International Electronics, Inc.
Trusted Access Solutions™
USA & Canada (800) 421-1587 & (800) 392-0123
(760) 438-7000 - Toll Free FAX (800) 468-1340
www.ieib.com

IEI eMerge™

Tasks Guide for System Users

Version 3.3

Contents

Monitoring Doors, Cameras, and System Resources

The Monitor Menu

The Monitor menu contains all your options for viewing system activity, alarm events, and cameras.

Choose this	To do this
Activity Log	View logs of recent system activity.
Cameras	View individual cameras.
Camera Views	View pre-defined groups of cameras.
Duty Log Entry	Enter or select a text message for inclusion in the Activity Log.
Floorplans	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.
Passback Grace	Allow a badgeholder's next badge access, free of anti-passback rules and restrictions.
Portal Unlock	View a list of portals and unlock a portal.

Monitoring all System Activities

All system monitoring functions are available on the Monitoring Desktop.

To monitor all system activities from one screen:

1. Select **Monitor : Monitoring Desktop**.
2. You can select either Events or the Activity Log to view in the upper left pane.

   NOTE: The **Events** tab will display all currently active system events. Events can be sorted by the **Date/Time**, **Priority**, or **Name** columns.
3. In the lower left pane you can also select **Events** or the **Activity Log** to view, as well as **Cameras**, **Camera Views** of multiple cameras, or **Floorplans**.
4. Four additional panes on the right side of the Monitoring Desktop allow you to view **Cameras**, which you may select, **Photo IDs** of individuals, a portal list in the **Portal Unlock** pane, and a **Threat Levels** pane indicating the current system threat level.

See Help: Configuring Floor Plans
Setting up Camera Views
Using Threat Levels

Monitoring the Activity Log

Select Monitor : Activity Log.

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.

NOTE: You can also view the Activity Log on the Monitoring Desktop.

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 person's 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 person's 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>

See Help: History Reports

The Monitoring Desktop

Entering Duty Log Comments into the Activity Log

Select Monitor : Duty Log Entry.

On this page you can:

- Enter a text message for inclusion in the Activity Log.
- Select a preset message for the Activity Log.

To enter a duty log entry into the Activity Log:

1. From the **Use Duty Log Response** drop-down you can select a preset text entry.
2. Alternatively you can enter your own text comment in the **Enter duty log message** text box.
3. Click **Save**.

   NOTE: You can see the entries in the Activity Log by clicking on the clipboard icon at the end of a **Duty log entry** line. You can double click on any Activity Log entry and a pop-up window appears to allow you to append a duty log entry to that particular activity log item.

See also: Monitoring the Activity Log

The Monitoring Desktop

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.

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.

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.

See Help: The Monitoring Desktop
Creating Camera Preset Positions
Setting up Camera Types
Setting up Digital Video Recording
Setting the Camera Menu Order

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 four 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 described below.

   NOTE: If the camera does not have these capabilities, or you have not set up 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 and 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.

See Help: The Monitoring Desktop
Setting up Camera Views
Creating Camera Preset Positions

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.

To monitor a floorplan:

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.

See Help: The Monitoring Desktop
Configuring Floorplans
Uploading Floorplans

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 t**o 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 Help: Monitoring the Activity Log.

Cameras Tab

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

See Help: Monitoring Cameras.

Camera Views Tab

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

See Help: 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 Help: 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 to which you wish to set the camera. 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.

See Help: Monitoring the Activity Log
Monitoring Cameras
Monitoring Camera Views
Monitoring Floorplans
Setting up Alarm Events
Setting up Camera Views
Setting up Digital Video Recording
Creating Camera Preset Positions

Unlocking Doors (Portals)

Select Monitor : Portal Unlock.

On this page you can:

- Perform an immediate momentary unlock of any portal.
- Specify and perform an extended (scheduled) unlock of any portal.

To perform an immediate momentary unlock:

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

To perform an extended (scheduled) unlock of a portal:

1. In the **Name** column, find the portal you wish to unlock.
2. Click the **Schedule** link in the **Extended Unlock** column. A **Scheduled Action** popup 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.

To create a regular schedule for doors to be unlocked:

1. Select **Setup : Access Control : Portal Groups**.
2. Create a Portal Group for the door.
3. From the **Unlock Timespec** drop-down, select the time specification you wish to use for a regular unlock time schedule.
4. Click **Save**.

See Help: Portal Groups
Scheduling Actions
Time Specifications
Monitor Cameras

Acknowledging and Responding to Alarm Events

Responding to alarm events may include taking steps to follow local site specific security policy as well as using the system to acknowledge and investigate the alarm event.

To acknowledge alarm events:

1. Select **Monitor : Monitoring Desktop**.

In the **Events** tab on the **Monitoring Desktop** events are sorted in priority order, by default. 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** button to stop the alarm event actions from occurring.

See Help: Setting up Alarm Events

The Monitoring Desktop

Managing People Data

The People Menu

Using options on the People menu, you can enter and change information about system users.

Select **Administration : People**.

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

Adding People to the System

Select Administration : People : Add.

A person must first be added to the system before issuing a badge, assigning an access level, or printing a badge.

To add a person to the system:

1. Select **Administration : People : Add**.
2. In the text boxes enter **Last Name** and **First Name**.
3. **Activation Date/Time** defaults to today but can be changed.
4. 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.
5. If your organization issues ID numbers this can be entered in the **ID#** text box.
6. If your organization uses personal identification numbers enter this 4 digit number in the **PIN** text box.
7. 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.

See Help: Changing/Adding Personal Information
Issuing an Access Card
Issuing a Temporary Card

Changing Personal Information

Select Administration : People : Change/delete.

On this page you can:

- Add or change personal information including contact and vehicle information, access level, photo, and user role permissions.
- Delete or Undelete a person's record. Note that deleting a person's record does not remove it from the system, but rather deletes it from the active roster. When viewing a deleted record the **Delete** action button changes to **Undelete**.

To change a particular person's record:

1. Select **Administration : People : Change/delete**. 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.
2. If you wish to also see deleted records check the **include deleted records** box.
3. If you wish to see expired records check the **include expired records** box.
4. Click the **Search** button.
5. The **Personal Information Detail** page, or a list of all matched names, appears. If the search returns a list of names, click on the name of the person whose record you wish to edit.
6. Make any needed changes and then click **Save**. The sections that follow describe the information you can view and change.

See Help: People Reports

Adding a Person

Personal Information Section

1. **Last Name**, **First Name** and **Activation Date/Time** fields are required entries. You can click on the calendar icon to display a calendar for selecting dates.
2. Enter an **Expiration Date/Time** if you wish the person's access to expire automatically at a particular date and time.

   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 it is recommended that the old expiration date be deleted.
3. If your organization issues ID numbers this can be entered in the **ID# text** box.

Access Control Tab

On this tab you can issue or revoke access cards and assign Access Levels.

See Help: Changing Access Control

Photo ID Tab

If your system is licensed for Badging you will see a **Photo ID** tab**.** On this tab you can capture and save user photos, digital signatures, and create and print access badges.

See Help: Printing Photo IDs

User-defined Tab

These five fields can be customized and used by your organization to contain any data that you need to capture about people in your system.

See Help: Configuring the Personal Information Page.

Contact Tab

This information is optional and is only for the reference of the security application user.

Other Contact Tab

This information is optional and is only for the reference of the security application user.

Vehicles Tab

This information is optional.

1. The **License #** field is for the state issued license plate number.
2. The **Tag #** field is for the company issued parking permit number.

The **Tag #** field can be used to search for a **Personal Information** record. If your organization does not issue parking tag numbers you can enter the license plate number in this field. You will then be able to search to determine who owns a particular vehicle.

Login Tab

An entry is made here only if the person is a user of the Security Application.

> **NOTE**: You can configure an LDAP server for single sign-on password authentication. Passwords would then not be entered here.

1. Enter a **Username**.
2. Have the user enter their password in both the **Password** and **Re-enter Password** fields.
3. Select from the **User Roles** drop-down the appropriate user role for this person.
4. Click **Save**.

In Release 2.5 and Release 3.3, there are four levels of user roles for security application users. From lowest to highest they are:

- **Monitor** -- these users may only use the functions in the Monitor menu.
- **Administer** -- these users may use the functions of both the Administration and Monitor menus.

- **Setup** -- these users may use the functions of the Setup, Administration, and Monitor menus.
- Custom User Roles -- in addition to the roles above you can also assign custom user roles created using the **Setup : Site Settings : User Roles** page.

The 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 roles.

See Help: Assigning Security Application User Roles.

Recent Activity Tab

This tab provides a report of the last ten (10) system events generated by this particular user.

See Help: Access History Report

Issuing Access Cards to Employees

Before an access card can be issued the employee name and activation date must first be entered into the system.

To issue an access card:

1. Select **Administration : People : Change/delete**. 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.
2. From the Access Cards list on the Access Control tab select <add new>.
3. In the **Card Format** field select from the drop-down list the card type being issued.
4. Enter the Hot stamp number printed on the card in the **Hot Stamp #** field.
5. Click the **Read Card** button.
6. The **Issue Card** pop-up window will appear.
7. Check the **Reader** drop-down to ensure that the enrollment reader you are using is selected and click the **Go** button.
8. Swipe or pass the card by the reader and the electronically encoded number in the card will appear in the **Encoded #** field back in the application window.

   NOTE: In the **Access Levels** section on the right side of the **Access Control** tab, be sure that this employee has appropriate access levels in the **Selected** list.
9. Click **Save**.

See Help: Setting up Access Levels

Adding people to the system

Changing Access Control

Select **Administration : People**, enter a name and click **Search**.

On the **Access Control** tab of the Personal Information page you can:

- Issue a new card.
- Revoke a card.
- Disable a card.
- Assign access levels.

Each individual in the system is limited to a maximum of 16 access levels.

To issue a new card using a reader:

1. Select **Administration : People**, enter a name and click **Search**
2. From the Access Cards list on the Access Control tab select <add new>.
3. In the **Card Format** field select from the drop-down list the card type being issued.
4. Enter the Hot stamp number printed on the card in the **Hot Stamp #** field.
5. Click the **Read Card** button.
6. The **Issue Card** pop-up window will appear.
7. Check the **Reader** drop-down to ensure that the enrollment reader you are using is selected and click the **Go** button.
8. Swipe or pass the card by the reader and the electronically encoded number in the card will appear in the **Encoded #** field back in the application window.
9. Click **Save**.

To issue a new card using keyboard entry:

1. Select **Administration : People**, enter a name and click **Search**.
2. From the **Access Cards** list on the **Access Control** tab select **<add new>**.
3. In the **Card Format** field select from the drop-down list the card type being issued.
4. Enter the Hot stamp number printed on the card in the **Hot Stamp #** field.
5. Enter the encoded card number in the **Encoded #** field.
6. Click **Apply**.
7. Click **Save**.

To temporarily disable a card:

1. Select **Administration : People**, enter a name and click **Search**.
2. On the **Access Control** tab select the card you wish to disable from the **Access Cards** list.
3. Click to place a check in the **Disabled** checkbox and click **Apply**.
4. Click **Save**. This card will not function until the check is removed.

You may wish to disable a person's card if they have forgotten their card and you are issuing them a temporary card. When the temporary card is returned their card can be re-enabled by clicking to uncheck the **Disabled** checkbox.

To assign access levels to a person:

1. Click on the **Access Control** tab.
2. In the **Access Levels** section select the access level from the **Available** box.

3. Click the right arrow button to move the access level to the **Selected** box.
4. If this individual needs extra time to get through a door then check the **Use Extended Unlock** box. (This is the ADA setting)
5. Click **Save**.

   IMPORTANT NOTE: **Access levels are assigned to people, not to cards**. All cards issued to a particular person will have the same access levels as assigned to the person. A person can have a maximum of 16 Access Levels.

To remove access levels assigned to a person:

1. Click on the **Access Control** tab.
2. In the **Access Levels** section select the access level from the **Selected** box.
3. Click the left arrow button to move the access level from the **Selected** box to the **Available** box.
4. Click **Save**.

See Help: Setting up Access Levels
Adding a Person to the System
Changing Personal Information

Revoking Access Cards

In the **Access Control** section of the Personal Information page you can issue a new card, revoke a card, temporarily disable a card, and assign access levels for any person in the system.

Revoking a card is not temporary. In this respect it differs from disabling a card. For a revoked card to function again you will have to use the procedure for issuing a new card.

To revoke a current card:

1. Select **Administration : People : Change/delete**.
2. Enter a name and/or other search data and click **Search**.
3. On the **Access Control** tab of the page select the card you wish to revoke from the **Access Cards** list box.
4. The card **Hot Stamp #** and **Encoded #** fields will fill with the card numbers.
5. Click the **Revoke Card** button.
6. This card will immediately be removed from the system and will not function.

See Help: Setting up Access Levels
Adding a Person to the System
Changing Personal Information

Changing a Password

Select Support/Utilities : Change Password.

Passwords are only needed by users allowed to log in to the security system.

> **NOTE**: You can configure an LDAP server for single sign-on password authentication. Passwords would then not be entered here. You CANNOT change an LDAP server password from this page.

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 will take effect immediately.

   NOTE: 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.

Valid Password Rules

- Passwords cannot contain quotation (' ") characters.

Tips for strong passwords

- Passwords should be changed periodically.
- Do not use passwords that can be easily guessed such as names of family members or birth dates.
- Passwords should contain at least one alpha and one numeric character.

See Help: Creating a Security Application User Account

Handling Lost Cards

Select Administration : Lost Cards.

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

To determine the identity of a 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.

See Help: Specifying Card Formats

Adding a Person

Issuing and Revoking Cards

Decoding Cards

Issuing Temporary Access Cards

Before you can issue a card to someone that person must first be added to the system.

> **NOTE**: For a card to be temporary there must be an expiration date entered into the person's record. Be aware that the expiration date attaches to the person, not to a card. When the person's record expires, all cards issued to the person also expire.

To issue a temporary card:

1. Select **Administration : People : Add**.
2. In the text boxes enter **Last Name** and **First Name**.
3. **Activation Date** defaults to today but can be changed.
4. For this entry to be temporary you must enter an **Expiration Date/Time**. If no expiration time is entered, this person, and any cards issued to this person, will expire just before midnight (23:59:59) on the **Expiration Date**.
5. Click the **Next** button. The page fills with additional fields for personal information and issuing cards.
6. On the **Access Control** tab in the **Access Cards** list select **<add new>**.
7. In the **Card Format** field select from the drop-down list the card format being issued.
8. Click the **Read Card** button.
9. The **Issue Card** pop-up window will appear.
10. From the **Reader** drop-down in the popup window select the reader to use for issuing this card and click the **Read Card Now** button.
11. Swipe or pass the card by the reader and the electronically encoded number in the card will appear in the **Encoded #** field back in the application window.
12. Click the **Apply** button.
13. Click **Save**.

See Help: Adding a Person
Revoking a Card

Working with the Photo ID Features

Multiple hardware and software products have been integrated to provide image capture and photo ID printing features from within this security application. Install the software and drivers from the CD provided and refer to the printable "Photo ID Badging Install and Setup Guide."

> **NOTE**: Photo ID printing features work with Internet Explorer only. Other browsers do not support the ActiveX controls required for these features.

On the photo ID tab you can:

- Capture ID photos and save them to the personal information record.
- Print a photo ID badge.
- Request printing of a photo ID badge.
- Print photo ID badges from the request queue.
- Capture and save digital signatures.

Capturing ID Photos

To capture ID photos and save them to a person's record:

> **NOTE**: Make sure that the Logitech QuickCam settings are set to an image size of no more than 640x480, and that **Face Tracking** is set to **Follow Me**. This will ensure that the image size remains under the maximum 80,000 bytes.

1. Select **Administration : People**.
2. Add a new person to the system or search for an existing person.
3. Click the **Photo ID** tab.
4. Select from the **Badge** drop-down the badge design you wish to use.
5. Click the **Photo ID** button and the **Photo IDs** pop-up window appears.

   NOTE: If the photo ID image window does not appear, turn off the pop-up blocker or add the Network Controller site to the allowed site list.
6. In the **Photo ID** window, click **Capture Image**. The **Select Image Source** window appears.
7. Select **Microsoft WDM Image Capture (Win32)** and click **OK**. The **Capture** window and the Logitech QuickCam application bar appear.
8. Ensure that the person is properly within the picture frame and is standing at least six feet from the camera, and then click the capture button. 

   NOTE: The software will perform “face-finding” and crop the image. This helps to ensure that the photo ID is less than the maximum allowed 80,000 bytes.
9. If the picture is acceptable click **OK**. If not, click the continue button  and recapture the photo.
10. The **Capture** window closes and the **Photo IDs** window redisplays with the image placed in the badge design. Confirm that the person’s image is correctly captured and click **Save Image**.
11. The captured image appears on the **Personal Information** page. Click the **Close** button in the **Photo IDs** window.
12. Scroll to the bottom of the **Personal Information** page and click **Save**.

NOTE: On the Personal information page you can right click on the image and select **Save Picture as**. You can then save this image separately as a jpg or bmp file.

Printing Photo ID Badges

To print a photo ID badge at your workstation:

1. The photo ID printer must be connected to your workstation with a USB cable. See the manufacturer documentation for guidance on hardware setup.
2. The printer's Windows driver listed above must be installed on your workstation. See the manufacturer documentation for guidance on software and driver installation.
3. On the Personal Information page click the **Photo ID** tab.
4. From the drop-down in the **Badge** box select the layout you wish to use.
5. Click **Photo ID**. A small photo ID window appears.
6. If you are encoding a magnetic stripe card, select the card id number from the **Access Cards** drop-down list.
7. Click **Print Photo ID**. The **Print** dialog box (or the **Card Printer Encoder Setup** dialog box if you are printing a magnetic stripe card) appears.
8. From the **Name** drop-down list, select the photo ID printer.
9. If you are printing a magnetic stripe card, click the **Magstripe** tab and select the name of the magnetic stripe encoder.
10. Click **OK** and retrieve the badge from the printer tray.
11. If you captured an image in the photo ID window, be sure to click **Save** on the **Personal Information** page. This saves the captured image and selected badge design with the person's record.

    NOTE: Magnetic stripe badge encoding is supported only in V3.3 build 344 and above of the security system software.

See Help: Uploading Photo ID Layouts

If you do not have a badge printer attached to your computer you can queue the print request for printing later at a computer that has an attached badge printer.

To request printing of a photo ID badge:

1. On the Personal Information page click the **Photo ID** tab.
2. Place a check in the **Request Photo ID** checkbox.
3. Click **Save**.
4. Select **Administration : Reports : People : Request Photo ID Report**. Verify that this report lists the request just made.

Any badge printing requests in the queue can be printed as follows:

To print requested photo ID badges:

1. The photo ID printer must be connected to your workstation with a USB cable. See the manufacturer documentation for guidance on hardware setup.
2. The printer's Windows driver listed above must be installed on your workstation. See the manufacturer documentation for guidance on software and driver installation.
3. Select **Administration : Reports : People : Request Photo ID Report**. This report lists all currently outstanding photo ID print requests.

4. Click the printer icon in the **Action** column (the rightmost column) for the badge you wish to print. A small photo ID window appears.
5. In the photo ID window click **Print Photo ID**. The **Print** dialog box (or the **Card Printer Encoder Setup** dialog box if you are printing a magnetic stripe card) appears.
6. From the **Name** drop-down list, select the photo ID printer.
7. If you are printing a magnetic stripe card, click the **Magstripe** tab and select the name of the magnetic stripe encoder.
8. Click **OK** and retrieve the badge from the printer tray.
9. Close the photo ID window.

See Help: "Photo ID Badging Install and Setup Guide" (printable)

Uploading Photo ID Layouts

Request Photo ID Report

System Data for Photo ID Layouts

Deleting Photo ID Layouts

Deleting Photo ID Layouts

Select Setup : Access Control : Utilities : Badge Layout Delete.

With this page you can delete badge layouts that have been uploaded to the controller.

NOTE: This utility can be reached from the Administration menu also. Select **Administration : Utility : Badge Layout Delete**.

To delete a badge layout:

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

See Help: Printing Badges

Request Photo ID Report

System Data for Badge Layouts

Uploading Badge Layouts for Printing

Uploading Photo ID Layouts

Select Administration : Utility : Photo ID Layout Upload.

With this page you can upload badge layouts to the controller for use in creating and printing badges.

Photo ID layouts must first be created using EPI Designer. EPI Designer is part of the EPI Builder SDK from ImageWare® Systems, Inc. For details regarding security system data that can be used in photo ID layouts see "System Data for Photo ID Layouts."

NOTE: This utility can be reached from the Setup menu also. Select **Setup : Access Control : Utilities**.

To upload a photo ID layout:

1. Click the **Browse** button to browse to the location of your photo ID layout files.
2. In the Browse dialog box select the photo ID layout file you want to upload and click **Open**.

   NOTE: Photo ID layout files must end with the .dgn extension and can be no larger than 600K.
3. Click **Save**.

See Help: Printing Photo IDs

Photo ID Requests Report

System Data for Photo ID Layouts

Creating Reports from System Data

The Reports Menu

Select **Administration : Reports**.

You can use options on the Reports menu to run a variety of system information reports.

Choose this	To see this
Configuration	Reports on the current configuration of system resources.
History	Reports on system activity history.
People	Reports on access information pertaining to people.

See Help: Using the Security Query Language

Monitoring the Activity Log

Configuration Reports

Select Administration : Reports : Configuration.

As Built Report

To run an **As Built** report, select a Node from the **Network Node** drop-down and click Run report. A new browser window will open and display an image of each application blade in the node and the specific resources configured for that blade. You can print this report.

See Help: Resources Report

Cameras Report

Displays all camera configuration information.

See Help: Creating Camera Definitions

Setting up Camera Types

Camera Presets Report

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

See Help: Creating Camera Preset Positions

Elevators Report

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

See Help: Defining Elevators

Floor Groups Report

Displays all configured floor groups for use in elevator control.

See Help: Creating Floor Groups

Naming Secure Floors

Holidays Report

Displays holiday specification information.

See Help: Creating Holidays

Creating Time Specifications

Portals Report

Displays portal definition information.

See Help: Setting up Portals

Setting up Portal Groups

Portal Groups Report

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

See Help: Setting up Portals

Setting up Portal Groups

Setting up Threat Level Groups

Reader Groups Report

Displays defined groups of readers.

See Help: Setting up Reader Groups

Resources Report

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

See Help: Setting up Readers

Setting up Alarm Inputs

Setting up Outputs

Slot and Position Numbers

Threat Level Groups Report

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

See Help: Using Threat Level to Change Portal Behavior
Using Threat Levels to Control Access
Add, Change, or Delete Threat Levels
Setting up Threat Level Groups
Threat Level Settings
Changing the System Threat Level

Threat Levels Report

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

See Help: Using Threat Levels to Change Portal Behavior
Using Threat Levels to Control Access
Add, Change, or Delete Threat Levels
Setting up Threat Level Groups
Threat Level Settings
Changing the System Threat Level

History Reports

Select **Administration : Reports : History**.

History reports can retrieve data from archives when the requested report data is no longer active on the controller board. In version 3.2 the controller maintains an active database of over 100,000 activity log records. Older data is kept in archive files both on the controller and on network attached storage devices. You can set up an FTP site or network attached storage (NAS) for this data.

Choose this	To do this
Access History Report	See reports tracing access attempts.
Custom Report	Create and run a custom report.
General Event History	See reports on specific events from the activity log.
Portal Access Count	See reports on the number of portal accesses for an individual.

See Help: Using the Security Query Language

About Archive Files

FTP Backup Settings

Setting the Network Storage Location

Access History Reports

Select Administration : Reports : History : Access History.

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.

To create an Access History report:

1. Select **Administration : Reports : History : Access History.**
2. 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.
3. 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.

4. To limit the report to a specific portal or portal group select it from the **At (portal name)** drop-down list.
5. To limit the report to specific types of events select from the **Event type(s)** list.
6. Click **Search**

See Help: About Archive Files

Security Query Language

FTP Backup Settings

Setting the Network Storage Location

Creating and Printing Custom History Reports

Select Administration : Reports : History : Custom Report.

On this page you can:

- Create custom history reports and save them for later re-use.
- Edit or delete saved custom reports.
- Run saved custom reports to get output as a tab delimited text file or a grid with columns and rows.

To create a custom history report:

1. Select **Administration : Reports : History : Custom Report**.
2. If no custom reports yet exist a tabbed interface for creating reports appears. If custom reports do exist you will see a list of them.
   - To edit an existing report, click the **Edit** link next to it.
   - To run a report, click the **Run** link next to it.
   - To create a new report, click the **New** button.
3. From the **Columns** tab select the specific columns of data that you want for this report by selecting them in the **Available** list and clicking the right arrow to move them to the **Selected** list.
4. You can sort the order of the columns by selecting an item in the **Selected** list and using the up and down arrows to move the selected item up or down the list.
5. From the **Date & Time** tab specify both a **From (date)** and a **Thru (date)** for records to be included in this report.
6. The **People Filter**, **Location**, and **Events** tabs are all filters. Anything that you specify on these tabs will restrict report results to records that match these specifications.
7. On the **Sort Order** tab you can specify the report sort order for up to five fields.
8. On the **Run-time Prompts** tab you can specify prompts for specific data entry by the report user. Report results will be filtered based on this data input at run-time.
9. On the **Output** tab you can specify the limit number of records, output format, and height and width screen display of the report.

   NOTE: The output format **Text** produces a tab delimited text file.

   The output format **Grid** produces a report in columns and rows that allows you to move columns right or left in the display or click on the column headers to sort by that column.
10. Click **Save**.

See Help: Creating and Printing Custom People Reports

About Archive Files

General Event History

Select Administration : Reports : History : 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. Select **Administration : Reports : History : General Event History.**
2. 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.
3. Click the calendar icon to select a **Thru (date)**. This is the end date for the report.
4. 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.
5. Enter in the **Limit to** text box the maximum number of records you wish to have in this report.
6. Uncheck the **All event types** checkbox in the **Parameter** column.
7. Check each specific event type you want included in a report.
8. Click **Run report**. It may take a minute for the report to be generated and displayed.

See Help: About Archive Files

Security Query Language

FTP Backup Settings

Setting the Network Storage Location

Portal Access Count Report

Select Administration : Reports : History : Portal Access Count.

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. Select **Administration : Reports : History : Portal Access Count.**
2. 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.
3. Click the calendar icon to select a **Thru (date)**. This is the end date for the report.
4. Select from the **at Portals** drop-down a specific portal for this report.
5. 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."
6. Enter a last name in the **Person (last name)** text box.
7. Click **Run report**.

See Help: Monitoring the Activity Log

The Monitoring Desktop

People Reports

Select Administration : Reports : People.

Access Levels Report

Displays all access levels entered into the system. For each access level, the report includes the specified description, time specification, reader or reader group, floor group, and threat level group.

See Help: Creating Time Specifications

Setting up Access Levels

Assigning Access Levels

Creating Floor Groups

Custom Report

On this page you can:

- Create custom reports on people and save them for later re-use.
- Edit or delete saved custom reports.
- Run saved custom reports to get output as a tab delimited text file or a grid with columns and rows.

1. Select **Administration : Reports : People : Custom Report**.
2. If no custom reports yet exist a tabbed interface for creating reports appears. If custom reports do exist you will see a list of them.
   - To edit an existing report, click the **Edit** link next to it.
   - To run a report, click the **Run** link next to it.
   - To create a new report, click the **New** button.
3. From the **Columns** tab select the specific columns of data that you want for this report by selecting them in the **Available** list and clicking the right arrow to move them to the **Selected** list.
4. You can sort the order of the columns by selecting an item in the **Selected** list and using the up and down arrows to move the selected item up or down the list.
5. The **People Filter**, and **Access Level** tabs are filters. Anything that you specify on these tabs will restrict report results to records that match these specifications.
6. On the **Sort Order** tab you can specify the report sort order for up to five fields.
7. On the **Run-time Prompts** tab you can specify prompts for specific data entry by the report user. Report results will be filtered based on this data input at run-time.
8. On the **Output** tab you can specify the limit number of records, output format, and height and width screen display of the report.

   NOTE: The output format **Text** produces a tab delimited text file.

   The output format **Grid** produces a report in columns and rows that allows you to move columns right or left in the display or click on the column headers to sort by that column.
9. Click **Save**.

See Help: Creating and Printing Custom History Reports

Current Users Report

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

See Help: Creating a Security Application User

Occupancy Report

Displays a list of defined Regions. For each region, the report includes the number of people currently occupying the region, the maximum number of occupants allowed (if a maximum has been specified), the time of the last entry into the region, the name of the person who last entered, the time of the last exit from the region, and the name of the last person to exit.

See Help: Configuring Regional Anti-Passback

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.

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**.

See Help: Printing Photo IDs

Uploading Photo ID Layouts

Portal Access Report

Displays the names and access levels of everyone allowed access at the portal you select from the **Portals** drop-down. To filter the list, you can specify a user-defined field and a value for that field. For example, if field 1 is defined as **Department**, you can include only employees from the Finance department in the report by selecting **field 1** from the **Where** drop-down and then selecting **Finance** as the field's value.

Roll Call Report

Allows you to select a defined **Region** from the drop-down to display a list of people currently in that region. To refine the report, you can select check boxes that appear below the drop-down:

- When **<all>** is selected, you can select **Ignore Uncontrolled Space** to exclude anyone who is not in a defined region.
- When **Uncontrolled Space** is selected, you can select **Show people not in the above region** to include only people who are not in the Uncontrolled Space.

- When a defined region is selected, you can select **Show people not in the above region** to include only people who are not in that region, **Ignore Uncontrolled Space** to exclude anyone who is not in a defined region, or both.

See Help: Configuring Regional Anti-passback

Roster Report

Displays a list of every person entered into the system and provides the following information for each person:

- Name
- ID Photo (thumbnail)
- Expiration date
- Date the person's record was last modified
- The region the person is in currently
- Access levels
- Card number and card format

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

See Help: Adding a Person to the System

Assigning Access Levels

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.

See Help: Creating Time Specifications

Creating Holidays

Backing up System Data and Other Utilities

Backing Up the Security Database

The system data is regularly backed up to ROM and the compact flash on the controller each night at 00:15 hours. The Sunday backup is a Full Backup. Backups on Monday through Saturday are Differential backups.

If an FTP server or NAS drive is configured all backups will be written there. We strongly recommend that an FTP site or a NAS server be set up for storing system backups off the controller board.

You can perform additional backups whenever you wish.

To back up system data:

1. Select **Administration : Utility : Backup System**.
2. Enter a **Comment** to explain the purpose of this backup.
3. Click **Full Backup**.
4. When the backup is complete it is listed in the **Existing Backups** section. You can download a copy of this backup to a disk drive by clicking the **get** link in the **Download?** column.

Configuring a NAS (Network Attached Storage)

NOTE: Once the NAS is properly set up the backup procedure backs up configuration, people, and log data, as well as user photos, floor plan images, badge designs, sound files, etc.

The regular nightly backup at 00:15 hours will write to this location if it is properly configured. To properly configure a NAS requires that both Network Administrator and Security System Setup tasks are completed as described below:

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. Select **Setup : Network Resources : Network Storage**.
2. Complete this page with the information for the share location created above.
3. Click **Save**.
4. Click **Backup Now**.

Configuring an FTP server

NOTE: Once the FTP server is properly set up the backup procedure backs up configuration, people, and log data, as well as user photos, floor plan images, badge designs, sound files, etc.

The regular nightly backup at 00:15 hours will write to this location if it is properly configured. To properly configure an FTP server requires that both Network Administrator and Security System Setup tasks are completed as described below:

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, TCP ports 20 and 21 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. Select **Setup : Network Resources : FTP Backup**.
2. Complete this page with the information for the FTP site created above.
3. Click **Save**.
4. Click **Backup Now**.

See Help: Setting up the Network Storage Location

Setting up an FTP Server for Backups

System Maintenance Database Backup

About Archive Files

Arming and Disarming Alarm Panels

Select Administration : Arm Alarm Panel.

Burglar alarm panels can be integrated with your access control system. On this page you can:

- Arm or disarm an alarm panel.

To arm or 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.

See Help: Setting up Alarm Panels

Setting up Alarm Panel Auto-arm Behavior

Setting up Alarm Panel Events

Setting up Alarm Events

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. When a threat level is changed by a system event it does not automatically reset when the event is acknowledged or cleared.

To set or change the current system threat level:

1. Select **Administration : Set Threat Level**.
2. Select in the left column the threat level that you wish to set the system to.
3. 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.
4. Click **Save**.

See Help: Using Threat Levels to change portal behavior

Using Threat Levels to control access

Assigning Security Application User Roles

Add, Change, or Delete Threat Levels

Setting up Threat Level Groups

Threat Level Settings

Configuration Reports

Setting up Access Levels

Setting up Portals

Setting up Portal Groups

Setting up Alarm Events

Monitoring the Activity Log

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.