S2 SECURITY

Integrated security for an IP-connected world

Task Guide for System Users

For the S2 NetBox™ Extreme, S2 Enterprise™, and S2 Enterprise™ Ultra

Version 4.1

S2 Security Corporation
50 Speen Street
Suite 300
Framingham, MA 01701
www.s2sys.com
S2 Support: 508 663-2505

Contents

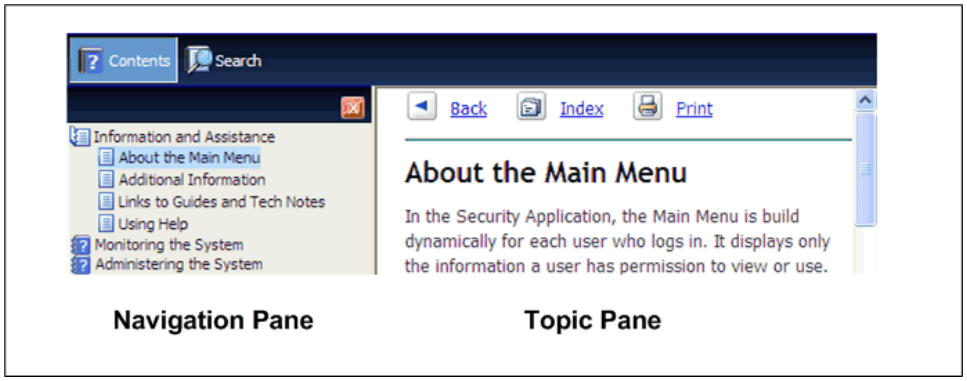
Introduction

This task guide is intended for users of the S2 Security Management System. It provides a printable version of the online help for common monitoring and administration tasks.

Note: Check the S2 Security web site (**www.s2sys.com**) for updated specifications, lists of supported devices, and software updates.

Getting Help

As you use the system, you can click the **Help** icon in the title bar to open the help window shown below. The information displayed in the topic pane provides assistance with the page you are currently viewing.



To use help:

- Click the **Contents** and **Search** buttons in the navigation pane to switch between the table of contents and the search feature.
- Click the close button to hide the navigation pane. To re-open the pane, click the **Contents** or **Search** button.
- In the table of contents, click a book to show or hide its topics. Click a topic to display it in the topic pane.
- To use the search feature, enter the text you want to find and then click **Go** or press **ENTER**. If the **Highlight search results** check box is selected, the text you entered will be highlighted in the search results.
- In the topic pane, click **Back** to return to the previous topic, click **Index** to display the help Index, and click **Print** to print the current help topic.

Monitoring Doors, Cameras, and System Resources

The **Monitor** menu contains options for viewing cameras, entering duty log entries, accessing live monitoring options, granting passback grace, viewing and unlocking portals, and selecting different partitions to monitor.

Choose this:	To do this:
Cameras	Monitor individual cameras.
Camera Views	Monitor multi-camera (quad) views.
Duty Log Entry	Enter duty log messages into the Activity Log.
Live Monitoring	See Live Monitoring Options.
Passback Grace	Grace an individual from an anti-passback violation on the person's next card access.
Portal Status	View a list of portals and their status, unlock a portal, and schedule a portal unlock.
Select Partition	If your system has multiple partitions, select a different partition to monitor.

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 set up 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 set up the home, tilt, pan, and zoom URLs, these controls will not appear.

 Click this to display VCR controls at the bottom of the camera widget. You can use these VCR controls to review recorded video

 Click this to display PTZ controls.

 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 ViconNet or Dedicated Micros DVR, 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, select a lower speed number from the camera speed drop-down, shown 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 (quad) view.

To move any camera in a multi-camera view:

1. Click in the pane displaying the camera view you want 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 want to see displayed. (This drop-down list automatically fills with the presets of the selected camera.)

You can also adjust the position of any camera using the icons listed 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 display the **Camera Preset** drop-down list.

From the **Camera Preset** drop-down list select the preset position you want to see displayed. (This drop-down list automatically fills with the presets of the selected camera).

 Click this to display VCR controls at the bottom of the camera widget. You can use these VCR controls to review recorded video

 Click this to display PTZ controls.

 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 ViconNet or a Dedicated Micros DVR, 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.

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 comment into the Activity Log:

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

Notes: You can view the comment in the Activity Log by clicking on the clipboard icon at the end of the **Duty log entry** line.

When you double click an Activity Log entry, a window appears in which you can append a duty log entry to that entry.

Live Monitoring Options

The **Monitor: Live Monitoring** menu contains options for viewing system activities and floorplans, and for initiating live monitoring sessions.

Choose this:	To do this:
Activity Log	View logs of recent system activity.
Floorplans	View the state of alarms and other system resources on a floorplan.
Monitoring Desktop	Use a familiar fixed display to view system information.
Widget Desktop	Use a custom real-time display to view system information.

Monitoring the Activity Log

Select **Monitor : Live Monitoring : Activity Log**.

Note: You can also view the activity log on the Monitoring Desktop and in the Activity Log widget on the Widget 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.

Descriptions of the message text and variables included in log messages follow.

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.

Navigating to a Person Record from the Activity Log

If you have the right to view a cardholder's person record, clicking that person's name within an Activity Log entry opens a window in which his or her person record is displayed. Any rights you have to view and edit information in a particular person record will apply when you access the record from the Activity Log.

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>**

Monitoring Floorplans

Select **Monitor : Live Monitoring : 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.
- Set up and perform scheduled or momentary portal unlocks.
- Set up and perform scheduled arming or disarming of inputs.
- Set up 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 floorplans:

1. Select from the **Floorplan** drop-down the floor you want 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.

Using the Monitoring Desktop

Select **Monitor : Live Monitoring : Monitoring Desktop**.

The Monitoring Desktop provides a fixed layout for viewing dynamic system information. It has separate tabbed pages for monitoring various system functions, such as events, camera views, and floorplans.

To use a fixed display to monitor all system activities:

1. In the upper left pane, click either the **Events** or **Activity Log** tab, depending on the type of system information you want to view in that pane.

   Note: The **Events** tab displays all currently active system events. Events can be sorted on the **Date/Time**, **Priority**, **Name**, or **Commands** column.

2. In the lower left pane, click the **Activity Log**, **Cameras**, **Camera Views**, **Camera Monitor**, **Floorplans**, or **Events** tab, depending on the type of information you want to view in that pane.
3. Use the windows on the right side of the desktop to view the current threat level, unlock portals, view cameras, and view a recent history of cardholders who have presented their access cards to readers in the system.

Activity Log Tab

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

Cameras Tab

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

Camera Views Tab

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

Camera Monitor Tab

You can select from the camera widgets on the right the specific camera you want to have displayed in the monitor tab. You can select IP cameras or DVR cameras.

 This icon will change to this icon  when you mouse over it. Click it and the Camera Monitor tab will display with the video stream or images from that camera widget.

Note: The small camera widgets on the Monitoring Desktop will, by default, display the first two cameras in the **Setup : Camera : Menu Order** page.

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

 Click this to display VCR controls at the bottom of the camera widget. You can use these VCR controls to review recorded video.

NOTE: If the camera does not have these capabilities these controls will not appear.

 Click this to display PTZ controls.

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 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, shown 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.

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.

Events Tab

By default events are sorted in priority order. To reverse the sort order, click the arrow next to the **Priority** column title. You can also click the arrows next to the **Date/Time**, **Name**, **and Commands** column titles to sort events by those columns.

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

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 and respond to alarm events:

1. Select **Monitor : Monitoring Desktop**.
2. Click icons on the page to execute the following actions:

    Click the camera icon to display the video for this event.

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

    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

Using the Widget Desktop

Select **Monitor : Live Monitoring : Widget Desktop**.

The Widget Desktop provides a custom real-time display for monitoring the system. When you open the Widget Desktop, you see one or more windows, called *widgets*, arranged in the default layout for your system. Each widget has a special function, such as displaying system activity, unlocking portals, or delivering real-time web content from another system.

Note: Internet Explorer 7 or higher is required for optimal viewing of the Widget Desktop. Page display problems occur when the Widget Desktop is viewed in other browsers or other versions of Internet Explorer.

If the default Widget Desktop layout does not meet your needs, you can select a different layout if others are available. You can also customize a layout for the current monitoring session, by adding available widgets and selecting a different background.

You may also be able to change the individual widgets in a layout, depending on how it was set up. For example, you may be able to:

- Move, size, minimize, and close a widget.
- Change a widget's unique properties.
- Change the scope of the data displayed in a widget.

Note: Changes you make to a layout are not saved across monitoring sessions. Once you close the Widget Desktop, the layout reverts to its original appearance.

To display the default Widget Desktop layout:

- Select **Monitor : Live Monitoring : Widget Desktop**. The default Widget Desktop layout appears automatically.

To select a different layout:

1. Select **Load Layout** from the Desktop menu in the lower left corner of the page.
2. In the Load Layout dialog box, select the layout you want, and then click **OK**.
3. To return to the default layout at any time, select **Default** from the Load Layout dialog box.

To add a widget to the selected layout:

- Select the widget from the Desktop menu in the lower left corner of the page.

To select a different partition to monitor:

1. Click the name of the active partition on the lower right edge of the page.
2. In the Switch Partition dialog box, select the partition you want to monitor.
3. Click **OK**.

   The partition you selected becomes the active partition until you select a different one.

To change the Widget Desktop background:

- Right-click anywhere on the background, select a number from the Background drop-down, and then click **OK**.

To get Help from the Widget Desktop:

- Click the information icon  in the lower right corner of the page.

To exit the Widget Desktop:

- Select Exit from the Desktop menu in the lower left corner of the page to return to the main menu.

Granting Passback Grace to Cardholders

Select **Monitor : Passback Grace**.

On this page, system users with at least an Administration user role can grant passback grace to cardholders. When a cardholder is "graced," the person's next card read is allowed, no violations are triggered, and the person is moved to the region specified by the Auto-passback Grace to Region setting on the Network Controller page. Thereafter, all anti-passback rules are in effect, as before.

Note: A system user with only a Monitor user role can also grace cardholders, if both of following settings are selected on the Network Controller page: **The monitoring role can grant passback grace** and **Show Region and Passback Grace info in the Roster and People reports**.

To grant passback grace to cardholders:

1. In the search form, select the region in which you want to search, and enter sufficient additional data to find the people you want to grace.
2. Click **Search**.

   A report containing the search results is displayed below the form. The report shows each person's name and current location.
3. To grace an individual cardholder, click the **Grace** button for that person. To grace all cardholders listed in the report, click the **Grace all shown** button.

Note: A **Grace pending** button appears for any cardholder who does not require passback grace—such as a person who was just added to the system and is still in the Uncontrolled Space region.

Unlocking Doors (Portals)

There are three ways to unlock a door. You can:

- Perform an immediate momentary unlock.
- Schedule an unlock action at a specific time.
- Create a portal group and assign an unlock time specification for a regular unlock schedule.

To perform an immediate momentary unlock:

1. Select **Monitor : Portal Status**.
2. In the Portal column find the portal that you want to unlock.

3. Click the Unlock link in the Action column. The portal will unlock for the unlock time setup with the portal.

To schedule an unlock action at a specific time:

1. Select **Administration : Schedule Action**.
2. In the **Name** column, find the door you want to unlock and click the Schedule link next to it in the **Action** column. A pop-up window will appear.
3. From the **Action** drop-down select **Unlock**.
4. In the **Start Date/Time** column click the **At** button and enter in the text box above it the date and time for the door to unlock.
5. In the **End Date/Time** column click the **At** button and enter in the text box above it the date and time for the door to relock.
6. Click **Save**.

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 want to use for a regular unlock time schedule.
4. Click **Save**.

Selecting Partitions

Select **Monitor : Select Partition**.

If your system is partitioned for monitoring multiple populations and/or resources separately, you can select a different partition to:

- Monitor the other partition's activity.
- Perform administrative functions within the other partition.
- Set up and configure resources within the other partition.

To select a different partition:

1. Select the partition in which you want to work.
2. Click **Save**.

Note: You will need an appropriate user role in a partition before you will see its resources and activity.

Managing People Data

You can use options on the **Administration : People** menu to enter and change information about system users.

Choose this:	To do this:
Add	Add a person to the system.
Change/delete	Edit or delete the information currently in the system for a person.

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:

1. In the text boxes enter a **Last Name** and **First Name**.
2. The **Activation Date/Time** defaults to today but you can change it.
3. For this record to be temporary, you must enter an **Expiration Date/Tim**e. 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.

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 an individual's record:

1. Search for person records by using any of the available fields.
   - 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 want to also see deleted records, select the **include deleted records** box.
3. If you want to see expired records, select the **include expired records** box.
4. Click the **Search** button.
5. 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 want to edit.
6. Make any needed changes on the full Personal Information page.
7. Click **Save**.

About the Personal Information Detail Page

Once you select the person whose personal information you want to change or delete, the **Change** page appears. The information you can change for the person is described below.

To make changes in the 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 want the person's access to expire automatically at a particular date and time.

Note: The activation date can be more recent than the expiration date. This might 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.

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.

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.

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.

- The **License #** field is for the state issued license plate number.
- 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 in the system.

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 higher there are four levels of user roles for security application users. From lowest to highest they are:

- **Monitor**. Users with this role may only use the functions available on the Monitor menu.
- **Administer**. Users with this role may use the functions on both the Administration and Monitor menus.
- **Setup**. Users with this role may use the functions of the Setup, Administration, and Monitor menus.
- **Custom User Roles**. In addition to the roles above, users with setup privileges can 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.

Recent Activity Tab

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

Partitions Tab

The Partitions tab is available only if the system has multiple partitions. It lists other partitions in which you have at least administrator privilege or that have been made visible to you by their administrators.

By selecting a partition from the **Partition** drop-down list, you can give administrators in that partition limited access to the currently selected person record in the active partition.

The administrators will then be able to search for the person, open his or her person record, and add or remove any of the access levels defined in their own partitions. The administrators will not be able to edit any other information on the page, such as the person's contact and login information.

For example, suppose that Thomas, an employee whose person record is in the Home Office partition, is about to begin a three-month assignment in a remote office. As the administrator of the Home Office partition, you can give Megan, the Remote Office partition's administrator, limited access to Thomas's person record for that period.

Megan will then be able to give Thomas any access levels he will need to enter and navigate the remote facility. Once Thomas's temporary assignment is completed, Megan can remove her partition's access levels from Thomas's person record.

Issuing Access Cards to Employees

Before an access card can be issued, the employee name and activation date must 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 available fields.
   - 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** and a **Department** name, and then click **Search**. A list of all people whose last names begin with the letter you entered AND whose department name matches the one you entered, 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 to display the **Issue Card** pop-up window.

6. Check the **Reader** drop-down to ensure that the enrollment reader you are using is selected, and then click the **Go** button.
7. Swipe or pass the card by the reader.

   The electronically encoded number in the card appears 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.

---

8. Click **Save**.

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 want 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 want to disable the card of a person who has forgotten his or her card and for whom you are issuing a temporary card. When the temporary card is returned the person's card can be re-enabled by clicking to uncheck the **Disabled** checkbox.

To add access levels to a person:

1. Click 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, select the **Use Extended Unlock** box. (This is the ADA setting)
5. Click **Save**.

Important: 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 from a person:

1. Click 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**.

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 want 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.

   This card will immediately be removed from the system and will not function.

Changing a Password

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

Passwords are needed only by users who are allowed to log in to the 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 a password:

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

   The new password takes effect immediately.

Notes: If the new password is identical to the current password, you will see an error message. The new password must be different from the current password.

If you re-enter the 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 marks (“ ‘) .

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.

Handling Lost Cards

Select **Administration : Lost Cards**.

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

To determine the identity of a cardholder:

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 to display a small reader window.
3. Select a reader from the **Reader** drop-down list and swipe the card through that reader.

   The card number fills the **Hot stamp #** text box.
4. Click the **Search** button.

Issuing Temporary Access Cards

Select **Administration : People : Add**.

Before you can issue a card to a person, he or she must 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 will also expire.

To issue a temporary card:

1. Select **Administration : People : Add**.
2. In the text boxes enter the **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**.

Creating and Printing Photo IDs

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.

To capture ID photos and save 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 30K.

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 want to use.
5. Click the **Photo ID** button and the **Photo IDs** pop-up window appears.
6. **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.
7. In the **Photo ID** window, click **Capture Image**, and the **Select Image Source** window appears.
8. Select **Microsoft WDM Image Capture (Win32)** and click **OK**. The **Capture** window and the Logitech QuickCam application bar appear.
9. Ensure that the person is properly within the picture frame and 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 30K.

10. If the picture is acceptable click **OK**. If not, click the continue button  and recapture the photo.
11. 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**.
12. The captured image appears on the **Personal Information** page. Click the **Close** button in the **Photo IDs** window.
13. 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.

To print a photo ID badge at your workstation:

The photo ID printer must be connected to your workstation with a USB cable. See the manufacturer documentation for guidance on hardware setup.

The printer's Windows driver listed above must be installed on your workstation. See the manufacturer documentation for guidance on software and driver installation.

1. On the **Personal Information** page, click the **Photo ID** tab.
2. From the drop-down in the **Badge** box, select the layout you want to use.
3. Click **Photo ID**. A small photo ID window appears.
4. In the photo ID window, click **Print Photo ID**. The **Print** dialog box appears.
5. From the **Name** drop-down list, select the photo ID printer, and click **OK**. Retrieve the badge from the printer tray.
6. In the photo ID window, click **Close**.
7. On the **Personal Information** page, be sure to click **Save**. This saves the captured image and selected badge design with the person's record.

Note: 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** and verify that this report lists your request.

Note: Any badge printing requests in the queue can be printed as described in the following procedure.

To print requested photo ID badges:

The printer must be connected to your workstation with a USB cable. See the manufacturer documentation for guidance on hardware setup.

The printer's Windows driver listed above must be installed on your workstation. See the manufacturer documentation for guidance on software and driver installation.

1. Select **Administration : Reports : People : Request Photo ID Report**. This report lists all currently outstanding photo ID print requests.
2. Click the printer icon in the **Action** column (the rightmost column) for the badge you want to print. A small photo ID window appears.
3. In the photo ID window, click **Print Photo ID**. The **Print** dialog box appears.
4. From the **Name** drop-down list, select the photo ID printer, and click **OK**. Retrieve the badge from the printer tray.
5. In the photo ID window, click **Close**.

Deleting Photo ID Layouts

Select **Administration : Utilities : Badge Layout Delete**.

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

To delete a badge layout:

1. Select the check box to the right of each of the badge layouts you want to delete,
2. Click **Delete File(s)**.

Uploading Photo ID Layouts

Select **Administration : Utilities : 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."

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**.

Creating Reports from System Data

The **Administration : Reports** menu provides a variety of system information reports.

Choose this:	To do 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**.

As Built

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.

Cameras Report

The Cameras report displays all camera configuration information.

Camera Presets Report

The Camera Presets report displays configured presets for each camera in the system. These presets must be set at each camera web site.

Elevators Report

The Elevators report displays elevator configuration information including Node, Reader, and Floor to output mappings.

Floor Groups Report

The Floor Groups report displays all configured floor groups for use in elevator control.

Holidays Report

The Holidays report displays holiday specification information.

Portals Report

The Portals report displays portal definition information.

Portal Groups Report

The Portal Groups report displays all portal groups, the portals included in each, and the assigned threat level group.

Reader Groups Report

The Reader Groups report displays defined groups of readers.

Resources Report

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

Threat Level Groups Report

The Threat Level Groups report displays all configured threat level groups and the threat levels assigned to them.

Threat Levels Report

The Threat Levels report displays all configured threat levels including the description and color assignment.

History Reports

Reports on the **Administration : Reports : History** menu let you retrieve data from archives when the requested report data is no longer active on the controller board. In version 3.2 and above 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.
CSV Export Report	Exports events from the Activity Log as a comma-separated values (CSV) file.
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.

Access History Report

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 want to limit the report to a specific person.
3. To limit the report to specific dates:
4. 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.

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

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 custom history reports:

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**.

CSV Export Report

Select **Administration : Reports : History : CSV Export**.

With this page you can export a report containing events from the Activity Log as a comma-separated values (CSV) file. The CSV file contains the following information for each event:

- Partition (if the **Include activity from all partitions** check box is selected)
- Person ID
- Node Date/time
- Date/time
- Description
- Last Name
- First Name
- Node UID
- Node Name
- Location
- Reader
- Card Number

To create a CSV Export report:

1. Select **Administration : Reports : History : CSV Export**.
2. Click the **From (date)** calendar icon and select the start date for the report.
3. Click the **Thru (date)** calendar icon and select the end date for the report.

4. Select the **Include activity from all partitions** check box if you want the report to include data from all partitions, rather than from the selected partition only.

   This option is available only if you are in the Master partition and you have the full system setup user role. If the check box is selected, the report data will include a Partition column showing the partition in which each event occurred.

5. Click **Export**.

6. In the File Download dialog box, click **Open** to open the CSV file or click **Save** to save it.

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 want 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.

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," 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**.

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.

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**.

Current Users Report

The Current Users report displays a list of all security system users currently logged in to the security system website.

Occupancy Report

The Occupancy report displays a list of defined Regions. For each region, it shows the number of people currently occupying the region and the maximum number of occupants allowed, if a maximum has been specified.

Photo ID Gallery

The Photo ID Gallery report 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

The Photo ID Request 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

The Portals Access report displays the names and access levels of everyone allowed access at the portal you select from the **Portals** drop-down.

Roll Call Report

The Roll Call Report lets you select a defined Region from the drop-down and see a list of people currently in that region.

Roster Report

The 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

The 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. As an example, 900 is 9:00 AM and 1700 is 5:00 PM.

Holidays are listed in groups as they were entered.

Backup System 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 want.

To back up system data:

1. Select **Administration : Utilities : 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, and so forth.

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, and so forth.

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**.

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 and disarm an alarm panel:

1. Select **Administration : Arm Alarm Panel**.

   The page displays a table listing all alarm panels configured in the system, their current states, 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.

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. In the left column, select the threat level to which you want to set the system.

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**.