



eMerge User Manual



Network Administrators Information



Place Dealer Sticker Here

Table of Contents	Page
Network Administrators Information	2
Initial System Setup Checklist	4
<u>Monitor Menu</u>	5
Activity Log	5
Cameras	8
Camera Views	9
Floor plans	10
Monitoring Desktop	11
Portal Unlock	12
<u>Administration Menu</u>	13
Arm Alarm Panel	13
Lost Cards	13
People Menu	14
Add	14
Change/delete	14
Reports Menu	15
Configuration	15
History	16
People	17
Schedule Action	19
Set Threat Level	20
Utility	20

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.

Choose this	To see Help for this
Activity Log	View logs of recent system activity.
Cameras	View individual cameras.
Camera Views	View pre-defined groups of cameras.
Floor plans	View the state of alarms and other system resources on a floorplan.
Monitoring Desktop	View alarms, logs, cameras and other system information from one desktop.
Portal Unlock	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.

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

Choose this	To see Help for this
Configuration	Reports on the current configuration of system resources.
History	Reports on system activity history.
People	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.

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 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.

5. 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:

1. Select in the left column the threat level that you wish to set the system to.
2. 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](#).

3. Click **Save**.

Administration Utility Menu

Utilities for system administrators.

Choose this	To see Help for this
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.