monitored devices are listed, unless filtered.
Select/Deselect All	Select (check-mark) or deselect all devices.

Surveillance feature

Surveillance is a license key-based upgrade designed for use with the Data Center Expert 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 Data Center Expert server, and the license has been enabled for each camera.

Users must be assigned Device Group Monitoring View Access or higher to view NetBotz Appliance camera images and clips in active and historical alarms.

Users must be assigned Device Group Surveillance View Access or higher to view and export surveillance clips.

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 Data Center Expert 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 enough Surveillance licenses available for the cameras at monitored NetBotz Appliances, a message is displayed at the top of the **Surveillance Settings** display.
Each Data Center Expert server comes with a one-node Surveillance license that allows you to evaluate the Surveillance features before purchasing additional licenses. The one-node Surveillance license does not expire. When any additional Surveillance 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 the **System** menu.
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 **Surveillance Settings** for one or more cameras.

1. Select **Surveillance Settings** in the **Device** 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.
2. In the "Surveillance Settings" display, to enable multiple cameras at the same time, select the cameras to be licensed.
3. Enable the License Camera option at the top of the display.

Surveillance deployments and Data Center Expert server performance

The number of cameras licensed for surveillance, and the surveillance settings for those cameras, can affect Data Center Expert server performance.

The **Camera Resolution** and **Target Image Capture Rate** (frames per second) you specify in the **Surveillance Activation Settings** section of the "Surveillance Settings" display determine the amount of data generated. To support a large volume of surveillance data, the maximum recommended number of cameras licensed for surveillance, and their surveillance activation settings, are the following:

- Basic server: A maximum of 15 cameras at 10 frames per second (150 fps total for all cameras) and a resolution of 640x480.
- Standard server: A maximum of 125 cameras at 2 frames per second (250 fps total for all cameras) and a resolution of 640x480.
- Enterprise server: A maximum of 250 cameras at 2 frames per second (500 fps total for all cameras) and a resolution of 640x480.

With the maximum recommended number of cameras licensed, Data Center Expert server performance can be affected when:

- SNMP or Modbus devices are also monitored by the Data Center Expert server.
- The Data Center Expert server connects to the camera using SSL, specified in the **Server Settings** section of the "Surveillance Settings" display.
- System activity, such as performing a server backup or purge, or exporting a large report, is occurring.

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 **Alarm Configuration** 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 **Device** menu option, allow you to perform all Data Center Expert 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: Some right-click menu options in the **Monitoring** perspective (**Enter/Exit Maintenance Mode**, **Create Thresholds** , 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 **Device** 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.

Note: If a NetBotz Appliance is mapped to an external share drive, a **Store Data on NetBotz Appliance** option is available in the "Surveillance Settings" display for each camera associated with that appliance. If that option is selected for a camera, its **Thumbnail** view cannot update, as thumbnail data cannot be sent to the Data Center Expert server. However, its **Camera View** will still provide real-time video, and its clip data, which is stored at the external share drive at the NetBotz Appliance, can still be accessed by the Data Center Expert server.
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, an 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 Data Center Expert 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 **Device** menu allows you to configure cameras for all device groups; **Surveillance Settings** in the **Device Groups** view allows you to configure cameras for a selected device group; **Surveillance Settings** in the **Camera** view allows you to configure one camera 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 **Change Resolution** icons ( ) to select to display small (**160x120**) or large (**320x240**) thumbnails.
- Use the **Toggle Extra Thumbnail Borders** ( ) to select whether the thumbnails include a border.
- Use the **Configure Thumbnail Details** 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 **Show in Monitoring Perspective** in the thumbnail's right-click menu).

Button icons (Thumbnails view)

In addition to standard minimize and maximize icons, five icons are available to perform specific **Thumbnails** view and surveillance functions.

Icon	Description
	Click the chevron associated with this icon to select to display small (**160x120**) or large (**320x240**) thumbnails.
	Click this **Toggle Extra Thumbnail Borders** icon to select whether the thumbnails include a border.
	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.

Icon	Description
	Click this **Retrieve Clips** icon to access the "Recorded Camera Clips" display for the selected cameras.
	Click this **Configure Thumbnail Labels** icon to select the camera-associated data to display under each thumbnail. • **Pod Label** • **Hostname** • **Location** • **Status** • **Licensed** • **Model** • **Device Groups** • **Camera Label**

"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
Pod Label	Sort by **Pod Label**.
Location	Sort by **Location**.
Status	Sort by **Status**.
Camera Label	Sort by **Camera Label**.
Model	Sort by model number of the camera's NetBotz Appliance.
Hostname	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.

"Configure Thumbnail Details" display

Use this display to select the camera-associated data that appears under each thumbnail in the **Thumbnails** view.

Element	Description
Pod Label	The label that identifies the pod.
Location	The location of the camera, if known.
Status	The status of the camera: **Online** or **Offline**.
Camera Label	The label that identifies the camera.
Model	The model number of the camera's NetBotz Appliance.
Hostname	The IP address or hostname.
Licensed	The license status.
Device Groups	The device groups to which the cameras are assigned.

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 **Pod Label**, **Camera Label**, **Hostname**, **Location**, **Status**, **Licensed**, **Model**, and **Device Groups** 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 the chevron associated with this **Change Resolution** icon to select the

Icon	Description
	resolution you want to use to display the real-time feed for the selected camera.
	Click this **Retrieve Clips** icon to view, tag, export, and delete existing surveillance clips.

You can use the right-click menu in the real-time feed area to do the following:

- Access the "Recorded Camera Clips" display to retrieve, view, and tag clips for the camera (**Retrieve Clips** option, or use the icon).
- Access the "Surveillance Settings" display to configure the camera (**Surveillance Settings** option).
  Note: **Surveillance Settings** in the **Device** menu allows you to configure cameras for all device groups; **Surveillance Settings** in the **Device Groups** view allows you to configure cameras for a selected device group; **Surveillance Settings** in the **Thumbnails** view allows you to configure selected cameras for a selected device group.
- Access the "Device Launch Settings" display to define the settings used to access the web interface at the camera's NetBotz Appliance (**Device Launch Settings** option).
- Launch to the web interface at the camera's NetBotz Appliance (**Launch to Device** option).
- View the Device View listing for the camera in the Monitoring perspective (**Show in Monitoring Perspective** option).
- Access the "Camera Settings" display to configure the camera at the monitored NetBotz Appliance (**NetBotz Appliance Camera Settings** option).

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 Data Center Expert 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" display associated with **Camera Settings**, a **NetBotz Appliance Configuration** option in the **Device** menu, and with **Camera Settings**, a right-click **NetBotz Appliance Configuration** menu option in the **Device Groups** view.

The **NetBotz Appliance Camera Settings** option 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 choose which camera you want to configure.
- "Camera Settings" display: accessed either from the **Configure Selected Camera** button, 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 Capture Data**: 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 Configuration** option in the **Device** 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 Configuration (Device menu).

Surveillance Settings options

Four options are available to access a "Surveillance Settings" display used to configure how the Data Center Expert server affects and responds to cameras at monitored NetBotz Appliances.

- Select **Surveillance Settings** in a right-click menu for a selected camera's thumbnail when only that thumbnail is selected in the **Thumbnails** view.
- 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 **Device** menu to configure cameras for all device groups.

"Surveillance Settings" display

Use this display to configure how the Data Center Expert server affects and responds to cameras at monitored NetBotz Appliances.

General Surveillance Settings

These settings are used by the Data Center Expert 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:** A status message appears when there are not enough surveillance licenses available for the selected cameras.
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.
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.
Store Data on NetBotz Appliance	Select to have camera data stored at the share drive mapped at the camera's NetBotz Appliance, instead of at the Data Center Expert server. When selected, the **Camera View**, which provides a real-time feed, will continue to operate properly, and clip data, which is stored at the external share drive at the NetBotz Appliance, can still be accessed by the Data Center Expert server; however, the **Thumbnail** view for the camera cannot update while this option is selected. **Note:** This option is available only when a NetBotz Appliance that supports using an external share drive for storage is mapped to a such a drive.

Server Settings

These settings are used to identify the Data Center Expert 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
Data Center Expert server	Identify the name of the Data Center Expert server where data from the selected camera will be sent. **Note:** By default, the name of the current Data Center Expert 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 Data Center Expert server's **Web Server** tab for **Server Access**, a **Server Administration Settings** option in the **System** 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 Data Center Expert 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** : the camera will send clip images to be stored whenever an alert triggers the camera. **Send on Motion Detected During Alerts** : 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 Settings option (NetBotz Appliance Configuration option).
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 Data Center Expert 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.
Surveillance Scheduling	Click to use the "Surveillance 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 **Surveillance Scheduling** option on the "Surveillance Settings" display.

Send Continuously During Alerts *:*
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 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 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 *:*

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** 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 **Surveillance 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.

"Surveillance 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 Data Center Expert server or the NetBotz Appliance has surveillance disabled; both must have surveillance enabled, to capture data.

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 **Device** 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 **Device** 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 Data Center Expert 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 **System** 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.

Data Center Expert ships with a Windows batch file and a Linux script located at the root directory of the Data Center Expert 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 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: • **Pod Label**: the label that identifies the pod. • **Camera Label**: the label that identifies the camera.
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** • **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.