

Place Dealer Sticker Here

# USER & SETUP MANUAL



<b>Table of Contents</b>	<b>Page</b>
Network Administrators Information	4
Initial System Setup Checklist	6
<b><u>Monitor Menu</u></b>	7
Activity Log	7
Cameras	10
Camera Views	11
Floor plans	12
Monitoring Desktop	13
Portal Unlock	14
<b><u>Administration Menu</u></b>	15
Arm Alarm Panel	15
Lost Cards	15
<b>People Menu</b>	16
Add	16
Change/delete	16
<b>Reports Menu</b>	17
Configuration	17
History	18
People	19
Schedule Action	21
Set Threat Level	22
Utility	22
<b><u>Setup Menu</u></b>	23
<b>Access Control Menu</b>	23
Access Levels	24
Card/Keypad Formats	25
Elevators	26
Person Sections	26
Portal Groups	26
Portals	27
Reader Groups	29
Reader/Keypads	30
Utilities	31
<b>Alarms Menu</b>	32
Alarm Panels	32
Input Groups	32
Inputs	33
Event Groups	34

Events	35
Output Groups	36
Outputs	37
Temperature Inputs	38
Virtual Inputs	39
<b>Cameras Menu</b>	40
Camera Groups	40
Configure DM_DVR	41
Configure Milestone NVR	42
Configure OnSSI NVR	43
Definitions	44
Menu Order	45
Presets	45
Types	46
Views	47
<b>Floor plans Menu</b>	48
Configure	48
Floor plan Groups	49
Upload	49
<b>Network Resources Menu</b>	50
Domain Name Servers	50
Email Settings	51
FTP Backup	51
Network storage	52
Time Servers	53
<b>Site Settings Menu</b>	54
Add Software License	54
Network Controller	54
System Rules	56
Network Nodes	57
User Roles	60
<b>System Maintenance Menu</b>	61
Backup Database	62
Restore Database	62
Update Software	63
Utilities	63

<b>Threat Levels</b>	66
Add/change/delete	66
Menu Order	67
Settings	68
Threat Level Groups	68
<b>Time Menu</b>	69
Holidays	69
Network Controller	70
Time Spec Groups	70
Time Specifications	71
<b><u>Support/Utility Menu</u></b>	72
About	72
Change Password	73
Dealer and Support Info	73
How to Use Help	73

## Information for Network Administrators

### How Nodes and the Network Controller Use the Network

1. When a Node boots it initially selects for itself a temporary random IP address in the zeroconf address space (169.254.X.Y where X and Y are randomly selected).
2. The Node then multicasts for a Network Controller at 224.0.72.62 UDP port 7262, and presents its Unique Identifier (UID).
3. A Network Controller answers the multicast at 224.0.72.62 UDP port 7262 providing its own IP address and presents an addressing method for the Node.

See Node Addressing Settings in Init Mode.

**There are three IP addressing methods available:**

1. **An existing DHCP server on the network can assign IP addresses.**
2. **A Static IP address can be assigned using nconfig.exe (This application is on the CD provided with the Network Controller).**
3. **The Network Controller can provide IP addresses to Nodes only from a specified address range.**
4. Once a proper IP address for the Node is selected further communications between Node and Network Controller occur directly between their respective IP addresses using TCP port 7262.
5. The Network Controller may also require:
  - TCP Port 23 open for Telnet server access. This can be used for remote debugging. The Telnet Server is disabled by default.
  - TCP Port 3000 open for communication from video management system inputs.
  - TCP Port 3306 open for MySQL report usage.

### **Network Port Usage Table (versions 1.4 and higher)**

TCP Port 80	Must be open to the Network Controller for Browsers to access the Security Application. This can be configured on a different port.
TCP Port 443	Must be open to the Network Controller for Browsers to access the Security Application using HTTPS (SSL). This can be configured on a different port.
TCP Port 7262	Must be open to the Network Controller for communications between the Controller and Nodes. Be sure that this port is open through routers and firewalls for any Nodes on different subnets from the Network Controller. (Communications between Controller and Nodes are authenticated and card downloads are encrypted for security.)
TCP Port 23	Must be opened to the Network Controller using a jumper on the Controller module for Telnet access to the Controller.
TCP Port 3000	Must be open to the Network Controller for the Video Management System virtual inputs to communicate camera up/down and motion detection messages.
TCP Port 3306	Must be open to the Network Controller for MySQL report usage.

TCP Ports 20, 21	<p>When using active FTP these ports must be open to the FTP server for FTP backups from the Network Controller.</p> <p>When using passive FTP port 20 will not be required.</p> <p>Ports must also be left open to the Network Controller for FTP server responses. The network administrator must set up these ports.</p>
------------------	---

**Network Port Usage Table (up to version 1.3)**

TCP Port 69	<p>Must be open to the Network Controller for the on-board TFTP server to pass software updates to the Nodes. This port can be opened temporarily for updates and then closed again.</p>
-------------	--

**NOTE: If you are updating a system from version 1.3 or lower you will need to leave port 69 open until the software update is complete. Once your version is 1.4 or higher you can close port 69 as it will no longer be needed.**

See Also: IP Setup Using Init Mode  
 Assigning Nodes Static IP Addresses

**Initial System Setup Checklist**

For initial system setup follow the order of this checklist. The checklist is ordered to ensure that prerequisite steps are completed first. Use the Back button to return here after each step is completed.

For **Login** the default **User name** is "admin." The default **Password** is "admin."

When system setup is completed be sure to change the ?admin? account password. Select **Support/Utilities** : [Change Password](#). Give the new password for the admin account to the network administrator or security director.

1. Entering Site Settings
  - [Network Controller](#)
  - [Network Nodes](#)
2. Setting up Time Specifications
  - [Holidays](#)
  - [Time specs](#)
3. Setting up Alarms
  - [Outputs](#)
  - [Output Groups](#)
  - [Events](#)
  - [Inputs](#)
  - [Input Groups](#)
  - [Alarm Panels](#)

4. Setting up Access Control

- [Card Formats](#)
- [Person Sections](#)
- [Readers](#)
- [Reader Groups](#)
- [Portals](#)
- [Portal Groups](#)
- [Elevators](#)
  - [Floors](#)
  - [Floor Groups](#)
- [Access Levels](#)

5. Setting up Cameras

- [Types](#)
- [Definitions](#)
- [Menu Order](#)
- [Presets](#)
- [Views](#)
- [Video Management System](#)

6. Setting up Floor plans

- [Upload](#)
- [Configure](#)

7. Setting up Network Resources

- [Domain Name Server](#)
- [Email Settings](#)
- [Network Storage](#)
- [Time Server](#)

8. System Maintenance

- [Upload the Support.htm file](#)
- [Backup Database](#)

See also: [Setup Menu](#)

The printed "Installation Guide"

## **Monitor Menu**

View system activity and cameras.

<b>Choose this</b>	<b>To see Help for this</b>
<a href="#">Activity Log</a>	View logs of recent system activity.
<a href="#">Cameras</a>	View individual cameras.
<a href="#">Camera Views</a>	View pre-defined groups of cameras.
<a href="#">Floor plans</a>	View the state of alarms and other system resources on a floorplan.
<a href="#">Monitoring Desktop</a>	View alarms, logs, cameras and other system information from one desktop.
<a href="#">Portal Unlock</a>	View a list of portals and unlock a portal.

## **Monitoring the Activity Log**

Select **Monitor : Activity Log**.

**NOTE:** You can also see the activity log on the Monitoring Desktop.

The Activity Log displays the 300 most recent entries in the log of system activity. The messages are color coded.

**Red** indicates a process failure or access control issue.

**Green** indicates a successful process.

Black is used for all other messages.

Log messages contain message text and a number of variables as described below.

### **Names**

Specific names entered into the system during setup and configuration will be used in log entries in place of variables such as: <username>, <portalname>, <nodename>, <eventname>, <elevatorname>, <alarmpanel>, and <threatlevel>. This is a strong reason for assigning names that are descriptive. The log will be much easier to understand.

### **Numbers**

Specific numbers will be used in log entries in place of <ipaddress>, <slotnumber>, and <rev>.

### **Reset Types**

Specific <reset\_type> messages for the "Network Node Ident" log entry include:

- **Power on reset** - The node reset on power up.
- **Watchdog timer reset** - The node was rebooted using the Reboot command on the Site Settings : Network Nodes page.
- **Normal reset** - Physical reset by pushing the node reset button on the controller/node blade.
- **Network loss** - No reset has occurred. The node lost network connectivity but has now reconnected.



## Reason Codes

Specific [<reasoncode>] messages for "Access denied" log entries include:

- **[NOT IN NODE]** - The network node has no record of this badge.
- **[TIME]** - Time specifications do not allow access for this person at this time.
- **[LOCATION]** - This persons access level does not allow the use of this reader.
- **[PASSBACK]** - This badge was used previously in this reader group and the anti-passback duration timer has not yet expired.
- **[EXPIRED]** - This badge is expired.
- **[BIT MISMATCH]** - The data format of this badge does not match any data format configured in the system.
- **[WRONG DAY]** - Time specifications or Holiday definitions do not allow access for this person on this day.
- **[THREAT LEVEL]** - This persons access level does not allow access under the current system threat level.
- **[PIN]** - Incorrect PIN entry.
- **[NO PIN]** - No PIN was entered within the **Pin entry timeout** setting on the Network Controller page.

There is only one [<reasoncode>] message for "Access granted" log entries.

- **[PASSBACK]** - This badge was used previously in this reader group and the anti-passback duration timer has not yet expired. However, this person's access level has set the **Accept and Log** selection for **Action on Passback Violation**.

## Log Entries

The following is a complete list of possible activity log entries:

- Access granted [<reasoncode>] for <username> at <portalname>
- Access denied [<reasoncode>] by <username> at <portalname>
- Portal held open at <portalname>
- Portal forced open at <portalname>
- Portal restored at <portalname>
- Network controller startup
- Network node startup IP address <ipaddress> for <nodename>
- Momentary unlock at <portalname>
- Unlock at <portalname>
- Relocked at <portalname>
- Network node timeout IP address <ipaddress> for <nodename>
- Network node restored IP address <ipaddress> for <nodename>
- Network node disconnect IP address <ipaddress> for <nodename>
- Network node connected IP address <ipaddress> for <nodename>
- Network node IDENT (Rev <rev>, <reset\_type>) for <nodename>
- Network node data disconnect IP address <ipaddress> for <nodename>

- Network controller new database
- Log archive succeeded
- Log archive failed
- Logged in IP Address <ipaddress> by <username>
- Logged out IP Address <ipaddress> by <username>
- Failed login IP Address <ipaddress> (username <username>)
- Response to network node IP address <ipaddress>
- Unknown network node IP address <ipaddress>
- Request momentary unlock by <username> at <portalname>
- Session expired IP address <ipaddress> for
- Portal restored at <portalname>
- Event deactivated for <eventname>
- Event activated for <eventname>
- Network node tamper alarm IP address <ipaddress> for <nodename>
- Network node DHCP failed IP address <ipaddress>
- Access granted [<reasoncode>] for <username> at <elevatorname>
- Access denied [<reasoncode>] by <username> at <elevatorname>
- Threat level set <threatlevel> by <username>
- Threat level set (API) <threatlevel>
- Threat level set (ALM) <threatlevel>
- Network node file xfer start <filename> for <nodename>
- Network node file xfer end <filename> (<result>) for <nodename>
- License read failure
- FTP backup complete
- FTP backup failed
- Alarm panel armed <alarmpanel>
- Alarm panel disarmed <alarmpanel>
- Panel arm failure <alarmpanel>
- Panel disarm failure <alarmpanel>
- Panel arm interrupted <alarmpanel>
- Blade not responding slot <slotnumber>
- NAS backup complete
- NAS backup failed
- Event acknowledged by <username> for <eventname>
- Event actions cleared by <username> for <eventname>
- Access not completed for <username> at <portalname>

## Monitoring Cameras

Select **Monitor : Cameras**.

On this page you can:

- Select and aim a camera for viewing. You can select IP cameras or DVR cameras.
- Select a portal from the **Select Portal** drop-down and unlock the door temporarily

### To send camera images to a monitor for viewing:

1. Select **Monitor : Cameras**.
2. You can now select any camera in the system from the **Cameras** menu.

The controls at the bottom of the camera monitor pane allow you to aim cameras, move them to their home position, and zoom in or out if you have setup the pan, tilt, and zoom URLs on the [Setting up Camera Types](#) page.

Clickable icons in the monitor window allow you to execute the following actions:

**NOTE:** If the camera does not have these capabilities, or you have not setup the home, tilt, pan and zoom URLs these controls will not appear.



Click this to open a video browser window. Using the video browser window you can monitor a live feed, rewind, fast forward, pause, and go forward and back one frame at a time to find a specific sequence.



Click this to move the camera to its preset home position.



Click the arrows to move the camera one step in the arrow direction.

**NOTE:** If the camera is connected to a Dedicated Micros DVR then a single click starts the camera movement and a second click is required to stop the camera movement. If the camera moves too quickly for accurate positioning then select a lower speed number from the camera speed drop-down. (See below.)



Click this to zoom in.



Click this to zoom out.



Select from this drop-down the speed of camera movement. 1 is the slowest, 10 is the fastest.

## Monitoring Camera Views

Select **Monitor : Camera Views**.

On this page you can monitor a four-camera view or a picture-in-a-picture view.

### **The Picture-in-Picture and Quad Views**

The Picture-in-Picture (**PIP**) view displays one camera in a thumbnail image in the lower right corner of the screen and any other camera in the main image of the screen.


The **Quad** view displays 4 cameras in one screen.


### To move any camera in a multi-camera view:


1. Click in the pane displaying the camera view you wish to adjust. The pane will highlight with a red outline to show that it is selected.

2. From the **Camera Preset** drop-down list select the preset position you wish to see displayed. (This drop-down list automatically fills with the presets of the selected camera.)
3. You can also adjust the position of any camera using the icons:


**NOTE: If the camera does not have these capabilities, or you have not setup the home, tilt, pan and zoom URLs these controls will not appear.**


 Click this to open a video browser window. Using the video browser window you can monitor a live feed, rewind, fast forward, pause, and go forward and back one frame at a time to find a specific sequence.


 Click this to move the camera to its preset home position.

 Click the arrows to move the camera one step in the arrow direction.

**NOTE:** If the camera is connected to a Dedicated Micros DVR then a single click starts the camera movement and a second click is required to stop the camera movement. If the camera moves too quickly for accurate positioning then select a lower speed number from the camera speed drop-down. (See below.)

 Click this to zoom in.

 Click this to zoom out.

 Select from this drop-down the speed of camera movement. 1 is the slowest, 10 is the fastest.

#### **To select a camera for the Picture-in-Picture thumbnail:**

1. From the **Camera** drop-down list select a camera.
2. The camera you selected displays in the main image.
3. Click in the Pip view.
4. The Pip view now displays the same camera as the main image.
5. You can now select again from the **Camera** drop-down list to have any other camera display in the main image.

### **Monitoring Floorplans**

Select **Monitor : Floorplans**.

On this page you can:

- View any floorplan that is configured in the system.
- See the locations of portals, cameras, and temperature sensors.
- Display temperature graphs for each temperature point.
- Setup and Perform scheduled or momentary portal unlocks.
- Setup and Perform scheduled arming or disarming of inputs.
- Setup and Perform scheduled activate or deactivate of outputs.
- Display thumbnail images from each camera.

**NOTE:** Viewing and configuring floorplans requires a browser plug-in from Macromedia called Flash Player 9.0 or later.

## **Monitoring Floorplans**

1. Select from the **Floorplan** drop-down the floor you wish to monitor.
2. Select any resource (camera, portal, or alarm) on the floorplan and the **Name** and **ID** of that resource appears in the **Resource Name** and **ID** text boxes.

**NOTE:** Selected icons are slightly grayed.

3. Right click anywhere on the floorplan and the Flash Player menu displays. You can use the options on this menu.
4. Left click and hold on any icon and a menu displays.
5. You can click on a portal icon and select **Momentary Unlock** or [Schedule Action](#).

**NOTE:** Upon any valid entry through a portal the name of the cardholder entering displays beneath the portal icon.

6. You can click on an input icon or an output icon and select [Schedule Action](#).
7. You can click on a camera icon and select a thumbnail image.
8. You can click on a temperature icon and select a temperature graph.
9. Alarm icons turn red if that [alarm event](#) is triggered.

## **The Monitoring Desktop**

Select **Monitor : Monitoring Desktop**.

The Monitoring Desktop tabbed pages display all system functions that can be monitored.

## **Events Tab**

By default events display sorted in priority order. You can click on the arrow next to the column title **Priority** to reverse the sort order. You can also click to the right of the column titles **Date/Time** and **Name** to sort events by those columns.

Events will display as long as they are still active and/or require acknowledgment.

Clickable icons on the events page allow you to execute the following actions:



Click the camera icon to display the video browser. Using the video browser window you can monitor a live feed, rewind, fast forward, pause, and go forward and back one frame at a time to find a specific sequence.



Click the **Details** button and an additional window displays the Operator long message from the [Setting up Alarm Events](#) page.



Click the **Camera** button to display the camera associated with that alarm event in the upper camera monitor.



Click the **Acknowledge** button to acknowledge the event. Otherwise the event will remain active until the event actions are concluded or the **Maximum Duration** counter from the Setting up Alarm Events page expires and the event auto-acknowledges.

Click the **Clear Actions** link to stop the alarm event actions from occurring.

## **Activity Log Tab**

The Activity Log displays the 300 most recent entries in the log of system activity.

See also: Monitoring the Activity Log.

## Cameras Tab

You can select any camera configured in the system for viewing.

See also: Monitoring Cameras.

## Camera Views Tab

You can monitor a four-camera view or a picture-in-a-picture view.

See also: Monitoring Camera Views.

## Floorplans Tab

You can monitor any floorplan that is configured in the system.

**NOTE:** Viewing and configuring floorplans requires a browser plug-in from Macromedia called Flash Player 9.0 or later. Your operating system and browser will automatically determine which version of the plug-in to install.

See also: Monitoring Floorplans.

## Camera Monitors

Select from the drop-down above the camera image the specific camera you wish to have displayed in the monitor pane. You can select IP cameras or DVR cameras.

Select from the drop-down beneath the camera image the preset position you wish to set the camera to.

**NOTE:** The preset positions must already be defined at each camera web site and they must already be created in the security system.

Clickable icons in the monitor window allow you to execute the following actions:

**NOTE:** If the camera does not have these capabilities, or you have not setup the home, tilt, pan and zoom URLs these controls will not appear.



Click this to take a snapshot of the current camera image.



Click this to open a video browser window. Using the video browser window you can monitor a live feed, rewind, fast forward, pause, and go forward and back one frame at a time to find a specific sequence.



Click this to move the camera to its preset home position.



Click the arrows to move the camera one step in the arrow direction.

**NOTE:** If the camera is connected to a Dedicated Micros DVR then a single click starts the camera movement and a second click is required to stop the camera movement. If the camera moves too quickly for accurate positioning then select a lower speed number from the camera speed drop-down. (See below.)



Click this to zoom in.



Click this to zoom out.



Select from this drop-down the speed of camera movement. 1 is the slowest, 10 is the fastest.

## **Unlocking Portals**

Select **Monitor : Portal Unlock**.

On this page you can:

- Perform a momentary unlock of any portal.
- Specify and perform a scheduled extended unlock of any portal.

### **To perform a momentary unlock of a portal:**

1. In the **Name** column find the portal that you wish to unlock.
2. Click the **Unlock** link in the **Momentary Unlock** column. The portal will unlock for the unlock duration setup with the portal.

### **To perform an extended (Scheduled) unlock of a portal:**

1. In the **Name** column find the portal that you wish to unlock.
2. Click the **Schedule** button in the **Extended Unlock** column. A **Scheduled Action** pop-up page appears.
3. In the **Action** column select **Lock** or **Unlock** from the drop-down.
4. In the **Start Date/Time** column the current time is the default. You can change this time if you wish or you can click the **In** button and enter a time delay in hours and minutes. The action will begin when this time has elapsed.
5. In the **End Date/Time** column you can enter a specific date and time for the action to end or you can click the **After** button and enter a duration in hours and minutes. The action will end after this duration.

**For Example:** Select **Unlock** and leave the **Start Time** at **Now**. Set the **End Time** to **After** 1:30 (one hour and thirty minutes). Click **Save**. The portal will unlock immediately and stay unlocked for one hour and thirty minutes.

## **Administration Menu**

Maintenance and viewing of system activity and people information.

<b>Choose this</b>	<b>To see Help for this</b>
<a href="#">Arm Alarm Panel</a>	Arming and disarming alarm panels.
<a href="#">Lost Cards</a>	Determine the owner of a lost card.
<a href="#">People</a>	Maintain people information and their access privileges.
<a href="#">Reports</a>	Review the current setup of the system and previous activity in the system.
<a href="#">Schedule Action</a>	Specify a schedule for activating/deactivating outputs, disarming inputs, or locking/unlocking portals.
<a href="#">Set Threat Level</a>	Setting or changing the system threat level.
<a href="#">Utility</a>	Database backups, photo ID layout upload and delete.

## **Arming and Disarming Alarm Panels**

Select **Administration : Arm Alarm Panel**.

On this page you can:

- Arm or disarm an alarm panel.

### **To arm/disarm an alarm panel:**

1. The Administration Arm Alarm Panel page displays a table listing all alarm panels configured in the system, their current state, and any activity information.
2. Click the **Arm/Disarm** link in the **Action** column.

**NOTE:** You cannot arm a panel if it shows any zone activity.

3. A password challenge is displayed and you must enter your password to arm, or disarm, the panel.
4. If you are arming the panel the [Panel arming warning output](#) activates for the Warning duration.

## **Lost Cards**

Select **Administration : Lost Cards**.

If a card is found and turned in you can determine the identity of the card holder.

1. In the **Hot stamp #** text box enter the number on the card and click the **Search** button.
2. If there is no number printed on the card click the **Use Reader** link and a small reader window will appear.
3. Select a reader from the **Reader** drop-down list and swipe the card through that reader. The card number will fill the **Hot stamp #** text box.
4. Click the **Search** button.



## People Menu

Maintain information about system users.

Choose this	To see Help for this
Add	Add a person to the system.
Change/delete	Edit or delete a person's information.

## Adding a Person

Select **Administration : People : Add**.

A person must first be added to the system before [issuing a card](#), [assigning an access level](#), or [printing a badge](#).

### To add a person to the system:

1. In the text boxes enter **Last Name** and **First Name**.
2. **Activation Date/Time** defaults to today but can be changed.
3. For this record to be temporary you must enter an **Expiration Date/Time**. This person's record and any cards issued to this person will expire on the expiration date at the time entered.

**NOTE:** Activation date can be more recent than Expiration date. This may happen when re-activating a person's record after it has previously expired. The most recent date takes precedence. This record will be active but we recommend that the old expiration date be deleted.

4. If your organization issues ID numbers this can be entered in the **ID#** text box.
5. If your organization uses personal identification numbers enter this 4 digit number in the **PIN** text box.
6. Click **Next**.

The page will refill with confirmation that the person has been added to the system. Additional fields required for personal information and issuance of cards will also display in a tabbed format.

## Adding/Changing Personal Information

### To add a person:

1. Select **Administration : People : Add**.
2. The [add Personal Information](#) page displays.

### To change a particular person's record:

1. Select **Administration : People : Change/delete**.
2. You can search for person records by using any of the fields offered.
  - Fields marked with an asterisk will find complete exact matches only. For example, if you enter an **ID#** of 123 and the person's ID# is 1234, no matches will be found.
  - Fields not marked with an asterisk can find partial matches. For example, enter the first letter of the **Last Name** and click **Search**. A list of all people whose last names begin with that letter will be displayed.

- Entries in multiple fields must match on all fields. For example, enter the first letter of the **Last Name**, a **Department** name, and click **Search**. A list of all people whose last names begin with that letter AND whose department name also matches, will be displayed.
3. If you wish to also see deleted records check the **include deleted records** box.
  4. If you wish to see expired records check the **include expired records** box.
  5. Click the **Search** button.
  6. The [full Personal Information](#) page, or a list of all matched names, displays. If the search returns a list of names, click on the name of the person whose record you wish to edit.
  7. Make any needed changes on the full Personal Information page.
  8. Click **Save**.

## **Reports Menu**

A variety of system information reports.

<b>Choose this</b>	<b>To see Help for this</b>
<a href="#">Configuration</a>	Reports on the current configuration of system resources.
<a href="#">History</a>	Reports on system activity history.
<a href="#">People</a>	Reports on access information pertaining to people.

## **Configuration Reports**

Select **Administration : Reports : Configuration**.

### **Cameras Report**

Displays all camera configuration information.

### **Camera Presets Report**

**Displays configured presets for each camera in the system. These presets must be set at each camera web site.**

### **Elevators Report**

Displays elevator configuration information including Node, Reader, and Floor to output mappings.

See also: [Defining Elevators](#)

### **Floor Groups Report**

Displays all configured floor groups for use in elevator control.

### **Holidays Report**

Displays holiday specification information.

### **Network Nodes Report**

**Displays all nodes in the system with IP addresses and UID (unique ID).**

### **Portals Report**

Displays portal definition information.

## Portal Groups Report

Displays all portal groups, the portals included in each, and the assigned threat level group.

## Reader Groups Report

Displays defined groups of readers.

## System Resources Report

Displays all configured system resources including readers, inputs, outputs, elevators, and temperature points.

## Threat Level Groups Report

Displays all configured threat level groups and the threat levels assigned to them.

## Threat Levels Report

Displays all configured threat levels including the description and color assignment.

### History Reports

Select **Administration : Reports : History**.

All history reports retrieve data from archives when the requested report data is no longer on the controller board. The controller can hold approximately 100,000 records. Older data is kept in archive files if you have set up an FTP site or set up network attached storage (NAS) for this data.

## Access History Report

Displays access history based on the query entered. You can enter your query in two ways.

In the [Query Parameters](#) section you can point and click to build your query. As you point and click your query will be displayed in the long text box in the [Query Language](#) section below.

In the [Query Language \(advanced\)](#) section you can type your own query in the long text box or select from the drop-down list the reserved words that you need to build your query. See [Using the Security Query Language](#).

### To build a query by point and click:

1. In the [Enter query parameters](#) section enter a last name in the **Person** text box if you wish to limit the report to a specific person.
2. To limit the report to specific dates:
  - Click the calendar icon next to the **From (date)** text box. On the displayed calendar click to select a start date. The date will appear in the text box. Alternatively you can select a month from the **or (month)** drop-down list to the right.

**NOTE:** If you do not enter a **From (date)** to specify the beginning date for the report the system will search back through the entire history available in archives.

  - Click the calendar icon next to the **Thru (date)** text box. On the displayed calendar click to select an end date. The date will appear in the text box. Alternatively you can select a month from the **or (month)** drop-down list to the right.
3. To limit the report to a specific portal or portal group select it from the **At (portal name)** drop-down list.

4. To limit the report to specific types of events select from the **Event type(s)** list.
5. Click **Search**.

## General Event History

With this page you can request a variety of system activity reports. The reports list time, type of activity, and details of the activity. The default report is [All event types](#).

### To generate a specific event type report:

1. Click the calendar icon to select a **From (date)**. This is the start date for the report.

**NOTE:** If you do not enter a **From (date)** to specify the beginning date for the report the system will search back through the entire history available in archives.

2. Click the calendar icon to select a **Thru (date)**. This is the end date for the report.
3. Select from the **at Portals** drop-down a specific portal for this report if it is relevant to the event types that you are investigating.
4. Enter in the **Limit to** text box the maximum number of records you wish to have in this report.
5. Uncheck the **All event types** checkbox in the **Parameter** column.
6. Check each specific event type you want included in a report.
7. Click **Run report**. It may take a minute for the report to be generated and displayed.

## Portal Access Count Report

With this page you can request a report of portal accesses by specific people. You can also specify dates, portals, and a user-defined field from the person detail record.

### To generate a portal access count report:

1. Click the calendar icon to select a **From (date)**. This is the start date for the report.

**NOTE:** If you do not enter a **From (date)** to specify the beginning date for the report the system will search back through the entire history available in archives.

2. Click the calendar icon to select a **Thru (date)**. This is the end date for the report.
3. Select from the **at Portals** drop-down a specific portal for this report.
4. Select from the **Where** drop-down a specific user-defined field and to the right select a value for this field.

**Example:** If your person records have a user-defined field called "Department" then you could restrict the report to only those records where the department is "Accounting" or "Manufacturing."

5. Enter a last name in the **Person (last name)** text box.
6. Click **Run report**.

## People Reports

Select **Administration : Reports : People**.

## Access Levels Report

Displays all access levels entered into the system including time specification, reader/reader group, and floor group.

## Access Validity Report

Displays all permitted access locations and time specifications for the person named. For example, in the text box enter "Smith." The permitted access locations and times for Smith are displayed.

## Current Users Report

Displays a list of all security system users currently logged in to the security system website.

## Photo ID Gallery

Displays all the photo ID pictures in the system and the person's name. Click on the person's name to go to the detailed Personal Information page.

Select a letter from the alphabet at the top of the page and the report will display only those persons whose last name begins with the selected letter.

You can also choose to **Include deleted records** by selecting the **Yes** button. You can exclude deleted records from the report by selecting the **No** button. By selecting the **Only** button you can display a report that includes deleted records only.

## Photo ID Requests Report

Displays all outstanding photo ID print requests and lists.

- ID
- Name
- Selected photo ID layout
- The person's activation date in the system
- The date of the photo ID print request

You can print photo IDs directly from this report page by clicking the printer icon in the **Action** column. The print photo ID window will appear. Click **Print Photo ID**.

## Portal Access Report

Displays the names and access levels of everyone allowed access at the portal you select from the **Portals** drop-down.

## Roster Report

Displays every person entered into the system and it lists:

- Name
- ID Photo (thumbnail)
- Expiration date
- Date their record was last modified
- User name
- Access level

Select a letter from the alphabet at the top of the page and the report will display only those persons whose last name begins with the selected letter.

You can also choose to **Include deleted records** by selecting the **Yes** button. You can exclude deleted records from the report by selecting the **No** button. By selecting the **Only** button you can display a report that includes deleted records only.

You can also choose to **Include expired records** by selecting the **Yes** button. You can exclude expired records from the report by selecting the **No** button. By selecting the **Only** button you can display a report that includes expired records only

## Time Specifications Report

Displays all defined time specifications currently in the system. Time specifications define allowed access times. They are used as part of an access level definition.

**Start** and **End** times for each time spec are in 24 hour format. For example, 900 is 9:00 AM and 1700 is 5:00 PM.

Holidays are listed in groups as they were entered.

## Scheduling Actions for Inputs, Outputs, and Portals

Select **Administration : Schedule Action** or **Monitor : Floorplans**.

On this page you can:

- Perform a momentary unlock of any portal.
- Specify an extended (scheduled) unlock of any portal.
- Specify a scheduled action (**Disarm**) for an input.
- Specify a scheduled action (**Activate/Deactivate**) for an output.

### To setup extended (Scheduled) actions from a floorplan:

1. Select **Monitor : Floorplan**.
2. Click an input, output, or portal on the floorplan and select **Schedule Action**. A Schedule Action pop-up window appears.
3. In the **Action** column select **Disarmed** (inputs), **Activate/Deactivate** (outputs), or **Lock/Unlock** (portals).
4. In the **Start Date/Time** column the current time is the default. You can change this time if you wish or you can click the **In** button and enter a time delay in hours and minutes. The action will begin when this time has elapsed.
5. In the **End Date/Time** column you can enter a specific date and time for the action to end or you can click the **After** button and enter a duration in hours and minutes. The action will end after this duration.

**For Example:** For an input select **Disarmed** and leave the **Start Time** at **Now**. Set the **End Time** to **After 1:30** (one hour and thirty minutes). Click **Save**. This input will be disarmed for one hour and thirty minutes.

5. Click **Save**.

### To setup an extended (Scheduled) actions from the Schedule Action page:

1. Select **Administration : Schedule Action**.
2. Click the **Schedule** link for the input, output, or portal for which you wish to schedule an action. A Schedule Action pop-up window appears.
3. In the **Action** column select **Disarmed** (inputs), **Activate/Deactivate** (outputs), or **Lock/Unlock** (portals).

**NOTE:** Do not unlock a portal by scheduling an action for its lock output. This may create an alarm condition as the portal may be opened without a valid card read.

- In the **Start Date/Time** column the current time is the default. You can change this time if you wish or you can click the **In** button and enter a time delay in hours and minutes. The action will begin when this time has elapsed.
- In the **End Date/Time** column you can enter a specific date and time for the action to end or you can click the **After** button and enter a duration in hours and minutes. The action will end after this duration.

**For Example:** For an output select **Activate** and leave the **Start Time** at **Now**. Set the **End Time** to **After 1:30** (one hour and thirty minutes). Click **Save**. This output will be activated for one hour and thirty minutes.

- Click **Save**.

## **Changing the System Threat Level**

Select **Administration : Set Threat Level**.

On this page you can set the system threat level. Only those holding at least an "[Administration](#)" user role can set system threat levels. Password entry can be required by using [threat level settings](#).

Threat level changes are written into the [Activity Log](#) and the threat level color or icon in the upper right of the application is updated. If other security system users are logged in, the threat level color or icon in the upper right of their application will be updated within one minute.

**NOTE:** It is also possible to change the system threat level with an [alarm event action](#), or an API command.

### **To set or change the current system threat level:**

- Select in the left column the threat level that you wish to set the system to.
- Password entry may be required to change threat levels. Enter your password in the **Password** text box.

**NOTE:** Changing the current system threat level may change the behavior of [access levels](#), [portals](#), [portal groups](#), or [alarm events](#).

- Click **Save**.

## **Administration Utility Menu**

Utilities for system administrators.

<b>Choose this</b>	<b>To see Help for this</b>
Backup Database	Creating a copy of the security database.
Photo ID Layout Delete	Deleting photo ID badge layouts from the controller.
Photo ID Layout Upload	Uploading photo ID badge layouts for printing.

## **Setup Menu**

System setup and configuration.

<b>Choose this</b>	<b>To see Help for this</b>
Access Control	Configure resources that control building access.
Alarms	Configure resources that identify and manage system alarms.
Cameras	Enter configuration information for cameras.
Floor plans	Configure floorplan information.
Network Resources	Enter information about network resources that provide services for this system.
Site Settings	Identify system hardware and user roles and permissions.
System Maintenance	Security database and security system software utilities.
Threat Levels	Create, set, and edit threat levels and threat level groups.
Time	Specify time-related settings.

## **Setup Access Control Menu**

Configure system resources that control building access.

<b>Choose this</b>	<b>To see Help for this</b>
<a href="#">Access Levels</a>	Create or edit access levels, specify allowed readers and a time spec for access.
<a href="#">Card Formats</a>	Specify a card type and bit length, enter start bits and bit lengths for card ID, facility code, and issue code.
<a href="#">Elevators</a>	Create elevators to include node, reader, and button activation time. Name floors requiring access control and create floor groups to include free access time specs.
<a href="#">Person Sections</a>	Configure some of what appears on the personal information page, specify the labels and appearance of the user-defined data fields.
<a href="#">Portal Groups</a>	Create or edit portal groups, and assign an unlock time specification to the group.
<a href="#">Portals</a>	Create or edit portals to include card readers, alarm outputs, a locking mechanism, a door switch monitor (DSM), and a Request-to-Exit (REX) function.
<a href="#">Reader Groups</a>	Create or edit groups of readers and specify anti-passback behavior.
<a href="#">Readers/Keypads</a>	Name readers, specify node, slot, and position.
<a href="#">Utilities</a>	Decode a card and upload or delete photo ID layouts.



## **Setting up Access Levels**

Select **Setup : Access Control : Access Levels**.

On this page you can create access levels and specify for each access level:

- Valid [readers](#).
- Valid [times](#).
- Valid [floors](#).
- Valid system [threat levels](#).
- An [alarm panel](#) to disarm
- Anti-passback violation behavior

Before you can complete the definition of access levels you must create appropriate [time specifications](#). The system can save a maximum of 512 access levels. Each individual is limited to a maximum of 16 access levels.

### **To create an access level:**

1. In the **Name** field enter a name for this new access level.
2. Enable this particular access level by placing a check in the **Enabled** checkbox to the right of the **Name** drop-down list.
3. Enter a **Description** that explains the purpose or use of this access level.
4. Select either **Reader group**, or **Single reader** to assign and from the appropriate drop-down list select the specific Reader or Reader group.
5. From the **Time Spec** drop-down list select the appropriate time specification for this access level.
6. From the **Floor Group** drop-down list you can select a floor group for access control of specific named floors. Be sure that the reader or reader group selected in step 3 above contains an elevator reader.
7. From the **Threat Level Group** drop-down list you can select a threat level group to associate with this access level. This access level will only function when the current system threat level is a member of the threat level group selected. If the current system threat level is not in the threat level group selected then the access level will not be valid and access will be denied.

**NOTE:** Select **<not applicable>** if the system threat level should NOT affect the behavior of this access level.

8. From the **Disarm alarm panel** drop-down list you can select any alarm panels configured in the system that should be disarmed for those holding this access level.

**NOTE:** The alarm panel will disarm only if the reader belongs to a [reader group specified for disarming](#) the alarm panel, and the [alarm panel is enabled for auto-arming](#).

9. From the **Passback Violation** drop-down select the system behavior for this access level in the case of a passback violation.

**NOTE:** It can be desirable to allow certain access levels, such as those for security personnel, to **Ignore** anti-passback violations.

10. Click **Save**.

### **To change an access level:**

1. From the **Existing Access Levels** drop-down list select an existing access level.
2. The other fields on this page will fill in with the details of this access level.
3. Edit the fields that require changes.
4. Click **Save**.

## Specifying Card/Keypad Formats

Select **Setup : Access Control : Card/Keypad Formats**.

The Access Control blade supports card readers and keypads that use the Wiegand Reader Interface.

The default values on this page are set for the Wiegand 26 bit format. If you are using cards or keypads of a different format you will need to know the values to use. Refer to the card manufacturer documentation.

### To create a new card/keypad format:

1. Click the **add** link under the **Name** drop-down list.

**NOTE:** If you are adding a card format that is substantially similar to a currently existing format, select the similar format from the drop-down and click **clone**. Enter a **Name** for the new format and make the needed changes to the format. This method will save time.

2. Enter a **Name** for the card format you are creating. This is a required entry.
3. Enter a **Description** for this card format.
4. In the **Bit Length** text box enter the number of bits in this card format. This is a required entry. The number entered here determines the number of bit definition drop-downs provided below.
5. Check the card manufacturer documentation for the facility code of the card batch that you are using. Enter this **Facility Code** number in the text box.

**NOTE:** Make sure that the facility code for keypads is different from the facility codes used in the card population. It is important that the system recognize keypad input as separate from card reads. For instructions on setting keypad facility codes refer to the keypad manufacturer documentation.

6. The following four fields will fill in automatically as you select the bit definitions in step 9:

- **Facility Code Start Bit:** The first bit of the facility code number.
- **Facility Code Bit Length:** The number of bits used to indicate the facility code.
- **Encoded # Start Bit:** The first bit of the card ID number.
- **Encoded # Bit Length:** The number of bits used to indicate the card ID number.

7. Check the **Hot Stamp # = Encoded #** box if the number printed on the card is the same as the card ID number.
8. **Bit definitions in card format:** For each bit in the card select from the drop-downs the function of the bit. **P** is for a parity bit. **F** is for a facility code bit. **N** is for a card number bit. The number of bit drop-downs will match the **Bit Length** entered above.

**NOTE:** If you are using Wiegand 26 bit cards and you wish your system to ignore the facility code when validating card reads then leave the fields for the Facility Code bits blank. Do not select **F** from the **Bit definitions** drop-downs. The mask values will be 0 127 255 128 0 0.

9. **Mask (char #'s):** the mask values will fill in automatically as you select the bit definitions. This mask indicates the significant bits to be read when validating a card read.
10. Click the **Save** button.

For assistance in setting the proper **Mask (char #'s)** for any other cases call for support.

## Elevators Menu

Configure system resources that control elevator access.

<b>Choose this</b>	<b>To see Help for this</b>
Definitions	Create an elevator and specify node, reader, and button activation time.
Elevator Groups	Specify groups of elevators for use in User Roles.
Floors	Name floors to be managed by elevator access control.
Floor Groups	Create floor groups from named floors and specify free access times.

## Configuring the Personal Information Page

Select **Setup : Access Control : Person Sections**.

Using this page you can:

- Configure some of what appears on the Personal Information page.
- Specify the labels and appearance of the User -defined data fields.

### To configure the appearance of the personal information page:

1. To display the personal information sections **Office Info**, **Emergency Contact**, and **Parking Info** place a check in the checkbox next to each.
2. To hide the personal information sections **Office Info**, **Emergency Contact**, and **Parking Info** remove the check from the checkbox next to the section you wish to hide.
3. To display the **User-defined** section, place a check in the **Show?** checkbox.
4. You can enter a label in the **Section Label** text box and this label will appear as the heading of the **User-defined** section of the Personal Information page.
5. Each data field in the **User-defined** section can be displayed or not by placing or removing the check from the checkbox next to it.
6. You can enter labels into the **Field Label** text boxes and those labels will appear next to the User-defined data fields in the Personal Information page.

## Setting up Portal Groups

Select **Setup : Access Control : Portal Groups**.

On this page you can:

- Create, change, or delete portal groups.
- Assign an unlock time spec and to the group. The portals in this group will be unlocked during the hours defined by the time spec.
- Assign a First-in Unlock rule to the portal group. The portals in this group will be unlocked during the hours defined by the time spec if the First-in Unlock rule is satisfied.

### To add a portal group to the system:

1. Click the **add** link under the **Name** text box.
2. Enter a name for the portal group in the **Name** text box, e.g. External doors.
3. Enter a **Description** for this portal group.

4. Select from the **Unlock Time spec** drop-down list a time specification to assign to this portal group. The portals in this group will be locked at all times except those defined by the chosen time spec.

**For example**, a portal group of the main employee entryways can be assigned an unlock time spec of 6:00 AM (06:00) to 8:00 PM (20:00). The portals in this group will remain unlocked during those times.

5. Select from the **First-in Unlock** drop-down list the rule to apply to this portal group behavior.

**NOTE:** The first-in unlock rule specifies an access level that the system must "see" at a reader in this portal group. Only when this condition is satisfied and the unlock time spec for this portal group is valid, will the portal group unlock.

6. Select from the **Threat Level Group** drop-down list a threat level group to assign to this portal group. The portals in this portal group will be unlocked during the hours of the unlock time spec selected above only if the current system threat level is a member of the assigned threat level group.

**NOTE:** Select **<not applicable>** if the system threat level should NOT affect the behavior of this portal group.

**For example:** Assign a threat level group called "Up2Elevated" containing Default, Low, Guarded, and Elevated threat levels. In this case the unlock time spec will unlock these portals if the current system threat level is Default, Low, Guarded, or Elevated. If the current threat level is High or Severe, the portals will not unlock during the unlock time spec.

7. In the **Portals Available** list click to highlight a specific portal needed for this group.
8. Click the right arrow button between the **Available** and **Selected** list boxes to move the highlighted portal from the **Available** list to the **Selected** list. Repeat this process until all portals needed for this group appear in the **Selected** list.
9. Click **Save**.

#### **To edit a portal group:**

1. Select a portal group from the **Name** drop-down list. The remaining fields on the page fill with the settings for this portal group.
2. Edit any part of the portal group definition.
3. Click **Save**.

#### **To delete a portal group from the system:**

1. Select from the **Name** drop-down list the portal group you wish to delete.
2. Click **Delete**.

## **Setting up Portals**

Select **Setup : Access Control : Portals**.

A portal is any access point. With this page you can change, delete, and create portal definitions.

When you create a portal you define the access and alarm behaviour of the access point. This can include:

- card readers and keypads
- an output for locking
- an input for monitoring the door switch (DSM)
- an input for the Request-to-Exit (REX) function

- local alarm outputs and system alarm events.

**NOTE:** To set an unlock time for a portal, include the portal in a [Portal Group](#) and select an **Unlock Timespec** for that portal group.

### **To create a portal:**

1. Click the **add** link under the **Name** drop-down list.

**NOTE:** The **Name** drop-down list contains all portals currently defined in the system. You can select any portal and this page fills with the data that define that particular portal.

2. Enter a name for the portal in the **Name** text box, for example: "Backdoor."
3. Select from the **Network Node** drop-down list the node to which the portal's inputs and outputs are wired.
4. Define the locking and unlocking behaviour of the portal.

- Select from the **Lock** drop-down the output that controls the door lock and enter the **Unlock** time in seconds.
- You can also enter an **Extended Time Unlock** in seconds. The extended time is for individuals requiring more time to enter a door (due to disability or other reasons). In the **Access Control** tab on the [Personal Information page](#) there is a checkbox for **Use Extended Unlock**.

**NOTE:** An output for a door lock cannot be assigned to both a portal and to another function. The only outputs that appear in this drop-down are those not currently assigned elsewhere.

- Select from the **DSM** drop-down the input that monitors the door switch and will communicate to the node when the door is open. Enter the **Shunt** time in seconds. Shunt time begins when the DSM indicates the door is open. Alarm outputs are suppressed for the duration of the shunt timer.
- You can also enter an **Extended Time Shunt** in seconds. The extended time is for individuals requiring more time to enter a door (due to disability or other reasons).

**NOTE:** A DSM input must be in an [Input Group](#). A DSM input cannot be assigned to both a portal and to another function. The only inputs that appear in this drop-down are those not currently assigned elsewhere.

- Place a check in the **Relock on Open** box if you want the door to relock once it is open, rather than wait for the unlock timer to expire.
- Select from the **REX** drop-down the input that notifies the node of a request-to-exit and select from **REX mode** whether the REX is a motion sensor or a manual switch such as a push button or a crash bar. When the REX is active, alarm outputs are suppressed until the shunt timer expires.

**NOTE:** A REX input must be in an [Input Group](#). A REX input cannot be assigned to both a portal and to another function. The only inputs that appear in this drop-down are those not currently assigned elsewhere.

- Place a check in the **Unlock on REX** box if the door is normally locked from the inside and must be unlocked to allow exit.

5. Specify the card reader(s) and keypads at this portal.

- Select from the **Reader 1** drop-down the reader required for entry at this portal.
- Select from the **Reader 2** drop-down the reader required for exit at this portal.

**NOTE:** A reader cannot be assigned to more than one function. The only readers that appear in this drop-down are those not currently assigned elsewhere.

- You can specify that readers must accept card reads even while the door is open or while an interior REX has fired by checking the **Accept Read While Open** box. If this box is not checked then the reader will not accept any card reads until the DSM indicates that the door is closed or the REX shunt timer has expired.
- Select from **Keypad 1** drop-down the keypad required for entry at this portal. You can set the allowable time for PIN entry on the [Site Settings : Network Controller](#) page.
- Select from **Keypad 2** drop-down the keypad required for exit at this portal. You can set the allowable time for PIN entry on the [Site Settings : Network Controller](#) page.

**NOTE:** A keypad cannot be assigned to more than one function. The only keypads that appear in this drop-down are those not currently assigned elsewhere.

- For both keypads and the outgoing reader you can specify a **Time Spec** and a **Threat Level Group** by selecting them from the appropriate drop-downs. Once a [Time Spec](#) and/or [Threat Level Group](#) is selected the keypad use and/or outgoing reader use will be required only during the hours of the selected time spec **and** when the current system threat level is contained within the selected threat level group.

**CAUTION:** When an outgoing reader or outgoing keypad is enabled the REX for that portal will not function. Such a portal may require an emergency manual REX to enable egress under dangerous conditions such as a fire.

**NOTE:** PIN numbers for keypads are 4 digits and must be entered into the [person record](#) for each card holder. Therefore, when both a reader and keypad are required the valid card read and the PIN must match.

#### 6. Define the alarm behaviour of the portal.

There are 4 portal alarm conditions: Forced, Held, Invalid, and Valid. Each can be assigned both a **Local to Node** system resource (an output), and a **System-wide alarm event**. **Local to Node** responses will not be logged in the security database. **System-wide** events will be logged in the security database.

- the **Local to Node** output selected from the **Output** drop-down will activate for the duration indicated in the **Time** box. Valid values are 0 to 255 seconds. **NOTE:** If you enter a 0 (zero) here the alarm output will remain active until the alarm condition is cleared.
- the **System-wide** alarm event selected from the **Event** drop-down will execute and log an entry in the security database.

**Forced:** A portal has been forced open and there has been no card read nor request-to-exit.

**Held:** A portal is held open past the expiration of the shunt timer.

**Invalid:** A card is passed through the reader and no valid entry for that card is found in the database.

**Valid:** A card is passed through the reader and a valid entry for that card is found in the database.

#### 7. Click **Save**.

**NOTE:** **Part of Group(s)** lists any Portal groups that this portal is part of. You cannot delete a portal while it is part of a portal group.

## **Setting up Reader Groups**

Select **Setup : Access Control : Reader Groups**.

On this page you can:

- Create, change, or delete reader groups.
- Specify timed anti-passback duration.

### **To add a reader group to the system:**

1. Click the **add** link under the **Name** text box.
2. Enter a name for the reader group in the **Name** text box, e.g. Lab doors.
3. Enter a **Description** for this reader group.
4. Place a check in the **Timed Anti-passback** box if you wish these readers to use the anti-passback function.
5. In the **Duration** box enter the time in seconds for anti-passback control.

**For example:** If you enter 600 seconds then a credential used in this reader group will not be valid for 10 minutes after first use. See also the **Passback Violation** setting for [access levels](#).

**NOTE:** Readers cannot be put into more than one group using anti-passback.

6. In the **Readers Available** list click to highlight a specific reader needed for this group.
7. Click the right arrow button between the **Available** and **Selected** list boxes to move the highlighted reader from the **Available** list to the **Selected** list. Repeat this process until all readers needed for this group appear in the **Selected** list.
8. Click **Save**.

### **To edit a reader group:**

1. Select from the **Name** drop-down list the reader group you wish to change. The remaining fields on the page fill with the settings for this reader group.
2. Make the needed changes to any of the fields.
3. Click **Save**.

### **To delete a reader group from the system:**

1. Select from the **Name** drop-down list the reader group you wish to delete.
2. Click **Delete**.

## **Setting up Readers/Keypads**

Select **Setup : Access Control : Readers/Keypads**.

On this page you can:

- Create, change, or delete readers and keypads.
- Enable or disable the readers and keypads.

Before you can complete the definition of [reader groups](#), [access levels](#), or [portals](#) you must configure the individual readers and keypads.

**Special Note on Keypads:** The system can support any reader, keypad, or combination reader/keypad device that outputs Wiegand formatted data. A keypad entry is converted into a 16 bit number which is placed into Wiegand formatted data with a facility code and parity bits.

Keypad facility codes must differ from facility codes used in the card population. The Node uses the facility code to recognize the difference between card reads and keypad PIN entries. (Facility codes on most keypad devices can be set.) Be sure to enter the keypad format and facility code using the **Setup : Access Control : Card/Keypad Formats** page.

PIN numbers for keypads are 4 digits and must be entered into the [person record](#) for each card holder. When both a reader and keypad are required the valid card read and the PIN must match both the card number and PIN entered in the person record.

### **To add a reader or keypad to the system configuration:**

1. Click the **add** link under the **Name** drop-down list.
2. Enter a name for the reader or keypad in the **Name** text box, e.g. Parking lot entry.
3. Be sure that the **Enabled** checkbox to the right of the **Name** text box is checked.
4. Enter a **Description** for this reader/keypad.
5. Select from the **Network Node** drop-down list the node that this reader/keypad is wired to.
6. Select from the **Expansion Slot** drop-down list the slot number of the board that the reader/keypad is connected to.
7. Select from the **Position** drop-down list the connector position number that the reader/keypad is connected to.
8. Select from the **Reader/Keypad Type** drop-down whether the device is a reader only, a keypad only, or a combination reader/keypad.
9. Click **Save**.

### **To edit a reader/keypad:**

1. Select from the **Name** drop-down list the reader/keypad you wish to change. The remaining fields on the page fill with the settings for this reader.
2. Make the needed changes to any of the fields.
3. Click **Save**.

### **To delete a reader/keypad:**

1. Select the reader/keypad you wish to delete from the **Name** drop-down list.
2. Click **Delete**.
3. If this reader is defined as part of any reader group then these groups will be listed next to **Part of group(s)**. You cannot delete a reader or keypad while it is part of a reader group.

## **Access Control Utilities Menu**

Select **Setup : Access Control : Utilities**.

<b>Choose this</b>	<b>To see Help for this</b>
<a href="#">Card Decoder</a>	Raw card information can help to identify an unknown card. Use this option to decode a card.
<a href="#">Badge Layout Delete</a>	Review and Select badge layouts for deleting.
<a href="#">Badge Layout Upload</a>	Upload badge layouts for badge printing.



## Setup Alarms Menu

Configure system resources that identify and manage alarms.

Choose this	To see Help for this
Alarm Panels	Configure alarm panels and specify auto-arming behavior.
Input Groups	Create or edit groups of inputs. Select a time specification for arming inputs in the group.
Inputs	Name inputs, specify node, slot, and position. Enter an output name as a following resource ID.
Event Groups	Specify groups of events for use in User Roles.
Events	Specify (alarm) events and system behavior in response to the event.
Output Groups	Create or edit groups of outputs. Select a time specification for activating outputs in the group.
Outputs	Name outputs, specify node, slot, and position. Enter a default state of Energized or Not Energized.
Temperature Inputs	Name temperature inputs, specify node, slot, and position. Select temperature related alarm events.
Virtual Inputs	Connect virtual inputs (VMS cameras) to events when motion is detected or a camera goes down.

## Creating Alarm Input Groups

Select **Setup : Alarms : Input Groups**.

On this page you can:

- Create, change, or delete input groups.
- Assign an auto-arm time specification to the input group. The inputs in this group will be armed during the times defined by the chosen time specification.

**For example**, an input group of interior motion detectors might be assigned an auto-arm time spec from midnight (0000) to 5 AM (0500) when no one is supposed to be in the building.

### To add an input group to the system:

1. Click the **add** link under the **Name** text box.
2. Enter a name for the input group in the **Name** text box, e.g. External door monitors.
3. Enter a **Description** for this input group.
4. Select from the **Auto-arm Time spec** drop-down list a time specification to assign to this input group. The inputs in this group will be armed during the times defined by the chosen time spec.
5. In the **Inputs Available** list click to highlight a specific input needed for this group.

**NOTE:** [Inputs](#), [Virtual Inputs](#), and [Temperature Inputs](#) can all be put into input groups.

6. Click the right arrow button between the **Available** and **Selected** list boxes to move the highlighted input from the **Available** list to the **Selected** list. Repeat this process until all inputs needed for this group appear in the **Selected** list.
7. Click **Save**.

#### **To edit an input group:**

1. Select from the **Name** drop-down list the input group you wish to change. The remaining fields on the page fill with the settings for this input group.
2. Make the needed changes to any of the fields.
3. Click **Save**.

#### **To delete an input group from the system:**

1. Select from the **Name** drop-down list the input group you wish to delete.
2. Click **Delete**.

### **Setting up Alarm Inputs**

Select **Setup : Alarms : Inputs**.

On this page you can:

- Create, change, or delete inputs.
- Enable or disable the input.
- Specify an output and/or an event to execute when the input goes into an alarm or trouble state.

Before you can complete the definition of [input groups](#), or [portals](#) you must configure the individual input devices.

Inputs have 2, 3, or 4 possible states depending upon which Input Supervision Type is selected. Refer to the "Installation Guide" for specifics regarding input states and resistance values.

#### **To add an input to the system configuration:**

1. Click the **add** link under the **Name** drop-down list.
2. Enter a name for the input in the **Name** text box, e.g. Backdoor switch monitor.
3. Be sure that the **Enabled** checkbox to the right of the **Name** text box is checked.
1. Inputs that are not defined as part of an [Input Group](#) will not arm. You must either check the **Always Armed** box or create an input group and assign a time spec to the group, during which the inputs in the group are armed.
2. Enter a **Description** for this input.
3. Select from the **Network Node** drop-down list the node that this input is wired to.
4. Select from the **Expansion Slot** drop-down list the [slot number](#) of the board that the input is connected to.
5. Select from the **Position** drop-down list the connector [position number](#) that the input is connected to.
6. If this input is to activate a particular output, select the output in the **Following Output** drop-down list.

A **Following Output** is fired in response to an input changing to the [Alarm](#) state. **For example**, a door switch monitor input may be defined to have a Trigger Output turn on a hallway light when the door opens. This action takes place on the Node only.

10. Select from the **Input supervision type** drop-down the circuit type (NO = normally open, NC = normally closed) and resistor configuration for this input.

**NOTE:** It is critical that this selection accurately reflect the input circuit. The system supports 1K Ohm resistors only and circuit diagram is displayed on the page next to **Termination Circuit**. The various circuits and resistor configurations create resistance values used by the system in determining normal, alarm, and trouble states. For more specific information on these wiring configurations and resistance values see Connecting Inputs in the "Installation Guide."

11. The **In group(s)** field lists input groups that this input is part of.

**NOTE:** You cannot delete an input while it is part of an input group.

12. If this input is to trigger an event when it enters an alarm state, select the appropriate event from the **Off-normal Event** drop-down list and check the **Enabled** box to the right.

An **Off-normal Event** is executed in response to an input changing to the Alarm state.

13. If this input is to trigger an event when it enters a trouble state (short or open), select the appropriate event from the **Supervision Error Event** drop-down list and check the **Enabled** box to the right.

An **Supervision Error Event** is executed in response to an input changing to Short or Open states.

**NOTE:** You cannot set up supervision error events for unsupervised inputs.

14. Click **Save**.

**NOTE:** The **Advanced Settings** allows you to set up multiple events to execute in response to an input entering any one of its states.

#### **Using Advanced Settings to set up events**

1. Click the **Advanced Settings** button in the **Events** section.
2. In the Advanced Settings window select an input state from the **State** drop-down.
3. From the **Event** drop-down select an event to execute when the input enters the selected state.
4. Click the **Apply** button to move the state/event pairing into the **Current Triggers** box.

**NOTE:** You can assign additional events to the same state.

5. Click **Save**.

#### **To delete an input:**

1. Select the input you wish to delete from the **Name** drop-down list.
2. If this input is defined as part of any input group then these groups will be listed next to **In group(s)**.

**NOTE:** You cannot delete an input while it is part of an input group.

3. Click **Delete**.

### **Creating Event Groups**

Select **Setup : Alarms : Event Groups**.

On this page you can:

- Create, change, rename, or delete event groups for use in specifying User Roles.

### To create an event group:

1. Click the **add** link just under the **Name** drop-down list.
2. Enter a name for the group in the **Name** text box, e.g. Held events.
3. In the **Events Available** list click to highlight a specific event needed for this group.
4. Click the right arrow button between the **Available** and **Selected** list boxes to move the highlighted event from the **Available** list to the **Selected** list. Repeat this process until all events needed for this group appear in the **Selected** list.
5. Click **Save**.

### To delete an event group:

1. Select from the **Name** drop-down list the group you wish to delete.
2. Click **Delete**.

## Setting up Alarm Events

Select **Setup : Alarms : Events**.

Events can be a complex series of actions taken in response to an input going into an alarm state. Once an event is defined it can be assigned to any number of supervised inputs or [portals](#).

### To create an event:

1. Click the **add** link under the **Name** drop-down list. If there is no **add** link then no events have yet been defined.
2. Enter a name for the event in the **Name** text box.
3. Enter a **Description** of the event.
4. Enter an **Operator short msg** and an **Operator long msg** in the text boxes. These messages will be presented to a system operator if this event is triggered. The **Operator long msg** text box can contain HTML. This could be used to display, for example, an image as the long message.
5. Select from the **Enabled Timespec** drop-down list a [time spec](#) during which this event will execute in response to an input alarm state.
6. Select from the **Priority** drop-down a priority number. One (1) is the highest priority and twenty (20) is the lowest priority. In the monitoring page the highest priority events are listed first. If actions specified by two different concurrent events conflict then the higher priority event takes precedence.
7. Select from the **Camera** drop-down the camera you want displayed on the [Monitoring Desktop](#) when this alarm event is triggered.
8. Set the **Acknowledgements**:
  - **Required**: check this box and the event will remain active until an operator acknowledges it.
  - **Maximum Duration**: enter a time duration for this event in seconds. The event will auto-acknowledge when the duration has elapsed. If no duration is set the event actions will continue until the event is cleared or the cause is resolved.

**NOTE:** If you required acknowledgement by checking the **Required** box then no duration can be set. Auto-acknowledge is not allowed.

- **Allow Clear Actions**: check this box and an operator can cancel the event actions.
- **While Active?**: check this box and an operator can cancel the event actions even if the input that triggered the event is still in an alarm state.

9. Define the **Actions** that the system will execute when this event is triggered.

You can also select and **Delete** actions here. A default action to create a security log entry already exists. You can delete this if you wish.

1. Select **<add new>** in the **Current actions** list box.
2. Complete the **Action details** in the right half of the **Actions** section.
  - Enter a **Name** for the action and check the **Enabled** box to enable this particular action.
  - Select from the **Action** drop-down the action to take and from the drop-down to the right select the appropriate resource for that action.

**NOTE:** If you select a **Threat Level** action then a **Change to Threat Level** drop-down list will appear to the right. The threat level you select here will become the current system threat level when this alarm event executes.

- **Priority:** select from the drop-down a priority number.
- **Duration:** enter a time duration for this action in seconds.
- **Threat Level Group:** Select from the drop-down list a threat level group to assign to this action. This action will execute only if the current system threat level is a member of the assigned threat level group.

**NOTE:** Select **<not applicable>** if the system threat level should NOT affect the behavior of this alarm event action.

3. Click **Apply changes to action**.
4. You can now add additional actions or edit any actions already applied to the event.

10. Define the event **Notification** details.

- Place a check in the **Announced** box if you want the event announced by playing a sound file.
- Select from the **Sound** drop-down the .wav file you want played when this event is triggered. If you select **<add new>** an **Upload Sound file** window appears and you can upload sound files to the Controller.

**NOTE:** Sound files (.wav) are each limited to 50K maximum, and a maximum of 10 can be stored on the Controller. If you have a compact flash installed on your Controller you can store up to 100 sound files on the compact flash.

- Select from the **Color** drop-down the text color for this event when displayed in the **Alarms** tab of the [Monitoring Desktop](#).

11. Click **Save**.

## **Creating Output Groups**

Select **Setup : Alarms : Output Groups**.

On this page you can:

- Create, change, or delete output groups.
- Assign an auto-activate time spec to the output group. The outputs in this group will activate during the times defined by the chosen time spec.

**For example**, an output group that controls the building exterior lighting can be assigned a [time spec](#) from 8:00PM (20:00) to 6:00AM (06:00). These outputs can still activate at other times if they are included as an action in an [alarm event](#), or if they are specified as a [following output](#) to some input.

**NOTE:** Do not use an output group **Auto-activate time spec** to set an unlock time for a portal. Include the portal in a [Portal Group](#) and select an **Unlock Timespec** for that portal group.

**To add an output group to the system:**

1. Click the **add** link under the **Name** text box.
2. Enter a name for the output group in the **Name** text box, e.g. External door monitors.
3. Enter a **Description** for this output group.
4. Select from the **Auto-activate Time spec** drop-down list a time specification to assign to this output group. The outputs in this group will activate during the times defined by the chosen time spec.
5. In the **Outputs Available** list click to highlight a specific output needed for this group.
6. Click the right arrow button between the **Available** and **Selected** list boxes to move the highlighted output from the **Available** list to the **Selected** list. Repeat this process until all outputs needed for this group appear in the **Selected** list.
7. Click **Save**.

**To edit an output group:**

1. Select from the **Name** drop-down list the output group you wish to change. The remaining fields on the page fill with the settings for this output group.
2. Make the needed changes to any of the fields.
3. Click **Save**.

**To delete an output group from the system:**

1. Select from the **Name** drop-down list the output group you wish to delete.
2. Click **Delete**.

## **Setting up Outputs**

Select **Setup : Alarms : Outputs**.

On this page you can:

- Create, change, or delete outputs.
- Enable or disable the outputs.

Before you can complete the definition of [output groups](#), or [portals](#) you must configure the individual output devices.

Completed Installation Description Forms from the printed [Installation Guide](#) will make this task much easier.

**To add an output to the system configuration:**

1. Click the **add** link under the **Name** drop-down list.
2. Enter a name for the output in the **Name** text box, e.g. Backdoor alarm.
3. Be sure that the **Enabled** checkbox to the right of the **Name** text box is checked.
4. Enter a **Description** for this output.
5. Select from the **Network Node** drop-down list the node that this output is wired to.

6. Select from the **Expansion Slot** drop-down list the [slot number](#) of the board that the output is connected to.
7. Select from the **Position** drop-down list the connector [position number](#) that the output is connected to.
8. Select from the **Default State Code** drop-down whether this output is normally **Energized** or normally **Not Energized**.
9. The **In group(s)** field lists [output groups](#) that this output is part of.  
**NOTE:** You cannot delete an output while it is part of an output group.
9. Click **Save**.

#### **To delete an output:**

1. Select the output you wish to delete from the **Name** drop-down list.
2. If this output is defined as part of any output group then these groups will be listed next to **In group(s)**.  
**NOTE:** You cannot delete an output while it is part of an output group.
3. Click **Delete**.

### **Setting up Temperature Inputs**

Select **Setup : Alarms : Temperature Inputs**.

On this page you can:

- Create, change, or delete temperature inputs.
- Enable or disable the input.
- Specify maximum and minimum temperatures.
- Select events for temperature alarm states.

#### **To add a temperature input to the system configuration:**

1. Click the **add** link under the **Name** drop-down list.  
**NOTE:** If you are adding an input that is substantially similar to a current one, select the current temperature input from the drop-down and click **clone**. Enter a **Name** for the new input and make the needed changes. This method will save time.
2. Enter a name for the input in the **Name** text box.
3. Be sure that the **Enabled** checkbox to the right of the **Name** text box is checked.
4. Inputs that are not defined as part of an [Input Group](#) will not arm. You must either check the **Always Armed** box or create an input group and assign a [time spec](#) to the group, during which the inputs in the group are armed.
5. Enter a **Description** for this input.
6. Select from the **Network Node** drop-down list the node that this input is wired to.
7. Select from the **Expansion Slot** drop-down list the [slot number](#) of the board that the input is connected to.
8. Select from the **Position** drop-down list the connector [position number](#) that the input is connected to.
9. Enter the **Max Temperature** and **Min Temperature**. Temperatures exceeding these boundaries will generate an alarm state.

**NOTE:** You can set the temperature scale to Celsius or Fahrenheit on the [Network Controller page](#). Internally the temperature data is stored and calculated using whole integers and the Celsius scale. This may result in temperatures entered in Fahrenheit being rounded to the nearest whole degree Celsius. **For example**, setting Max Temperature to 99 F will display as 98.6 F (37 C).

**NOTE 2:** The default and highest maximum temperature is 125 C. The default and lowest minimum temperature is -55 C. These defaults will not display.

10. Select from the **Local Status Output** drop-down, the output to fire if this temperature input exceeds either of the temperature limit boundaries.

You can, for example, wire an output to a blinking light at the location of each temperature input point. This would make it easy to find the temperature point that has entered an alarm state.

11. Select from the drop-downs a **High Temp Event**, and **Low Temp Event**. Check the **Enabled** check box.
12. Select from the **Point Fault Event** drop-down an event to execute if the temperature point is no longer communicating temperature data to the system.
13. Click **Save**.

## **Setting up Virtual Inputs for VMS Cameras**

Select **Setup : Alarms : Virtual Inputs**.

On this page you can:

- Enable and arm virtual inputs.
- Select an event to follow camera Fail, Normal, and Motion events.

Virtual inputs are named cameras. Strictly speaking you do not set up virtual inputs. Virtual inputs auto-populate. These are determined during DVR setup through the DVR web UI. Virtual inputs may include: camera down (Fail), camera up (Normal), and motion detection (VMD) events on any camera in the DVR system.

Time specifications for the inputs must be configured in the DVR web UI during DVR setup. Events are reported to the network controller only during the time specification assigned to the inputs in the DVR web UI.

### **Assigning an event to a virtual input:**

1. From the **Name** drop-down select a virtual input. Click to place a check in the **Enabled** check box for this virtual input.
2. Inputs that are not defined as part of an [Input Group](#) will not arm. You must either check the **Always Armed** box or create an input group containing this input and assign a [time spec](#) to the group, during which the inputs in the group are armed.
3. From the **Camera Normal Event** drop-down select the event to execute when a camera returns to normal status. Click to place a check in the **Enabled** check box for this event.
4. From the **Video Motion Event** drop-down select the event to execute when a camera detects a motion event. Click to place a check in the **Enabled** check box for this event.
5. From the **Video Fail Event** drop-down select the event to execute when a camera fails or stops sending data to the system. Click to place a check in the **Enabled** check box for this event.
6. Click **Save**.



## **Setup Cameras Menu**

Change and enter settings for cameras.

<b>Choose this</b>	<b>To see Help for this</b>
<a href="#">Camera Groups</a>	Specify groups of cameras for use in User Roles.
<a href="#">Configure Dedicated Micros DVR</a>	Setup and maintain the integration of Dedicated Micros DVRs.
<a href="#">Configure Milestone Systems NVR</a>	Setup and maintain the integration of Milestone Systems NVRs.
<a href="#">Configure OnSSI NVR</a>	Setup and maintain the integration of OnSSI NVRs
<a href="#">Definitions</a>	Change the general settings for a camera including DNS name, camera type, IP information, username and password.
<a href="#">Menu Order</a>	Set the order of cameras in the Main Menu and lists.
<a href="#">Presets</a>	Configure in the security system the preset positions already defined at each camera web site.
<a href="#">Types</a>	Setup the URLs for each camera used to control the pan, tilt, zoom, preset and brightness features.
<a href="#">Views</a>	Setup multi-camera collections in quad views and picture-in-a-picture.

## **Creating Camera Groups**

Select **Setup : Cameras : Groups**.

On this page you can:

- Create, change, rename, or delete camera groups for use in specifying User Roles.

### **To create a camera group:**

1. Click the **add** link just under the **Name** drop-down list.
2. Enter a name for the camera in the **Name** text box, e.g. Parking cam.
3. In the **Cameras Available** list click to highlight a specific camera needed for this group.
4. Click the right arrow button between the **Available** and **Selected** list boxes to move the highlighted camera from the **Available** list to the **Selected** list. Repeat this process until all cameras needed for this group appear in the **Selected** list.
5. Click **Save**.

### **To delete a camera group:**

1. Select from the **Name** drop-down list the camera you wish to delete.
2. Click **Delete**.

## **Setting up a Dedicated Micros DVR**

Select **Setup : Cameras : Configure DM DVR**.

On this page you can:

- Add a Dedicated Micros DVR to the system.
- Enable delivery of video events to the network controller.
- Enable the use of a Java applet for viewing live streaming video

Before configuring the video management system on the network controller ensure that the DVR and cameras have been set up and verified through the DVR's own web UI.

We strongly recommend the use of a static IP address for the DVR. If the IP address of the DVR changes the connection between the DVR and the network controller will be lost. The static IP address must be set using the DVR's own web UI.

### **Setting up the Dedicated Micros DVR:**

1. In the **DVR IP Address** text box enter the IP address of the DVR and click **Check Connection**.  
**NOTE:** The **Discovered Information** section will automatically fill in.
2. In the **Name** field enter a name for this DVR.
3. The **DVR HTTP port** and **DVR FTP port** fields default to 80 and 21 respectively. These need not be changed unless the network administrator specifies other port numbers.
4. The **DVR FTP username** and **DVR FTP password** fields default to "dm" and "ftp" respectively. These need not be changed unless the FTP username and FTP password were changed during the DVR setup.
5. The **DVR WEB or VIDEO username** and **DVR WEB or VIDEO password** fields default to "dm" and "web" respectively.

**NOTE:** If you create a Video account in the Dedicated Micros Administrator you will need to use this username and password here.

In addition, the first time you monitor a camera you will be required to login by entering this username and password. This is required only once per browser session.

2. Click **Save**.
3. Click the **List VMS Cameras** link at the bottom of the **Discovered Information** section. A list of cameras appears.
4. Verify that the camera list is correct and complete. These cameras were previously set up during the configuration of the DVR through its own web UI.

**NOTE:** If you change any camera names here you will have to click **Save** for these changes to be communicated back to the DM DVR.

### **Configuring optional Settings:**

1. **Public IP Address:** This IP address automatically fills in when you save a new DVR configuration.  
**NOTE:** If this address is on another subnet or behind a firewall you may have to change this to the external public address of the router or firewall. The network administrator will have to setup the port translation for communications and video to and from this address.
2. **Public HTTP port:** This port number defaults to 80. Do not change.
3. **Combine VMD events arriving within seconds:** Video Motion Detection (VMD) events occurring within the specified number of seconds are combined into one network controller event.

**Example:** If you set this field to 60 seconds, then additional motion detection events will not be reported to the network controller unless at least 60 seconds has passed since the last motion detection on that camera.

4. **Use Java applet for live video:** Place a check in this box to use the DVR Java applet for viewing live streaming video. If there is no check in this box then JPEG images are delivered once per second.

**NOTE 1:** Using live streaming video consumes considerable network bandwidth.

**NOTE 2:** When you view a camera using the Java applet you will be asked to allow the applet signed by "john ellison" to run on your computer.

**NOTE 3:** To use this applet your computer must have the Java™ 2 Runtime Environment version 1.4.2 or version 5.0. You can download this from <http://java.sun.com/j2se/1.4.2/download.html>.

5. **Deliver Events to the Network Controller:** Place a check in this box for DVR events to be delivered to the network controller.
6. **Configure directly:** Click this link to display the DVR's own web UI in a separate browser window. You will then have to login using the administrator username and password for the DVR.
7. Click **Save**.

## **Setting up a Milestone Systems NVR**

Select **Setup : Cameras : Configure Milestone NVR**.

On this page you can:

- Add a Milestone NVR to the system.
- Enable delivery of video events to the network controller.

**NOTE 1:** Before configuring the video management system on the network controller ensure that the NVR and cameras have been set up and verified through the NVR's own web UI.

**NOTE 2:** We strongly recommend the use of a static IP address for the NVR. If the IP address of the NVR changes the connection between the NVR and the network controller will be lost. The static IP address must be set using the NVR's own web UI.

**NOTE:** Using live streaming video consumes considerable network bandwidth.

### **Setting up the Milestone Systems NVR:**

1. In the **NVR IP Address** text box enter the IP address of the NVR and click **Check Connection**.  
**NOTE:** The **Discovered Information** section will automatically fill in.
2. In the **Name** field enter a name for this NVR.
3. The **Engine Username** and **Engine Password** fields default to "Engine1Name" and "Engine1Pass" respectively. We recommend that you leave these defaults here and in the Milestone system.
4. The **Image Server Username** and **Image Server Password** fields default to "test" and "test" respectively. Enter here the Image Server user name and password that you created when setting up the Milestone Systems Image Server.
5. The **Image Server Port** defaults to 80. If you change this in the Milestone System you will have to change it here.
6. The **Engine Listener Port** defaults to 1237. We recommend that you do not change these defaults.
7. The **Event Trigger Port** defaults to 1234. We recommend that you do not change these defaults.
8. Click **Save**.

9. Click the **List VMS Cameras** link at the bottom of the **Discovered Information** section. A list of camera names appears. You cannot change these names here.
10. Verify that the camera list is correct and complete. These cameras were previously set up during the configuration of the NVR through its own web UI.

### **Configuring Settings:**

1. **Public IP Address:** This IP address automatically fills in when you save a new DVR configuration.

**NOTE:** If this address is on another subnet or behind a firewall you may have to change this to the external public address of the router or firewall. The network administrator will have to setup the port translation for communications and video to and from this address.

2. **Public HTTP port:** This port number defaults to 80. Do not change.
3. **Combine VMD events arriving within seconds:** Video Motion Detection (VMD) events occurring within the specified number of seconds are combined into one network controller event.

**Example:** If you set this field to 60 seconds, then additional motion detection events will not be reported to the network controller unless at least 60 seconds has passed since the last motion detection on that camera.

4. Click **Save**.

### **Setting up an OnSSI NVR**

Select **Setup : Cameras : Configure OnSSI NVR**.

On this page you can:

- Add an OnSSI NVR to the system.
- Enable delivery of video events to the network controller.

**NOTE 1:** Before configuring the video management system on the network controller ensure that the NVR and cameras have been set up and verified through the NVR's own web UI.

**NOTE 2:** We strongly recommend the use of a static IP address for the NVR. If the IP address of the NVR changes the connection between the NVR and the network controller will be lost. The static IP address must be set using the NVR's own web UI.

**NOTE:** Using live streaming video consumes considerable network bandwidth.

### **Setting up the OnSSI NVR:**

1. In the **NVR IP Address** text box enter the IP address of the NVR and click **Check Connection**.

**NOTE:** The **Discovered Information** section will automatically fill in.

2. In the **Name** field enter a name for this NVR.
3. The **Engine Username** and **Engine Password** fields default to "Engine1Name" and "Engine1Pass" respectively. We recommend that you leave these defaults here and in the OnSSI system.
4. The **Image Server Username** and **Image Server Password** fields default to "test" and "test" respectively. Enter here the Image Server user name and password that you created when setting up the OnSSI Image Server.
5. The **Image Server Port** defaults to 80. If you change this in the OnSSI System you will have to change it here.
6. The **Engine Listener Port** defaults to 1237. We recommend that you do not change these defaults.

7. The **Event Trigger Port** defaults to 1234. We recommend that you do not change these defaults.
8. Click **Save**.
9. Click the **List VMS Cameras** link at the bottom of the **Discovered Information** section. A list of camera names appears. You cannot change these names here.
10. Verify that the camera list is correct and complete. These cameras were previously set up during the configuration of the NVR through its own web UI.

#### **Configuring Settings:**

1. **Public IP Address:** This IP address automatically fills in when you save a new DVR configuration.

**NOTE:** If this address is on another subnet or behind a firewall you may have to change this to the external public address of the router or firewall. The network administrator will have to setup the port translation for communications and video to and from this address.

2. **Public HTTP port:** This port number defaults to 80. Do not change.
3. **Combine VMD events arriving within seconds:** Video Motion Detection (VMD) events occurring within the specified number of seconds are combined into one network controller event.

**Example:** If you set this field to 60 seconds, then additional motion detection events will not be reported to the network controller unless at least 60 seconds has passed since the last motion detection on that camera.

4. Click **Save**.

#### **Creating Camera Definitions**

Select **Setup : Cameras : Definitions**.

On this page you can:

- Create, change, rename, or delete camera definitions.
- See definitions of all cameras currently defined in the system.

All networked cameras that are used in the system must be defined in the software using this page. All fields are required.

**NOTE:** Cameras connected to the DVR are defined using the DVR web site. Those cameras should not be defined here.

To complete the creation of camera definitions the network administrator will have to provide an **IP Address** and **DNS Name**, and assign an **IP Port** to the camera.

**NOTE:** If the **Camera Type** drop-down list does not contain your camera type you will have to [create this camera type](#) and return to this page.

#### **To add a camera definition to the system:**

1. Click the **add** link just under the **Name** drop-down list.
2. Enter a name for the camera in the **Name** text box, e.g. Parking cam.
3. **Browser Address:** Enter the address used for the video feed. You can enter this as a DNS name or as an IP address. A DNS name is preferred if the camera and the Network Controller are on different sides of a firewall.
4. **Control Address:** Enter the address used for camera control signals such as Zoom or Move Left. You can enter this as a DNS name or as an IP address. A DNS name is preferred if the camera and the Network Controller are on different sides of a firewall.

5. **IP Port:** Enter the port number set up for the camera. Get this number from the network administrator.
6. **Admin Username:** Enter the username specified for the camera when the camera was setup.
7. **Admin Password:** Enter the password specified for the camera when the camera was setup.
8. Select from the **Camera Type** drop-down list the correct camera type for this camera.
9. Click **Save**.

**To delete a camera definition from the system:**

1. Select from the **Name** drop-down list the camera you wish to delete.
2. Click **Delete**.

**To change a camera definition:**

1. Select from the **Name** drop-down list the camera definition you wish to edit.
2. Make any necessary changes in the other fields.
3. Click **Save**.

**To rename a camera:**

1. Select from the **Name** drop-down list the camera you wish to rename.
2. Click the **rename** link just under the **Name** drop-down list.
3. Edit the camera name.
4. Click **Save**.

## **Setting the Camera Menu Order**

Select **Setup : Cameras : Menu Order**.

You can determine the order in which cameras appear in the **Monitor** section of the **Main Menu** by using this page.

**To change the camera order:**

1. Select a camera in the list by clicking on it. It will highlight to show that it is selected.
2. Click the **Move up** or **Move down** arrow to move the selected camera up or down the list.
3. Click **Save**.

## **Creating Camera Preset Positions**

Select **Setup : Cameras : Presets**.

On this page you can:

- Create, change, or delete camera preset positions in the system.
- Save changes to camera preset positions to the camera website.

Camera preset positions must first be set at each camera web site. See the camera manufacturer's documentation for how to set presets for your camera.

For setting up camera presets in the system you will need to enter the preset **Name** and **Preset Number** exactly as it is entered on the camera's web site.

### To add a camera preset position to the system:

1. Click the **add** link just under the **Name** drop-down list.
2. Select from the **Cameras** drop-down list the camera that you wish to create a new preset position for.
3. Enter in the **Name** text box the exact name for this preset position that was entered on the camera's web site.
4. If this is the home position place a check in the **Home Preset?** checkbox.
5. Enter in the **Preset Number** text box the exact number for this preset position that was entered on the camera's web site.
6. Click **Save**.

### To save position changes to camera websites:

1. Select from the **Name** drop-down list a camera preset position. The **Camera** text box will have the name of the camera with the selected preset position.
2. The current image from that camera will display in the camera view. Use the camera movement controls beneath the camera image to alter the selected camera preset position.



Click the arrows to move the camera one step in the arrow direction.

Click (+) to zoom in.

Click (-) to zoom out.

3. Click **Save to Camera**.

## Setting up Camera Types

Select **Setup : Cameras : Types**.

On this page you can add, delete, and rename camera types, and edit camera type URLs.

Release 2.5 of the Network Controller supports the following camera types:

- Panasonic NM 100
- Panasonic NS 324
- Axis 2120, 232D
- Axis 205, 206
- Vivotek IP2111
- Sony SNC-DF40N/DF40P
- Sony SNC-P1
- Sony SNC-RZ30N

**NOTE:** Both the Axis and Vivotek camera types support active images using Motion JPEGs. Motion JPEGs provide smoother motion but require up to 5 megabits per second of network bandwidth. We recommend that Motion JPEGs not be used on 10 megabit networks or over remote (DSL, WAN) connections.

Axis and Vivotek camera types both default to the use of Motion JPEGs. To stop the use of Motion JPEGs and force these camera types to use standard JPEG images delete the Motion JPEG URL from the **Motion JPEG URL** text box and click **Save**. This will significantly reduce network bandwidth usage.

Motion JPEGs are supported by the Mozilla Firefox browser.

Motion JPEGs are **not** supported in Internet Explorer.

#### **To add a camera type:**

1. Click the **add** link just under the **Name** drop-down list.
2. Enter the new camera type in the **Name** textbox.
3. The camera's web site has URLs for pan, tilt, zoom, preset, and brightness functions. Enter these URLs into the appropriate URL text boxes. See the camera manufacturer documentation for these exact URLs.
4. Click **Save**.

### **Setting up Camera Views**

Select **Setup : Cameras : Views**.

On this page you can create, change, rename, or delete camera views of two (picture in a picture), or four cameras. You can select IP cameras and/or DVR cameras.

These views will be available from the [Monitoring Desktop](#) or from **Monitor : Camera Views**.

#### **To create a camera view:**

1. Click the **add** link under the **Name** drop-down list
2. In the **Name** text box enter a name for the camera view you are creating.
3. Select from the **View Type** drop-down list the type of view you want to create.
4. Select from the **Cameras Available** list a camera you wish to include in the view. You can select IP cameras and/or DVR cameras.
5. Click the right arrow button to move the selected camera to the **Selected** list.
6. Continue moving cameras to the **Selected** list until you have all the cameras needed for your view. For a **Picture-in-Picture** view choose two cameras. For a **Quadview** choose four cameras.
7. You can change the positions of cameras in the **Selected** list by selecting a camera and clicking the **Move up** or **Move down** arrow. This determines each camera's placement in the view. Cameras are placed in a view from left to right starting with the top row. For example: in a quad view the first camera in the list is in the upper left position, the second camera is in the upper right, the third camera is in the lower left, and the fourth camera in the list is in the lower right position.
8. Click **Save**.

#### **To delete a camera view:**

1. Select from the **Name** drop-down list the view you wish to delete.
2. Click **Delete**.

#### **To rename a camera view:**

1. Select from the **Name** drop-down list the view you wish to rename.
2. Click the **rename** link under the **Name** drop-down list.
3. Edit the name.
4. Click **Save**.



## **Setup Floorplans Menu**

Configure floorplan information.

<b>Choose this</b>	<b>To see Help for this</b>
<a href="#">Configure</a>	Place system resources into a floor plan image.
<a href="#">Floor plan Groups</a>	Specify groups of floor plans for use in User Roles.
<a href="#">Upload</a>	Upload an image of a site floor plan to the network controller in jpeg format.

## **Configuring Floorplans**

Select **Setup : Floorplans : Configure**.

On this page you can:

- Create or delete any floor plan in the system.
- Change the configured resources in any existing floor plan.
- Link a floor plan to another floor plan.
- Add a new floor plan to the system and add resources.

**NOTE:** Viewing and configuring floor plans requires a browser plug-in from Macromedia called Flash Player 9.0 or later.

Because configuring floor plans requires referencing existing [portals](#), [cameras](#), and [alarm events](#), create those resources before setting up floor plans.

### **To create a floorplan and add resources:**

1. Select **add new** from the drop-down list in the **Floorplan** section.
2. Select from the **Background** drop-down in the **Floorplan Details** section the jpeg image of that floor. The Background drop-down lists all previously uploaded floorplan jpegs. If you need to upload a jpeg file to use as a background see [Uploading Floorplans](#).
3. Enter a name for this floorplan in the **Name** textbox under **Floorplan Details**. This name will be added to the drop-down list in the **Floorplan** section when you click **Save Floorplan**.
4. To add resources to the floorplan image move the pointer over the floorplan image. The pointer changes to a hand icon. Click on the background image and a portal resource image appears by default. You can click and drag the icons to the correct location on the floorplan.
5. Select from the **Type** drop-down in the **Resource** section the appropriate resource type. The selected resource image changes to that resource type.
6. The **Name** drop-down in the Resource section lists all previously configured resources of that type.

Examples: if you select **Camera** from the **Type** drop-down the **Name** drop-down lists all defined cameras in the system, if you select **Link** from the **Type** drop-down the **Name** drop-down lists all other defined floorplans.

1. Click **Save Floorplan**.

### **To edit an existing floorplan:**

1. Select from the drop-down list in the **Floorplan** section the floorplan you wish to change.
2. You can edit the Name of the floorplan in the **Name** text box.
3. Any system resource in the floorplan can be selected. In the **Resource** section in the upper right of the page you can:
  - change the resource type by selecting from the **Type** drop-down list.
  - delete the resource by clicking the **Delete** button. The floorplan turns gray and you must confirm the deletion by clicking **Delete Icons**, which appears on the gray background.
  - select a different name for the resource from the **Name** drop-down list.
4. You can also click and drag any resource to a new location.
5. Click **Save Floorplan**.

### **To delete a floorplan:**

1. Select from the drop-down list in the **Floorplan** section the floorplan you wish to delete.
2. Click **Delete Floorplan**. The floorplan turns gray and you must confirm the deletion by clicking **Delete**, which appears on the gray background.

**NOTE:** This deletes the defined floorplan but does not delete the uploaded floorplan jpeg. The floorplan jpeg image is still available from the **Background** drop-down for inclusion in a new floorplan definition.

## **Creating Floor Plan Groups**

Select **Setup : Floorplans : Floorplan Groups**.

On this page you can:

- Create, change, rename, or delete floor plan groups for use in specifying User Roles.

### **To create a floor plan group:**

1. Click the **add** link just under the **Name** drop-down list.
2. Enter a name for the group in the **Name** text box, e.g. Factory floorplans.
3. In the **Events Available** list click to highlight a specific floor plan needed for this group.
4. Click the right arrow button between the **Available** and **Selected** list boxes to move the highlighted floor plan from the **Available** list to the **Selected** list. Repeat this process until all floor plans needed for this group appear in the **Selected** list.
5. Click **Save**.

### **To delete a floor plan group:**

1. Select from the **Name** drop-down list the group you wish to delete.
2. Click **Delete**.

## **Uploading Floorplans**

Select **Setup : Floorplans : Upload**.

On this page you can upload a jpeg or jpg image to the Network Controller to use as part of a floor plan.

**NOTE:** The maximum size of a floor plan jpeg image is 256K. The upload function enforces this limit.

**To upload a floorplan image:**

1. Click the **Browse** button.
2. In the **File Upload** dialog browse to the jpeg or jpg file you want to upload, select it and click **Save**.
3. The full path to the file now displays in the **Select file** text box.
4. Click **Save**.

Now that the floor plan image is uploaded you will need to create a floor plan and configure it with system resources using [Setup : Floor plans : Configure](#).

**Setup Network Resources Menu**

Specify network servers for email, storage, time and DNS services.

<b>Choose this</b>	<b>To see Help for this</b>
Domain Name Server	Enter names for primary and secondary DNS servers.
Email Settings	Enter email server name, email account name, and alert email addresses.
FTP Backup	Enter server, user name, password and directory for system backup via FTP.
Network Storage	Enter domain name, server name, share name for a network storage location, and username and password.
Time Server	Enter names for primary and secondary time servers to use to set system time.

**Domain Name Server Settings**

Select [Setup : Network Resources : Domain Name Servers](#).

The network administrator will have to supply you with the IP addresses of the domain name servers. The address must be in the form of a numeric IP address such as 192.168.1.240.

**To setup Domain Name Servers:**

1. Enter in the **Server 1** text box the IP address of the primary domain name server. This entry is required.
2. Enter in the **Server 2** text box the IP address of the secondary domain name server. This entry is optional but highly recommended.
3. Click **Save**.

## **Email Server Settings**

Select **Setup : Network Resources : Email Settings**.

On this page you can:

- Specify the email server that is setup to relay email sent from the network controller.
- Specify the email address used by the network controller.

**NOTE:** For the system to provide email notification of alert conditions the network administrator will have to setup the network mail server to relay email for the IP address of the Network Controller.

### **To setup an email server for the network controller:**

1. Enter the mail relay server name into the **Email Server** text box. Enter this in the form of an IP address or DNS name.
2. Enter in the **From email address** text box the email address for the network controller.
3. Click **Save**.

## **FTP Backup Settings**

Select **Setup : Network Resources : FTP Backup**.

On this page you can:

- Specify the FTP server that is setup to accept backups from the network controller.
- Specify the user name, password, and directory for FTP backups.
- Perform an immediate FTP backup.

The network controller serially performs daily backups and other system maintenance activities at 00:15 hours. These backups are written to the network controller board and to an FTP server if one is configured here. Backups are also automatically written to network attached storage if a local share location is configured using [Setup : Network Resources : Network Storage](#).

Backup to an FTP server will backup the:

- Security database with all configuration information.
- Photos and badge designs
- Floor plans
- Sound files
- Other images that you may have uploaded to the Controller

**NOTE:** To complete the setup of **FTP Backup** you will need the assistance of a network administrator. Once the network administrator has completed their steps they can supply you with the information for the fields on this page.

You can also perform manual backups to the network controller board and manually download them to off-board storage by selecting [Setup : System Maintenance : Backup Database](#).

### **To setup the network storage location:**

#### **Network Administrator tasks:**

1. On the FTP Server create a user name, password, and directory for the security system FTP Backups.

**NOTE:** A password is optional. The backup directory must be created at the root level of the FTP server.

2. Decide whether Active mode FTP or Passive mode FTP shall be used and ensure that firewalls will not block the needed ports.

**NOTE:** When using active FTP these ports must be open to the FTP server for FTP backups from the Network Controller.

When using passive FTP port 20 will not be required.

Ports must also be left open to the Network Controller for FTP server responses. The network administrator must set up these ports

#### **Security System setup tasks:**

1. **Enabled:** Click to place a check in the box.
2. **FTP Server:** Enter the IP address, or the DNS name of the FTP server.
3. **User name:** Enter the network controller's user account name for the FTP Server..
4. **Password:** Enter the network controller's password for the FTP Server account. A password is optional.
5. **Directory:** Enter the directory name on the FTP Server for saving backups. This directory must be at the root level on the server.
6. **Passive Mode:** If passive mode FTP is used click to place a check in this box. If this box is not checked then active mode FTP is used by default.
7. Click **Save**.
8. Now that the FTP server is configured you can click the **FTP Backup Now** button to perform an immediate backup.

#### **Setting the Network Storage Location**

Select **Setup : Network Resources : Network Storage**.

To automatically store backups to a network drive this page must be completed. The network controller performs daily backups at 00:15 hours. These backups are written to the network controller board and automatically written to network storage if a local share location is configured here. In this release the security application provides no integration with Active Directory or Domain level shares.

Backup to a network storage location will backup the:

- Security database with all configuration information.
- Photos and badge designs
- Floor plans
- Sound files
- Other images that you may have uploaded to the Controller

**NOTE:** To complete the setup of **Network Storage** you will need the assistance of a network administrator. Once the network administrator has completed their steps they can supply you with the information for the fields on this page.

You can also perform manual backups of the security database to the network controller board and manually download them to off-board storage by selecting [Setup : System Maintenance : Backup Database](#).

### **To setup the network storage location:**

#### **Network Administrator tasks:**

1. Create a network share on the same sub-net as the network controller.  
**NOTE:** The share name may **not** include spaces.
2. Create a local user account and password (as opposed to a Domain user account) for the network controller to access the network share.
3. Grant the user account share permissions and security permissions for the network share.

#### **Security System setup tasks:**

1. **Domain:** Reserved for future use.
2. **Server IP Address:** Enter the IP address of the server where the network share is located. Get this IP address from the network administrator.
3. **Share name:** Enter the name for the network share. Get this share name from the network administrator.  
**NOTE:** The share name may **not** include spaces.
4. **Directory:** Enter the directory name in the network share for saving backups. Get this directory name from the network administrator.
5. **User name:** Enter the network controller's local user account name for the network share. Get this account name from the network administrator.
6. **Password:** Enter the network controller's password for the local user account. Get this password from the network administrator.
7. Click **Save**.
8. Now that the NAS server is configured you can click the **NAS Backup Now** button to perform an immediate backup.

### **Setting the Network Time Server**

Select **Setup : Network Resources : Time Server**.

Use of a network time server ensures that the Network Controller and its nodes will be regularly synchronized with the exact time used by all other network resources. If no time server is available the network controller clock may drift slightly. Time can be manually set using [Init Mode](#).

#### **To setup a network time server:**

1. Enter in the **Server 1** text box the DNS host address name of the primary network time server. This entry is required. Get this time server name from the network administrator.
2. Enter in the **Server 2** text box the DNS host address name of the secondary network time server. This entry is optional but highly recommended.
3. Enter in the **Server 3** text box the DNS host address name of the tertiary network time server. This entry is optional.
4. Select from the **Timezone** drop-down the correct time zone for this installation. This enables the network controller to determine the correct local time.
5. Click **Save**.

**NOTE:** If you have specified an internet time server and there is no internet connection, then there will be several minutes delay when booting the Network Controller.

## Setup Site Settings Menu

Specify hardware and application user roles.

Choose this	To see Help for this
<a href="#">Add Software License</a>	Uploading and applying a software license file.
<a href="#">Network Controller</a>	Specify Network Controller name, location, IP information, time zone, and daily backup schedule. Enter support contact information, picture URL and select an enrollment reader.
<a href="#">Network Nodes</a>	Configure each node's resources.
<a href="#">System Rules</a>	Define system rules for portal group behavior.
<a href="#">User Roles</a>	Select roles and privileges for authorized security application users.

## Adding a Software License File

Select **Setup : Site Settings : Add Software License**.

With this page you can upload a new license file (\*.lic). the license file determines which features of the security system are available.

**NOTE:** When a license file is uploaded it is automatically and immediately applied. Any system users, other than the user applying the license, must log out and log back in to start a new session for their menus to update.

### To upload a software license file:

1. Click the **Browse** button to browse to the location of your license file.
2. In the Browse dialog box select the license file you want to upload and apply.

**NOTE:** License files must end with the .lic extension.

3. Click **Save**.

See also: The application About page. Select **Support/Utility : About**. This page displays version information.

## Setting up the Network Controller

Select **Setup : Site Settings : Network Controller**.

### **Network Controller**

**Company name:** Enter the organization name here.

**Location name:** Enter the location name of the Network Controller here. This name will appear in the header of the application window whenever you are logged in to this particular Network Controller.

### **Current Status**

Nodes shown here in **green** are enabled and communicating with the network controller. Nodes shown here in **red** are not currently communicating with the network controller.

## Time Settings

In this section you can manually set the correct time and date on the network controller.

## Initmode Settings

**Initmode:** these IP settings are usually set during initial installation.

## Localization

Click the link to select the interface and Help system language, and date formats.

## Support Information

**Support:** Enter the name of the organization that will provide support for this installation.

**Person:** Enter the name of the person who will be the primary support contact for this installation.

**Phone:** Enter the support contact phone number.

**Email:** Enter the support contact email address.

**URL:** Enter the URL (Universal Resource Locator) of the organization that will provide support for this installation.

## API

In this section you can enable the API for programmatic data exchange between existing personnel systems and security database records. By default this API interface is disabled.

When using API commands the security system uses SHA authentication, and message sequence numbers to ensure the security and integrity of the system. Each API command is accompanied by a MAC (message authentication code) and a sequence number. The MAC must be correct and the sequence number must be greater than sequence number of the previous command or the system will ignore the message.

**Enabled:** Click to check this box if you wish to enable the use of the API for data exchange.

**Use Authentication:** This box is checked by default. It is strongly recommended that this be left checked. SHA authentication makes API usage secure.

**SHA Secret:** Enter your SHA secret password. This password is used, along with other data, by the SHA calculator in creating a unique message authentication code.

**Re-enter SHA Secret:** Enter the SHA secret again to ensure accuracy.

**Sequence Number:** This number increments sequentially. You cannot enter anything in this box.

**Reset Sequence Number to '0':** Click to check this box and then click **Save**. This resets the sequence number to zero.

## Misc. Information

**Photo ID URL:** Enter the URL for storage of pictures of people used on the Personal Information page. These images can be in jpeg, png, or gif format.

- Select the **On Network Controller** radio button to use the URL on the network controller, **/upload/pics/**. **NOTE:** the on-board storage space for image files is limited.
- To use off-board storage for image files select the radio button beside the text box and enter in the text box the URL of any web accessible server.

**Default Photo ID Layout:** Select from the drop-down the badge design the you wish to use for most ID cards. You can change this, if necessary, when issuing cards.



**Enrollment reader:** Select from the drop-down list the reader that you wish to use for issuing access cards.

**Default Card Format:** Select from the drop-down list the most common card format. You can change this, if necessary, when issuing cards.

**Hide unpermitted Access Levels:** Selecting **Yes** will hide access levels from system users who do not have the proper [User Role](#) to see these access levels.

**PIN entry timeout** sets the time allowed for PIN entry after a card read at a portal.

**ODBC Report user password:** You can connect directly to the network controller with ODBC and create reports from the security database. Enter here the password for use with this feature. Be sure to click the **Enabled** checkbox to the right to enable this feature. The default password is "report." The Username is "report."

**Log Archive Interval:** Select from the drop-down the desired time interval for automatic creation of [Activity Log](#) archive files.

**Temperature Scale:** Select Celsius or Fahrenheit for temperature inputs.

**Unacknowledged Alarm Audio:** Select **Yes** for the system to play a wav file once per minute as long as an unacknowledged alarm is active. From the **Sound** drop-down select the sound file you want to hear.

If you select **<add new>** an **Upload Sound File** window appears. Click Browse and select the sound file you want to upload to the Controller.

**NOTE:** Sound files (.wav) are limited to 50K and no more than 10 can be uploaded to the Controller. To delete sound files select Setup : System Maintenance : Utilities.

## User Interface

SSL Certificates: **Click the Configure SSL button to display a pop-up window where you can enter certificate information.**

**Require SSL Connections:** The default value here is **NO**. If you wish to require the use of SSL connections select **YES** from this drop-down.

**Limit Session to single IP address:** The default value here is **YES**. This is the more secure setting. This ensures that if an IP address changes during a session that the user will be required to login again. Changing this to **NO** will allow more than one IP address to participate in a single session.

**Session Timeout:** Select from the drop-down the timeout duration for each session. If there is no system activity for the duration of the timeout counter you are automatically logged out and will have to log in again.

**NOTE:** If you are monitoring the activity log then the session will not timeout since the log continually updates, thus maintaining system activity.

**Display the Person PIN in the Person Detail page?:** The default value here is **YES**. If you wish to hide the display of individual PIN numbers select **NO** from this drop-down.

**Floorplan refresh every:** Select the frequency in seconds for refreshing the floorplan displays.

## Creating Rules to Change System Behavior

Select **Setup : Site Settings : System Rules**.

On this page you can:

- Create or delete a First-in Unlock rule for use in specifying portal group unlock behavior. This rule is used to modify the regular locking and unlocking behavior of a [portal group](#) with an assigned [unlock time spec](#).

**For Example:** The main entrance to a facility should be unlocked from 9AM to 5PM as long as there is a receptionist on duty.

- Place the "main Entrance" portal into a portal group and assign it an unlock time specification of 9:00AM to 5:00PM.
- Create an access level called "Receptionist In" and another called "Receptionist Out."
- Create a First-in Unlock rule that requires a read of the "Receptionist In" access level before a portal group can unlock. This rule should also specify that the portal group relocks when the system receives a read of the "Receptionist Out" access level.
- Assign the "Receptionist In" access level to the receptionist and issue them a badge.
- At 9AM the main entrance will unlock only if the system has seen a badge read with the access level "Receptionist In."

**NOTE:** The portals in the group unlock only when the First-in Unlock rule is satisfied **AND** the unlock time spec is valid.

- The portals in the group will relock at 5PM (when the unlock time spec becomes invalid) **OR** when the system has seen a badge read with the access level "Receptionist Out."

**CAUTION:** You cannot grant both "In" and "Out" access levels to the same person and badge. The portal group will unlock and relock immediately. These access levels must be on separate badges. We suggest adding 2 "people" to the system named "Receptionist In" and "Receptionist Out." The appropriate access level can be granted to each of these "people" and two badges issued.

#### **To create a First-in Unlock rule:**

1. Click the **add** link just under the **Name** drop-down list.
2. Enter a name for the First-in Unlock rule in the **Name** text box, e.g. weekday unlock rule.
3. On the **First-in Unlock** tab select from the **unlock access level** drop-down an access level for use as an unlock rule.
4. Select from the **rellock access level** drop-down an access level for use as a rellock rule.
5. Click **Save**.

**NOTE:** You must assign this rule to a [portal group](#) with an [unlock time spec](#).

#### **To delete a system rule:**

1. Select from the **Name** drop-down the rule you wish to delete.
2. Click **Delete**.

## **Configuring Network Nodes**

Select **Setup : Site Settings : Network Nodes**.

With this page you can:

- [Enable a selected node](#) for communication with the Network Controller.
- [Change node network settings](#).
- [Set the discovery method](#) used by the node to find the controller.
- [Protect a node](#) IP configuration to keep it from changing.
- [Configure tamper and disconnect events](#) for a node.
- [Reboot a node](#).
- [Reset a node to factory default settings](#).

- [Swap node unique identifiers.](#)
- [Reset node networking settings.](#)
- [View the slot positions and resources](#) of Access, Input, Output, and Temperature application blades.

A node consists of a Node blade and any combination of Access, Input, Output, and Temperature blades. Nodes broadcast their 16 character unique IDs to register with any available Network Controllers. Once registered they will appear in the **Name** drop-down list. However, communications between the Network Controller and the Node can go no further until the node is enabled. If you are installing a system with multiple nodes it is recommended that nodes be brought up one at a time because the 16 character unique IDs will not indicate which node is which.

#### **To enable a Node:**

1. Select from the **Name** drop-down the node you wish to enable.
2. You can click the **Rename** link under the drop-down to enter a name that will help you to identify it, e.g. "FirstFloor Node."
3. Click to check the **Enabled** box to the right of the **Name** drop-down. This allows the communication of security data between the Network Controller and the Node.
4. Do not change the **Unique Identifier** field. This contains the 16 character unique node ID.
5. Click **Save**.

#### **To change node network address settings:**

This procedure allows changing node network settings for nodes that are either on the same subnet as the controller, or nodes that are on another subnet but already connected. To see if a node is connected select **Setup : Site Settings : Network Controller**.

To change node network settings for nodes on other subnets that are not yet connected and therefore not accessible to the controller, you will have to run the [nconfig utility](#) on a computer that is on the same subnet as the node.

**NOTE:** You cannot change both the node network address settings and the controller discovery settings at the same time. Change one first, save it and then change the other.

1. Select from the **Name** drop-down the node for which you wish to change network settings.
2. Click the **Network** tab.
3. The text boxes for, **Node IP Addressing Scheme**, **IP Address**, **Subnet Mask**, and **Gateway**, display the values associated with the selected Node. You can edit these values.
4. You can protect this IP configuration by placing a check in the **Configuration Protected** checkbox.
5. Click **Save**. It may take several minutes for the node and the Network Controller to complete this communication.

#### **To set the discovery method:**

1. Select from the **Name** drop-down the node for which you wish to change the controller discovery method.
2. Click the **Network** tab.
3. The text boxes for, **Node IP Addressing Scheme**, **IP Address**, **Subnet Mask**, and **Gateway**, display the values associated with the selected Node.

4. You can **Allow Network Controller autodiscovery** by the node by placing a check in the checkbox or you can uncheck the box and enter the IP address of the controller in the **Network Controller IP Address** text box.
5. Click **Save**.

**NOTE:** You cannot change both the node network address settings and the controller discovery settings at the same time. Change one first, save it and then change the other.

#### **To protect a node IP settings:**

1. Select from the **Name** drop-down the node whose IP settings you wish to protect.
2. Click the **Network** tab.
3. Put a check in the **Configuration Protected** box.
4. Click **Save**.

**NOTE:** The IP settings for this node cannot be changed until you uncheck the **Configuration Protected** checkbox.

#### **To configure Tamper and disconnect events for a node:**

**NOTE:** Before you can assign events you must define the events using [Setup : Alarms: Events](#).

1. Select from the **Name** drop-down the node for which you wish to configure events.
2. Click the **Events** tab.
3. Select from the **Tamper Alarm Event** drop-down the event to execute if the tamper switch on the Node cabinet enters an alarm state. Click to check the **Enabled** box to the right.

**NOTE:** The tamper switch enters an alarm state if the system cabinet door is opened.

4. Select from the **Disconnect Event** drop down the event to execute if the Node should disconnect from the Controller. Click to check the **Enabled** box to the right.
5. Click **Save**.

#### **To reboot a node:**

The **Reboot** button causes the node to restart. This can take from one to several minutes. Resources (portals, inputs, etc.) associated with this node will be inaccessible during that time.

1. Select from the **Name** drop-down the node you wish to reboot.
2. Click the **Commands** tab.
3. Click **Reboot**.

Look in the [Activity Log](#) for confirmation that the node reboot has completed.

#### **To reset a node to its factory defaults:**

**CAUTION:** The **Reset to Factory Defaults** button deletes all configuration information from the Node except the IP settings information. It also resets the code version to that installed at the factory.

For example: If you purchased a version 2.2 system and then upgraded to version 2.5, the **Reset to Factory Defaults** option will make the node version 2.2 again. However, as soon as the node reconnects to a version 2.5 controller it will be automatically upgraded.

Call for support before using this option.

### **To swap node unique identifiers:**

Typically this node ID swapping option would be used only when replacing a node for service reasons. The new node can be associated with the old node's **Unique Identifier** so that the **Resource Details** will not have to be re-entered for the new node blade.

Call for support before using this option.

1. Select **Setup : Site Settings : Network Nodes** and note the name of the node you will replace.
2. Power down the system.
3. Replace the old node blade with the new node blade.
4. Power up the system.
5. Select **Setup : Site Settings : Network Nodes**.
6. Select the new node from the **Name** drop-down and rename it "Temp Node."
7. Click **Save**.
8. Click the **Commands** tab.
9. Click **Swap Node**. A message window appears.
10. In the message window select the old node from the **with node** drop-down.
11. In the message window click **Save**.

**NOTE:** The newly installed node blade is now associated with the resources (inputs, portals, etc.) formerly managed by the old node.

12. Select **Temp Node** from the **Name** drop-down.
13. Click **Delete**.

### **To reset node networking settings:**

This resets all the networking settings on the node. It will adopt a zeroconf IP address and begin multicasting for a controller.

1. Select from the **Name** drop-down the node whose networking settings you wish to reset.
2. Click the **Commands** tab.
3. Click **Reset Node Networking**.

### **To view blade positions and resources:**

1. Select from the **Name** drop-down the node whose resources you wish to view.
2. Click the **Blades** tab.
3. In the **Blade Type** column click the link for the blade you wish to view.

A picture of the application blade appears and to the right are links for **Resource Details** and the **Status** of each resource.

## **Assigning Security Application User Roles**

Select **Setup : Site Settings : User Roles**.

On this page you can define and name detailed custom user roles for users of the Security Application.

**NOTE:** For selecting a user role for a specific system user use the [Login tab](#) of the [Personal Information page](#).

The Security Application Main Menu is built dynamically for each user who logs in. It will show only those menus, cameras, access levels, elevators, floor plans, events, and personal information that the user has permission to view or use based upon their assigned user role.

### **To create a custom set of user roles**

1. Click the **add** link just under the **Name** drop-down list.
2. Enter a name for this set of user roles in the **Name** text box, e.g. security monitor roles.
3. Select from the **View System/Node Messages** drop-down whether this role should include seeing [controller and node message files](#).
4. Select from the **Threat Level Group** drop-down list a threat level group to assign to this user role. This user role will function only if the current system threat level is a member of the assigned threat level group.

**NOTE:** Select **<not applicable>** if the system threat level should NOT affect the behavior of this user role.

5. For **Camera Groups**, **Elevator Groups**, **Floorplan Groups**, **Portal Groups**, **Event Groups** and **Access Levels** select from the **Available** list boxes and click the right arrow to move them to the **Selected** list boxes. Do this for all the items that you wish included in this user role.

**NOTE:** To the right of each group's list boxes are one to three check boxes. A check in these check boxes enables that particular user role. For example: for **Camera Groups** check **View** to allow a user to see the camera images, check **Presets** to allow the user to move cameras to preset positions, and check **PTZ** to allow a user to have full pan, tilt, and zoom control.

**CAUTION:** Floorplan permissions are a special case. Allowing a system user access to a floorplan will allow them access to all resources placed on the floorplan regardless of the permissions granted elsewhere on this page.

If, for example, you wish to restrict some user's access to a particular portal you can create two floorplans. Place the particular portal on one of the floorplans, and not on the other. Assign the two versions of that floorplan appropriately.

6. Select from the **Personal Information Available** list box the specific permissions you wish to assign to this user role and click the right arrow to move them to the **Selected** list box.
7. Click **Save**.
8. Now go to the **Login** tab of the [Personal Information](#) page to assign this defined user role to a specific person.

### **Setup System Maintenance Menu**

Backup, Restore, refresh, and update system software and databases.

<b>Choose this</b>	<b>To see Help for this</b>
Backup Database	Perform an immediate security database backup to the controller board or download an existing backup to off-board storage.
Restore Database	Perform an immediate restore of the on-board security database backup or upload an existing backup from a network storage location.
Update System Software	Update the security application to the latest revision.
Utilities	Refresh security database and system configuration data to nodes, file cleanup of images and backups, System Halt and Reboot, upload database backups and dealer info files to the controller board.

## **Backup the Security Database**

Select **Setup : System Maintenance : Backup Database**.

The network controller serially performs daily backups and other system maintenance at 00:15 hours. These backups are written to the network controller board ROM, to a network storage local share location if one is configured, and to an FTP Server if one is configured.

With this page you can:

- Backup the security database from RAM to ROM on the network controller board.
- Backup the security database to a network attached storage if one is configured using [Setting the Network Storage Location](#).
- Download a backup of the security database to off-board storage.

### **To manually backup to the network controller:**

1. The **Existing Backups** list contains the date and comment of existing security database backups.
2. In the **Backup Database** section enter a descriptive comment about this backup. This comment will later appear above under **Existing Backups**.
3. Click **Backup Database** and the current security database is copied to ROM on the network controller board and to the [network storage location](#) if one is configured. It may take the network controller a couple of minutes to complete this operation.
4. Click **Full Backup** and the database as well as all other system files (e.g. user photos, floor plans, sound files, etc) are saved to a [NAS](#) or [FTP](#) server if they are configured. It may take the network controller up to 2 minutes to complete this operation.

### **To download a backup to off-board storage:**

1. In the **Existing Backups** table click **get** for the backup you wish to save to off-board storage.
2. In the **File Download** dialog click **Save**.
3. In the **Save As** dialog browse to the location where you wish to save this backup.
4. Click **Save**.

## **Restoring the Security Database**

Select **Setup : System Maintenance : Restore Database**.

The network controller maintains an on-board backup copy of the security database. The network controller performs daily backups at 00:15 hours. These backups are written to the network controller board and to a network storage location if one is configured. See [Setting the Network Storage Location](#).

The security database can only be restored from copies on the network controller board. You can upload to the controller board database backup copies that have been stored off-board by selecting the upload link provided or choosing [Setup : System Maintenance : Utilities](#).

### **To restore the security database from on-board backup:**

1. Select from the list of backups the one that you wish to restore by clicking the radio button in the **Restore?** column.
2. Click **Restore Now** and the selected backup security database is restored.

## Updating the Security Application Software

Select **Setup : System Maintenance : Update Software**.

Updating the Security Application is a 3-step process.

1. Click the **1. Backup Database** link and [backup the security database](#).
2. To return to the Software Update page select **Setup : System Maintenance : Update Software**.
3. Click the **2. Upload the file** link and from the Upload page browse to the appropriate .tgz file and click **Save**. This copies the update file to the Network Controller.

**NOTE:** Refer to Tech Note 3.X "Software Upgrade Paths" for specific information about the updates to apply.

4. Click the **3. Apply the update file** link and the security application will display all available on-board software update files.
5. Select the software update you wish to apply by clicking the appropriate button in the **Apply?** column.
6. Click **Apply Update Now**. This may take several minutes to apply, and then you will hear a double-beep. It will then take several more minutes to reboot and reload services and you will then hear a single beep.
7. Log back in to the Security Application.

## System Maintenance Utilities

Select **Setup : System Maintenance : Utilities**.

### File Management \_\_\_\_\_

You can review and delete Floorplan images, Photo ID Layouts, Photo IDs, Database backups, sound files, and System updates.


#### To delete a Photo ID Layout:

1. Click the **Photo ID Layouts** link.
2. Select the badge layouts you wish to delete by placing a check in the **Delete?** checkbox to the right of each.
3. Click **Delete File(s)**.

#### To delete Database backups:

1. Click the **Database backups** link.
2. Select the backups you wish to delete by placing a check in the **Delete?** checkbox to the right.

Note that all database backup filenames contain date and time stamps.

Filename	Delete?
s2config_20041214_112554.dmp.gz	<input type="checkbox"/>
	

- #1 - Date stamp YYYYMMDD
- #2 - Time stamp HHMMSS

4. Click the **Delete File(s)** button.



### **To delete Floorplan images, Photo IDs, System updates, or Sound files:**

1. Click the appropriate link.
2. Select the items you wish to delete by placing a check in the **Delete?** checkbox to the right of each.
3. Click the **Delete File(s)** button.

## **Upload Service Provider Files**

You can upload an HTML page (which must be named "support.html") and any gif, jpeg, or png images used by that page, for display when Setup : Support/Utility : Dealer Info is selected.

### **To upload a support information file and images:**

1. Click the **Upload the file** link.
2. Click the **Browse** button to browse to the location of your "support.html" file and any images that it uses.
3. Click **Save**. The selected file is saved to the network controller board

## **Upload Sound File**

You can upload sound files to use in announcing alarms. To set up the use of a sound file to announce an alarm event use Setup: Alarms: Events.

**NOTE:** Sound files (.wav) are each limited to 50K maximum, and a maximum of 10 can be stored on the Controller. If you have a compact flash installed on your Controller you can store up to 100 sound files on the compact flash.

### **To upload a sound file:**

1. Click the **Upload Sound file** link.
2. Click the **Browse** button to browse to the location of your .wav file.
3. Click **Save**. The selected file is saved to the network controller board

## **Update Disk Usage**

Clicking the **Update Disk Usage** button refreshes the ROM, RAM disk, and Flash Card usage statistics displayed when you select Support/Utility : About.

## **Add/Remove Compact Flash Card**

The system will not auto-detect the presence or absence of compact flash cards.

Click the **Add CF Now** button **after** you have physically installed the compact flash card on the Network Controller blade.

Click the **Remove CF Now** button **before** you have physically removed the compact flash card from the Network Controller blade.

**NOTE:** You must completely power down the system before installing or removing compact flash cards.

## **Manage files on the remote server**

Click the **FTP Server** button to select and upload the most recent backup files from the FTP server to the controller board. You can then restore the database backup to the system by using the Restore Backup page.

Click the **NAS Server** button to select and upload the most recent backup files from the NAS server to the controller board. You can then restore the database backup to the system by using the Restore Backup page.

**NOTE:** The database backup is the only file that requires a "Restore" action. All other files (user photos, floor plans, sound files, badge layouts, etc) need only be "Retrieved" by clicking the **Retrieve** button after making your selections.

## Database Maintenance \_\_\_\_\_

### Repair Database Tables

Clicking the **Repair Tables** button executes a MySQL command designed to repair some data table corruptions that can occur. Normally this should not be necessary. System support may request that you perform this operation.

### Reset Events

You can reset all events and event actions by clicking **Reset Events**. Normally this should not be necessary. If an event persistently reappears then the inputs involved should be investigated as they may have wiring problems.

## Diagnostics \_\_\_\_\_

### Test Network Connection

You can ping a known network IP address to check for connectivity between the security system Network Controller and other network devices.

#### To test a network connection:

1. Click the **Test Network Connection** link. The Test Network Connection page displays.
2. Enter the **IP address or DNS name** into the text box and click **Check Connection**.
3. Within a few seconds the PING results display on the page.

### Get Node Messages File

This file may be requested by system support for diagnostic purposes.

### Get Network Controller Messages File

This file may be requested by system support for diagnostic purposes.

### Network Node Refresh

You can refresh the security database and configuration data to all system nodes by clicking the **Refresh Now** button. Nodes will normally be refreshed automatically whenever the Network Controller has new data. However, you may wish to force an immediate refresh of node data after changes have been made to the security database or configurations.

### Portal Status Display

This utility displays in table form all configured nodes, portals, readers, inputs, and outputs. Slot and position number, status and/or state for each resource is shown.

This is a very useful report for diagnosing system configuration issues.

## System Functions \_\_\_\_\_

### System Shutdown

You can stop the system by clicking the **Shutdown Now** button. Before the system shuts down it will store the current security database in ROM. The system will remain stopped until power is removed and reconnected. When the system reboots the security database image in ROM is read and used as the current database.

This function is intended for use when physically moving the system or performing hardware service requiring the disconnection of power.

### System Reboot

You can reboot the system by clicking the **Reboot** button. Before the system shuts down it will store the current security database in ROM. When the system comes back up the security database image in ROM is read and used as the current database.

### Setup Threat Levels Menu

Change and enter settings for threat levels and threat level groups.

A threat level or a change in threat level can effect a change in the behavior of the security system. The areas of security system behavior that threat levels can change are portal unlock behavior, alarm event actions, and the function of access levels.

Choose this	To see Help for this
<a href="#">Add/change/delete</a>	Name, set color code, and enter descriptions for threat levels.
<a href="#">Menu Order</a>	Set the order of threat levels in the menus and lists.
<a href="#">Settings</a>	Require passwords for changing threat levels and upload an image to use as a threat level color.
<a href="#">Threat Level Groups</a>	Create or edit threat level groups for assignment to access levels, alarm event actions, portals, and portal groups.

### Add, Change, or Delete Threat Levels

Select **Setup : Threat Levels : Add/change/delete**.

On this page you can:

- Add new threat levels to the system.
- Edit or delete existing threat levels.

You can configure up to eight threat levels. By default the system contains 6 threat levels: Default, Low, Guarded, Elevated, High, Severe.

Levels "Low" through "Severe" are named and color-coded to follow the United States Department of Homeland Security threat level designations. These can be edited or deleted.

Threat level "Default" cannot be edited or deleted.

#### To add new threat levels to the system:

1. Click the **add** link under the **Name** drop-down list.

2. Enter a name for the threat level in the **Name** text box. It is recommended that the name be descriptive of the threat, e.g. Unauthorized Entry, or Fire Alarm. (These are conditions under which you may wish to alter the system behavior.)
3. Enter a **Description** for this threat level.
4. Select from the **Color code** drop-down list the color to associate with this threat level.
5. Click **Save**.

#### **To edit a threat level:**

1. Select a threat level from the **Name** drop-down list. The remaining fields on the page fill with the settings for this threat level.
2. Edit any part of the threat level definition.
  - **NOTE:** Editing a threat level that is assigned to [threat level groups](#) will NOT cause a change in system behavior. The threat level ID is used to determine system behaviors. Changing the threat level name, description, or color will not change this ID.
3. Click **Save**.

#### **To delete a threat level:**

1. Select from the **Name** drop-down list the threat level you wish to delete.
2. If this threat level is defined as part of any threat level group then these groups will be listed next to **Part of group(s)**. You cannot delete a threat level while it is part of a threat level group.
3. Click **Delete**.

### **Setting the Threat Levels Menu Order**

Select **Setup : Threat Levels : Menu Order**.

On this page you can set the order in which the threat levels appear in menus and lists.

#### **To change the threat levels menu order:**

1. Select a threat level in the list box by clicking on it. It will highlight to show that it is selected.
2. Click the **Move up** or **Move down** arrow to move the selected threat level up or down the list.
3. Click **Save**.

### **Threat Level Settings**

Select **Setup : Threat Levels : Settings**.

On this page you can:

- Require password entry to change the current system threat level.
- Upload an image to the network controller to use as a threat level color or icon.

#### **To require password entry to change the system threat level:**

1. Place a check in the **Require Password** checkbox by clicking.
2. Click **Save**.

### To upload images to use for threat level colors or icons:

1. Click the **Upload Threat Level Image** link.
2. In the **Select file** text box enter the directory and file name or click the **Browse** button and select the file.
  - **NOTE:** The image file must be less than 20KB and must be named one of the following names: green.jpg, blue.jpg, yellow.jpg, orange.jpg, red.jpg, color1.jpg, color2.jpg, color3.jpg.
3. Click **Save**.

### Setting up Threat Level Groups

Select **Setup : Threat Levels : Threat Level Groups**.

On this page you can:

- Create threat level groups.
- Edit or delete threat level groups.

It is important to understand the difference between threat levels and threat level groups. The system can be in only one threat level at a time but threat level groups may contain multiple threat levels. The groups are used to alter security system behaviors.

**Example 1:** A threat level group called "Up2Elevated" is created containing the Default, Low, Guarded, and Elevated threat levels. This threat level group is assign to a [portal group](#) comprised of all portals providing access to the most security sensitive area of the building. In this case the unlock time spec for the portal group will not unlock the portals if the current system threat level is High, or Severe.

**Example 2:** A threat level group called "Severe only" is created containing only one threat level, "Severe." This threat level group is assigned to an [access level](#) allowing access to a research lab. This access level is given to all security personnel. In this case security personnel would normally not be allowed access to the research lab except when the security system is at the Severe threat level.

### To create a threat level group:

1. Click the **add** link under the **Name** drop-down list. (If no groups have yet been created there will be no **add** link. Go to step 2.)
2. Enter a name for the threat level group in the **Name** text box. It is recommended that the name be descriptive of the group, e.g. "Severe only," or "Up to Elevated."
3. Enter a **Description** for this threat level group.
4. In the **Threat Levels Available** list click to highlight a specific threat level needed for this group.
5. Click the right arrow button between the **Available** and **Selected** list boxes to move the highlighted threat level from the **Available** list to the **Selected** list. Repeat this process until all threat levels needed for this group appear in the **Selected** list.
6. Click **Save**.

### To edit a threat level group:

1. Select a threat level group from the **Name** drop-down list. The remaining fields on the page fill with the settings for this threat level group.
2. Edit any part of the threat level group definition.
  - **NOTE:** Editing a threat level group that is assigned to [access levels](#), [portals](#), [portal groups](#), or [alarm events](#) will cause a change in system behavior.
3. Click **Save**.

### **To delete a threat level group:**

1. Select from the **Name** drop-down list the threat level group you wish to delete.
  - **NOTE:** Deleting a threat level group that is assigned to [access levels](#), [portals](#), [portal groups](#), or [alarm events](#) will cause a change in system behavior.
2. Click **Delete**.

## **Setup Time Menu**

Specify time and holiday definitions for access.

<b>Choose this</b>	<b>To see Help for this</b>
<a href="#">Holidays</a>	Name holidays, specify start date and time, end date and time, and holiday groupings.
<a href="#">Network Controller</a>	Set the system time and time server.
<a href="#">Time Spec Groups</a>	Specify groups of time specs to create more complicated schedules.
<a href="#">Time Specs</a>	Name time specifications, specify start time, end time, select included weekdays and holiday groups.

## **Creating Holidays**

Select **Setup : Time : Holidays**.

With this page you can:

- Create, change, or delete holidays.
- Specify start date/time and end date/time for holidays.
- Group holidays into one of three groups for inclusion in time specs.

Holidays act as exclusions to time specifications. For example: if you create a holiday that falls on a Monday then a time specification of "weekdays" (Monday through Friday) will not include the Monday on which the holiday falls. Access attempts on that particular Monday will be denied.

If certain employees require access on that particular Monday then you must include the holiday in one of the Holiday groups provided and include the group in the [time specification](#) definition.

Holiday groups can also be used for access that must differ based on a person status, e.g. union vs non-union. Time specifications for union employees might be assigned the **Holiday group 1** (determined by contract), and time specifications for management employees might be assigned the **Holiday group 2** in order to allow access on those particular holidays.

### **To create a holiday:**

1. Click the **add** link just under the **Name** drop-down list.
2. **Name**, **Start Date**, and **End Date** are required entries. You can click the calendar icon to select a date from a calendar.
3. Start time will default to 00:00 and end time will default to 24:00. You can edit these times. Use 24 hour time format, e.g. 17:00 is 5:00 PM.
4. Select a holiday group or groups for this holiday to be a part of.
5. Click the **Save** button.

### **To edit a holiday definition:**

1. Select from the **Name** drop-down list the holiday you wish to change. The remaining fields on the page fill with the settings for this holiday.
2. Edit any of the fields.
3. Click **Save**.

**CAUTION!** Changing a holiday definition will change any [time specification](#) that the holiday belongs to and this in turn will change any [access level](#) using this time specification.

### **To delete a holiday:**

1. Select from the **Name** drop-down list the holiday you wish to delete.
2. Click **Delete**.

## **Setting the Network Controller Time**

On this page you can:

- Set the current time on the network controller.
- Enter network time server DNS names.
- Set the time zone for your area.

## **Time Settings**

Use of an NTP network time server ensures that the Network Controller will be regularly synchronized with the exact time used by all other network resources. At least one time server must be designated for the Network Controller to synchronize its own time. If no timeserver is available the Network Controller time will drift.

**Current Network Controller Time** displays the current time of the Network Controller clock.

### **Setting the Network controller time:**

1. Select from the **Manually Set Date/Time** drop-down lists the correct current time.
2. In the **Timeserver 1** field the default preset name is **pool.ntp.org**. If the network controller is installed on a network with Internet access then this setting need not be changed.

**NOTE:** If there is no Internet access then:

- the network administrator can supply you with a local network timeserver name and you can enter that name here.
  - if there is no timeserver then remove the timeserver name from this field or the network controller will spend several minutes searching for this server.
3. The **Timeserver 2** and **Timeserver 3** fields also contain the default **pool.ntp.org**. These fields can be changed as appropriate.
  4. Select from the **Timezone** drop-down the correct time zone for your area.

## **Creating Groups of Time Specifications**

Select **Setup : Time : Time Spec Groups**.

On this page you can:

- Create, change, rename, or delete groups of time specifications for use in creating complex time specifications.

These time specification groups can be used in the system anywhere that time specs can be used, such as free-access time specs with [portal groups](#) or [floor groups](#), auto-activate time specs with [output groups](#), and auto-arm time specs with [input groups](#).

#### **To create a time spec group:**

1. Click the **add** link just under the **Name** drop-down list.
2. Enter a name for the time spec group in the **Name** text box, e.g. weekend time specs.
3. In the **Time Specs Available** list click to highlight a specific time spec needed for this group.
4. Click the right arrow button between the **Available** and **Selected** list boxes to move the highlighted time spec from the **Available** list to the **Selected** list. Repeat this process until all time specs needed for this group appear in the **Selected** list. There is a limit of 8 time specs per group.

**NOTE:** As you select each time spec the graphic time spec map to the right will display the hours affected by the time spec. You can also click on the time spec map and under the list boxes the page will display the time specs that match that hour.

5. Click **Save**.

#### **To delete a time spec group:**

1. Select from the **Name** drop-down list the group you wish to delete.
2. Click **Delete**.

## **Creating Time Specifications**

Select **Setup : Time : Time Specs**.

On this page you can create, change, and delete time specifications.

Time specifications define allowed access times. You may wish to define a variety of time specs for different purposes. For example: weekdays 8AM to 6PM for those requiring access during a standard work week. Or weekdays 7PM to 10PM for those requiring only evening access such as a cleaning crew.

**Always** and **Never** are default system time specs and cannot be edited or deleted.

**NOTE:** The Always time spec allows access at **all** times, even on Holidays.

Everything on this page is a required entry except for holidays.

**NOTE:** Holidays act as exclusions to time specifications, (except for the "Always" time spec).

**For example:** If you create a holiday that falls on a Monday then a time specification of "weekdays" (Monday through Friday) will not include the Monday on which the holiday falls. Access attempts on that particular Monday will be denied. If certain employees require access on that particular Monday then you must include the [Holiday in one of the Holiday groups](#) provided and include the group in the time specification definition.

#### **To create a time specification:**

1. Click the **add** link under the **Name** pulldown.
2. In the **Name** field enter a name. Meaningful descriptive names are best, for example "Weekdays8to6."
3. In the **Description** field enter an explanation for the use of this time spec.
4. Enter a **Start Time** and an **End Time** in 24 hour format: 09:00 (for 9 AM), 17:30 (for 5:30 PM)
5. Click the **Days of the Week**, and **Holiday group** check boxes that you want included in this time spec. If no [holiday group](#) is included then no holiday access will be allowed.



6. Click **Save**.

#### **To edit a time specification:**

1. From the **Time Specification** drop-down list select an existing time spec.
2. The other fields in this page will fill in with the details of this time spec.
3. Edit the fields that require changes.
4. Click **Save**.

#### **To delete a time specification:**

1. Select from the **Name** pulldown the time spec you wish to delete.
2. If this time spec is defined as part of any access level then these access levels will be listed next to **In Access Level(s)**. You cannot delete a time spec while it is part of an access level.
3. Click the **Delete** button.

**CAUTION!** Time specifications are part of [access level definitions](#). When you change a time spec you are changing any access level that uses the time spec as part of its definition.

#### **To rename a time specification:**

1. Click the **rename** link just under the **Name** drop-down list.
2. Edit the Name text box to change the time spec name.
3. Click the **Save** button.

## **Support/Utility Menu**

Information to support the use of the security system.

<b>Choose this</b>	<b>To see Help for this</b>
About	Copyright and version information about your system.
Change Password	Change and confirm a new password.
Dealer Info	Contact information about the installing security dealer.
Help	How to use online Help.

## **About the Security Application**

Select **Support/Utility : About**.

This page displays:

- The last database backup information.
- Support contact information.
- Software version and Updates information.
- ROM, RAM, and Flash Card usage statistics.
- Licensing information.

A background task updates the ROM, RAM, and Flash Card usage statistics every 5 minutes. You can click the **Refresh** link to update them immediately.

**NOTE:** When the **% used** rises above 85% the data displays in yellow. When the **% used** rises above 95% the data displays in red and the system will reboot when the data next updates if the usage number is still above 95%. During reboot some cleanup tasks are performed which should bring the usage numbers down below 95%.

The purpose of this function is to ensure that no data are lost due to lack of space.

This is the Security Application Help version 2.5.

© 2004-2006

## **Changing a Password**

Select **Support/Utilities : Change Password**.

### **To change your password:**

1. Enter your **Current password**. Passwords are case sensitive.
2. Enter your **New password**.
3. Enter your new password again in the **Re-enter password** box.
4. Click **Save** and your new password takes effect immediately.

If your new password is identical to your current password you will see an error message. A new password must differ from the current password.

If you re-enter your new password incorrectly you will see an error message. A new password must be entered precisely as it was first entered.

## **Dealer and Support Information**

If you have any questions about the operation of your Security System call your dealer/installer.

## **How to Use Help**

### **How do I get to Help?**

Click on **help** in the upper right of your Security Application window.

### **Help Conventions**

The Security Application has a full help system that appears in a separate window. This help system is context-sensitive.

- If a help topic is available for the current application page then that help topic will automatically display when you click for Help.
- If no help topic exists for the current application page then the Help Table of Contents will display when you click for Help.

To assist you in finding specific fields or buttons in the security application, any text in Help that appears in **bold blue**, will be exactly the text that appears on the application page.

## Navigating and Printing Help

At the top of each topic in the Help system you will find 3 clickable navigation icons and one print icon.

- Click **Back** to return to the previous topic.
- Click **Contents** to display the Table of Contents. The table of contents is organized like the Main Menu.
- Click **Index** to display the Index. The index is alphabetically organized by keyword.
- Click **Print** to print the current help page.

Help does not have a search capability.

Many topics contain links to related topics.