ReadykeyPRO Unlimited

Combining people and technology

BOSCH

Alarm Monitoring User Guide

Readykey*PRO Unlimited,* Version 6.5

Bosch ReadykeyPRO® Unlimited Alarm Monitoring User Guide, product version 6.5
This guide is part 1 of a 2-document suite, item number DOC-201-01-2-026, revision 2.026, April 2012.

Table of Contents

Introduction

Chapter 1: Introduction

The Alarm Monitoring application displays information about individual alarms and events as they occur. Operators can acknowledge alarms and manually change the status of devices as well as monitor video and launch Guard Tours.

With the correct permissions, Operators can also perform a variety of administrative tasks such as adding, modifying, deleting and tracking cardholders, visitors and assets as well as print badges.

Conventions Used in this Documentation

- Where a term is defined, the word is represented in *italics*.
- Field names, menus and menu choices are shown in **bold**.
- Keyboard keys are represented in angle brackets. For example: <Tab>.
- Keyboard key combinations are written in two ways:

  <Ctrl> + <Z> means hold down the first key and press the second

  <Alt>, <C> means press the first key, then press the second
- Window buttons on the screen are represented in square brackets. For example: [OK].

How this Document is Organized

The Alarm Monitoring User Guide is divided into three sections: the System Administrator Procedures section, the Operators section and the Advanced Operator Procedures section.

The System Administrator section outlines the steps involved in setting up an Alarm Monitoring station. Most of the procedures in these chapters reference other manuals because they cannot be performed in the Alarm Monitoring application.

The Operator Procedures section focuses on procedures to monitor alarms, monitor video, trace devices and execute commands.

The Advanced Operator Procedures section covers the administrative procedures operators can perform in Alarm Monitoring. For example, adding cardholders or visitors, printing badges, adding assets to the database and assigning assets to cardholders.

Note: Depending on the workflow of your company, some of the procedures covered in this section may be considered System Administrator procedures.

Getting Started

Passwords

ReadykeyPRO®includes strong password enforcement, which checks the user's password against password standards. This functionality is designed to enhance password security if single sign-on is not used. If single sign-on is used (automatic or manual), ReadykeyPRO does not enforce password standards. For more information on single sign-on, refer to Single Sign-On on page 31.

The system's strong password enforcement also checks the Bosch database user's password when logging into applications. Database user passwords apply only to SQL databases. For information on changing your database password, refer to the Accounts and Passwords chapter in the Installation Guide.

Password Standards

When creating a strong password keep the following guidelines in mind:

- Passwords cannot be blank.
- Passwords cannot be the same as the user name (e.g. SA, SA).
- Passwords cannot be Bosch keywords.
- Although not required, your password should contain numbers, letters, and symbols. Spaces are also acceptable. (e.g. August 18, 2002).
- ReadykeyPRO user passwords are *not* case-sensitive.
- Database passwords conform to the rules of the specific database being used; passwords in SQL Server are case sensitive.
- The maximum value for a strong password is 127 characters. The minimum value is 1.

Enable/Disable Strong Password Enforcement

Strong password enforcement is enabled/disabled in System Administration or ID CredentialCenter. When you install ReadykeyPRO, by default strong password enforcement is enabled. When you upgrade, by default strong password enforcement is disabled. To manually enable or disable strong password enforcement:

1. Select **System Options** from the **Administration** menu.
2. Select the General System Options tab.
3. Click [Modify].
4. Select or deselect the **Enforce strong passwords** checkbox.

Note: If you disable the option to enforce strong passwords, you will continue to receive a message stating your password is weak every time you log into an application until you change your ReadykeyPRO password to meet the password standards.

5. Click [OK].

Error Messages

Read weak password messages/warnings carefully to avoid confusion about whether your user password or database password is weak.

If you have a weak database password you will receive a warning every time you log into any application, until you change your database password. Although it is not recommended, you can acknowledge the warning and continue working in the application. This table describes the password-related error messages that may be generated and which password you need to correct.

- To correct the database password, refer to the Accounts and Passwords chapter in the Installation Guide.
- To correct the user password, select a password that meets the standards specified in Password Standards on page 28.

Warning message	Password to correct
Database password violations: Your password is a keyword that is not allowed. It is highly recommended that you change your password to meet our minimum password standards.	Database
Your password cannot be blank. Please enter a password.	User
User password violations: Passwords cannot be the same as the user name.	User
Your password is a keyword that is not allowed.	User

Accounts

Anyone who wishes to use ReadykeyPRO applications must enter a user name and password in order to access the software. The System Administrator should create a unique account for each user of the applications. The System Administrator can also, for each user, create a list of *permissions*, which specifies precisely which screens, fields, and buttons the user can access.

During initial installation of the application, default accounts are created. These include:

User name	Password	Type
sa	sa	system account
admin		sample
user		sample
badge		sample

These are provided as samples. You may change the passwords and use the accounts, or remove them. The exception to this is the system account, SA. By definition this account has permission to do anything in the system. A user with system access has unlimited access to the application. You cannot delete or change the system account except to modify the password, which you are strongly encouraged to do as soon as possible to discourage unauthorized use.

The first time you log into ReadykeyPRO to configure the application, you should log in as **SA** and your password should be **SA**.

Log In

This procedure describes how to log in without using single sign-on. For a description of single sign-on, refer to Single Sign-On on page 31. To log in using single sign-on, refer to Configure Single Sign-On on page 33.

1. Click the Start button, select **Programs** > **ReadykeyPRO Unlimited**, and then select the desired application.
2. Your system may be configured to prompt you to select a database to log into. If it is not, proceed to the next step. If it is:
   a. In the **Database** drop-down, all ODBC system databases currently defined on your computer are listed. Select the database that you wish to use for your application.
   b. Click [OK].
3. The Log On window displays.
   a. In the **User name** field, type the user name assigned to you. When logging in for the first time, your user name is **SA**.
   b. In the **Password** field, type the password assigned to you. When logging in for the first time, your password is **SA**. Note that the characters you type do not appear in the field. Instead, for each character you type, an “*” displays. This is intended to protect against unauthorized access in the event that someone else can see the screen while you type.

Important: After logging in for the first time, you are strongly encouraged to modify the password for the system account as soon as possible to discourage unauthorized use.

   c. In the **Directory** field, select the directory that you wish to log into. For user accounts not using single sign-on, the default is “<Internal>.”
   d. Select the **Remember user name and directory** checkbox if you want the values you just entered in the **User name** and **Directory** fields to automatically be selected the next time that you log in.
   e. Click [OK].
4. Your system may be configured to prompt you to confirm that you are authorized to use the application. To accept the terms of the authorization warning click [Yes].
5. If you are prompted to select a monitor zone:
   a. Select a monitor zone from the drop-down list. If segmentation is enabled, only the monitor zones for the segment that you logged into are available.

b. Select the **Save as monitoring station assignment** checkbox if you wish to make the monitor zone selection the default assignment for the monitoring station. This means when any operator logs into Alarm Monitoring at this workstation, this zone will be monitored unless the operator has monitoring zones assigned to them as a user or the operator has permission to view multiple zones. This checkbox is only enabled if the user has proper permissions.

c. Select the **Save as user assignment** checkbox if you want to log onto the same monitor zone EVERY time you log in. This is a persistant assignment. You will not be prompted to select a monitor zone during future log ins. This checkbox is only enabled if the user has permission. To restore the prompt to select a monitor zone, simply remove the selection from the User's Monitor Zone Assignment using System Administration.

d. Click [OK].

Notes: Monitor zone user assignments take precedence over monitoring station user assignments.

For more information, refer to the Monitor Zones Folder chapter in the System Administration User Guide.

6. If you are prompted that the monitoring station you are logging into is set up for event queuing:

   a. Select **No**, if you want all the queued events deleted.

   b. Select **Yes**, if you want all queued event for the monitor zone displayed.

Single Sign-On

Single sign-on simply means logging into ReadykeyPRO with the same user name and password that you use to log into Windows or logging into ReadykeyPRO using an LDAP user name and password for authentication. *LDAP* (Lightweight Directory Access Protocol) is a software protocol that enables you to locate businesses, people, files, and devices without knowing the domain name (network address).

Single sign-on allows scripts using the DataConduIT API to authenticate. These scripts will be run under a Windows account. The account that is making the call to the API can be obtained easily this way, and the script can be restricted to those actions that the user is permitted to perform (using standard ReadykeyPRO permissions).

Note: The use of the explicit username and password for directory authentication to Windows is strongly discouraged. It is recommended that you do not store Windows passwords in the ReadykeyPRO system, since ReadykeyPRO uses reversible encryption and Windows does not. If explicit authentication is required, you should use an account that has view only permission to the directory in question.

It is possible to assign both an internal account and one or more directory accounts to a single user. Assigning both types of accounts increases the flexibility of the system during the authentication process. If the directory service is down or cannot be found from the workstation where the user is logging on, that user can instead use the internal account. Using both types of accounts means that you need to manage the internal account user names and passwords in addition to managing the directory accounts.

Important: Allowing a user to log on in multiple ways increases the probability that the user's access to the system could be compromised. It is recommended that you standardize on either internal or directory accounts, but not both.

There are cases where assigning both an internal account and a directory account to a user may make sense. In a system where directory accounts are predominantly used, you may also assign an internal account to a user who needs to access the system from locations where the directory service is unavailable. If internal accounts are predominantly used, you may want to assign a directory account to a user so that the user does not need to enter in a password to log on.

Directory Accounts

To log into ReadykeyPRO using single sign-on, a user name, password, and directory are required. A *directory* is a database of network resources, such as printers, software applications, databases, and users. The following directories are supported by ReadykeyPRO: Microsoft Active Directory, Microsoft Windows NT 4 Domain, Microsoft Windows Local Accounts, and LDAP.

Automatic and Manual Single Sign-On

When a user account is configured for single sign-on, the user can log into ReadykeyPRO automatically or manually.

For example, with automatic single sign-on, users simply start ReadykeyPRO and they are automatically logged in under their Windows account and directory.

With manual single sign-on, users must manually enter their Windows or LDAP account information (user name and password). Users also have the option of selecting a different configured directory.

If single sign-on is not used, users manually enter a user name and a password that is different from their Windows or LDAP password. The directory is hard-coded to refer to the internal ReadykeyPRO user directory.

Notes: *Manual* single sign-on can be used with the following directories: Microsoft Active Directory, Microsoft Windows NT 4 Domain, and LDAP.

Automatic single sign-on can be used with every directory supported by ReadykeyPRO *except* LDAP because it doesn’t provide all the account information required.

Configure Single Sign-On

By default, user accounts do **not** use sign-on. To configure single sign-on the System Administrator must add a directory and link a user account to the directory.

Log In Using Automatic Single Sign-On

Automatic single sign-on is supported with Windows domain accounts.

1. Click the Start button, select **Programs** > **ReadykeyPRO Unlimited**, and then select the desired application.
2. Your system may be configured to prompt you to select a database to log into. If it is not, proceed to step 3. If it is:
   a. In the **Database** drop-down, all ODBC system databases currently defined on your computer are listed. Select the database that you wish to use for your application.
   b. Click [OK].
3. If your Windows account is linked to a user, a message will be displayed that says, “Attempting to automatically log you on using your Windows account. To bypass this, hold down SHIFT.” To automatically be logged in, do nothing.
4. Your system may be configured to prompt you to confirm that you are authorized to use the application. To accept the terms of the authorization warning, click [Yes].
5. If you are prompted to select a monitor zone:
   a. Select a monitor zone from the drop-down list. If segmentation is enabled, only the monitor zones for the segment that you logged into are available.
   b. Select the **Save as monitoring station assignment** checkbox if you wish to make the monitor zone selection the default assignment for the monitoring station. This means when any operator logs into Alarm Monitoring at this workstation, this zone will be monitored unless the operator has monitoring zones assigned to them as a user or the operator has permission to view multiple zones. This checkbox is only enabled if the user has proper permissions.
   c. Select the **Save as user assignment** checkbox if you want to log onto the same monitor zone EVERY time you log in. This is a persistant assignment. You will not be prompted to select a monitor zone during future log ins. This checkbox is only enabled if the user has permission.

To restore the prompt to select a monitor zone, simply remove the selection from the User's Monitor Zone Assignment using System Administration.

d. Click [OK].

Notes: Monitor zone user assignments take precedence over monitoring station user assignments.

For more information, refer to the Monitor Zones Folder chapter in the System Administration User Guide.

6. If you are prompted that the monitoring station you are logging into is set up for event queuing:
   a. Select **No**, if you want all the queued events deleted.
   b. Select **Yes**, if you want all queued event for the monitor zone displayed.

Log In Using Manual Single Sign-On

Both users who want to log into ReadykeyPRO using an LDAP user name and password for authentication and users who want to log in using a Windows domain account can do so using manual single sign-on.

1. Click the Start button, then select **Programs** > **ReadykeyPRO Unlimited**, and then select the desired application.
2. Your system may be configured to prompt you to select a database to log into. If it is not, proceed to step 3. If it is:
   a. In the **Database** drop-down, all ODBC system databases currently defined on your computer are listed. Select the database that you wish to use for your application.
   b. Click [OK].
3. If your Windows account is linked to a user, a message will be displayed that says, “Attempting to automatically log you on using your Windows account. To bypass this, hold down SHIFT.”
   To manually login or to login using a different user name and password, hold down the <Shift> key. The Log On window opens.
   a. In the **Directory** field, select the directory that you wish to log into. The default is “<Internal>.”
   b. In the **User name** field, type the Windows user name assigned to you. Do not enter the domain\user name just enter your user name.
   c. In the **Password** field, type the Windows password assigned to you.
   d. Select the **Remember user name and directory** checkbox if you want the values you just entered in the **User name** and **Directory** fields to automatically be selected the next time that you log in.
   e. Click [OK].
4. Your system may be configured to prompt you to confirm that you are authorized to use the application. To accept the terms of the authorization warning, click [Yes].

5. If you are prompted to select a monitor zone:
   a. Select a monitor zone from the drop-down list. If segmentation is enabled, only the monitor zones for the segment that you logged into are available.
   b. Select the **Save as monitoring station assignment** checkbox if you wish to make the monitor zone selection the default assignment for the monitoring station. This means when any operator logs into Alarm Monitoring at this workstation, this zone will be monitored unless the operator has monitoring zones assigned to them as a user or the operator has permission to view multiple zones. This checkbox is only enabled if the user has proper permissions.
   c. Select the **Save as user assignment** checkbox if you want to log onto the same monitor zone EVERY time you log in. This is a persistant assignment. You will not be prompted to select a monitor zone during future log ins. This checkbox is only enabled if the user has permission. To restore the prompt to select a monitor zone, simply remove the selection from the User's Monitor Zone Assignment using System Administration.
   d. Click [OK].

Notes: Monitor zone user assignments take precedence over monitoring station user assignments.

For more information, refer to the Monitor Zones Folder chapter in the System Administration User Guide.

6. If you are prompted that the monitoring station you are logging into is set up for event queuing:
   a. Select **No**, if you want all the queued events deleted.
   b. Select **Yes**, if you want all queued event for the monitor zone displayed.

Troubleshoot Logging In

If you attempted to log in and were unable to do so, make sure that the following conditions have been met:

- You entered a correct user name/password and specified the correct directory.
- If your system is configured to display an authorization warning, you accepted the terms.
- A valid license is installed.
- You have permission to use the application.
- If you attempted to log in and were unable to do so, make sure the following conditions have been met:
  – You entered the correct user name and password for the selected directory of a user with permission to use the application.

- If the system is configured to display an authorization warning, then you accepted the terms.
- Verify your acs.ini file has the correct LicenseServer Host and Port settings. The LS License Server service must be started on the specified Host.
- Log into the License Administration application to verify a valid license is installed.
- Software based licenses must be activated.
- USB and Parallel licenses must have License Key Drivers installed.
- If using single sign-on, ensure the pc user you are logged in as is linked to an internal ReadykeyPRO user through an operational directory.

Assigning Directory and Internal Accounts to the User

It is possible to assign both an internal account and one or more directory accounts to a single user. Assigning both types of accounts increases the flexibility of the system during the authentication process. Meaning, if the directory service is down or cannot be found from the workstation where the user is logging on, then the user can use the internal account instead.

However, using both types of accounts means that you need to manage the internal account user names and passwords in addition to managing the directory accounts. Allowing a user to log on in multiple ways increases the probability that the user's access could be compromised. For that reason, it is recommended that you standardize on either internal or directory accounts, but not both.

There are cases where assigning both an internal account and a directory account to a user may make sense. In a system where directory accounts are predominantly used, you may also assign an internal account to a user who needs to access the system from locations where the directory service is unavailable. If internal accounts are predominantly used, you may want to assign a directory account to a user for that user's convenience, so that the user does not need to enter in a password to log on.

Switch Log On

Switch Log On is often used when multiple operators use the same Alarm Monitoring station. Instead of logging out of the application operators can use the switch log on feature. This simultaneously logs out the previous operator and logs in the new operator.

1. Select **Switch Log On** from the **File** menu.
2. The Log On to Alarm Monitoring window displays.
3. Enter the user name and password.
4. Select the desired directory.
5. Click [OK].

Notes: When using switch log on, the person who’s logged into Windows can be a different person than the one logged into Alarm Monitoring.

Switch log on cannot be used if the new user has a monitor zone/user assignment different from the current user.

Log Out of the Application

When you log out of the application the entire application closes.

1. Select **Log Off** from the **File** menu.
2. The current user is logged off but the application remains open.

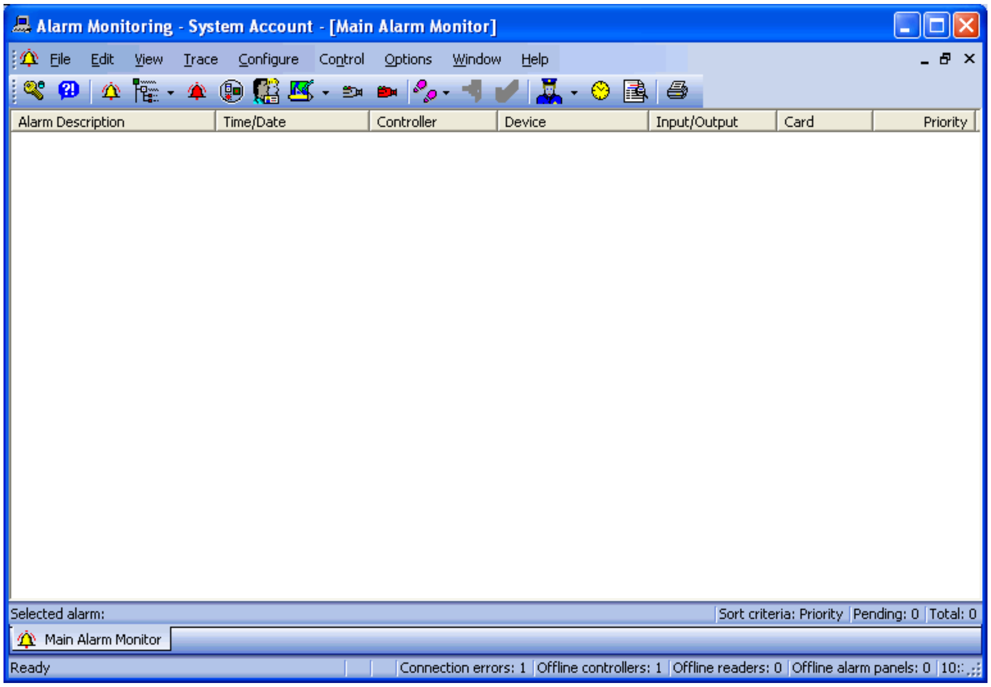
Exit the Application

You can close and exit the application using the following methods:

- Select **Exit** from the **File** menu.
- Double-click the icon located in the upper left corner of the title bar. When prompted to log off, click [Yes].
- Single click the icon located in the upper left corner of the title bar and select Close. When prompted to log off, click [Yes].
- Click the close button in the window’s upper right corner. When prompted to log off, click [Yes].

Chapter 2: Main Alarm Monitoring Window

The Main Alarm Monitoring window displays automatically when you log into the application. You can open and close additional windows but the Main Alarm Monitoring window remains open until you log out of the entire application.



Selected alarm: | Sort criteria: Priority | Pending: 0 | Total: 0

Connection errors: 1 | Offline controllers: 1 | Offline readers: 0 | Offline alarm panels: 0 | 10:

Note: You can toggle the display mode of the additional windows between standard and floating behavior that allows you to position the additional windows outside the main Alarm Monitoring window. For more information, refer to Toggle Window Display Modes on page 68.

Menus and Toolbars

The menu bar is a horizontal list of options that appears at the top of the main window. Scroll over each option to view a drop-down menu. A toolbar is a strip of buttons positioned by default just below the menu bar. If you place your cursor over a toolbar button, a tool tip identifies the name of the toolbar button.

Operators can customize how the toolbar displays; they can:

- Change the toolbar from anchored to floating

  Toolbars are anchored by default and are displayed in horizontal rows below the menu bar. Anchored toolbars can be changed to floating toolbars, which allows the toolbar to be repositioned anywhere in the window. For more information, refer to How to Use the Toolbars on page 52.

- Control if the toolbar is displayed

  By default the toolbar is displayed. Operators can control if the toolbar is displayed by selecting or deselecting **Toolbar** from the **View** menu. For more information, refer to How to Use the Toolbars on page 52.

File menu

Menu option	Toolbar button	Function
Print	🖨	Prints information displayed in the active (topmost) window. The print toolbar button does not display if the Main Alarm Monitoring window is minimized.
Log On/Log Off	🔑	Logs you into or out of the application.
Switch Log On		Displays the login window, allowing a different user to log in without the previous user manually exiting the application. When the new user is successfully logged in, the old user is simultaneously logged out.
Change Password		Opens the Change Password dialog, enabling you to change your password (you must have the corresponding system level permission to do so).
Exit		Ends the session of every person logged on.

Edit menu

Menu option	Toolbar button	Function
Note: The following menu options are active when an alarm window is displayed.		
Acknowledge		Acknowledges the currently selected alarm.
Fast/Group Acknowledge	✓	Allows a user to acknowledge a group of alarms simultaneously.
Delete		Removes the selected alarm from the window.
Delete All		Removes all alarms from the window.
Select All		Selects all alarms in the window.

View menu

Menu option	Toolbar button	Function
Badge Info	🪪	Displays the cardholder folder/window which contains nine forms/tabs: Cardholder, Badge, Access Level, Biometrics, Visits, Assets, Directory Accounts, Guard Tours and Reports. **Note:** When the cardholder folder/window displays, an additional menu option, **Cardholder** displays. For more information, refer to Cardholder menu on page 50.

View menu (Continued)

Menu option	Toolbar button	Function
Visits		Displays the Visits folder/window which contains the Status search, Visit, Details, Email and Reports forms/tabs. From the Visits folder/window you can: • search visit records based on scheduled time in or out and date and time the record was last changed • display visit records for a selected date range • add, modify or delete • print disposable badges • sign in or out a visit • send e-mail notifications • generate reports
Asset Info		Displays the Asset folder/window which contains the Assets, Assets Classes and Assignments forms/tabs.
System Status		Displays the System Status window which lists all access control devices defined in System Administration.
Device Groups		Displays the various device groups for a particular monitoring zone. Bulk operations can be performed on all parts of the device group. Types of device groups include (but are not limited to) Readers, Cameras and Input and Output groups.
Pending Alarms		Displays the Pending Alarms window. To return to the Main Alarm Monitoring window click the View Alarms toolbar button.
Video Verification		Launches the Video Verification window where you can compare live video to a cardholder's photograph.
Video Monitoring		Launches the Live Video window which is used to run a video tour of the cameras defined in Camera Groups.
SkyPoint Application		Launches the SkyPoint application for viewing video. **Note:** This option is only available if you have the SkyPoint client application, which is a separate installation and not included with the ReadykeyPRO installation.

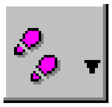
View menu (Continued)

Menu option	Toolbar button	Function
Map	🗺 ▾	Displays a map containing the device associated with the selected alarm (if the Main Alarm Monitoring window is active) or the selected device (if the System Status window is active). • If the selected device is represented on more than one map you will be prompted to select the map of choice. • A message displays if the selected device is not represented on any map. • To display the **View Map** menu option, right-click a device in the System Status window or select an alarm in the Main Alarm Monitoring window. • To print a map, select **Print** from the **File** menu. The map must be the up most window to print.
Default Map		Displays the map that is assigned to that monitoring zone. This menu option is dimmed if no map has been assigned to this zone. This menu option is displayed through the Map icon drop-down.
Map Selection		Displays a window in which all available maps are listed. This menu option is dimmed if no map has been assigned to this zone. This menu option is displayed through the Map icon drop-down.
Scheduler	🕒	Displays the Scheduler window which is used to add, modify and delete scheduled actions within the ReadykeyPRO system. An *action* is any task that can be performed by software as a result of an event of schedule, for example; download a database, mask/unmask alarm inputs, pulse open a door and reset the use limit. **Note:** The Scheduler window is also available by selecting **Administration** > **Scheduler** in System Administration. For more information, refer to the Scheduler Folder chapter in the System Administration User Guide.
Reports	📄	Displays the Reports folder/window of data entry forms/tabs.
Sort by		Sorts alarms according to criteria chosen in the submenu.
Toolbar		Displays the toolbar when selected (checked).
Status Bar		Displays the status bar when selected (checked).

Trace menu

Menu option	Toolbar button	Function
Monitor Zone		Monitors or traces alarms for the selected monitor zone.
Area		Monitors or traces alarms for the selected intrusion area. The **Area** menu option becomes active (not grayed out) when you highlight a device in the System Status window.

Trace menu (Continued)

Menu option	Toolbar button	Function
Asset		Monitors or traces alarms for the selected asset. The **Asset** menu option becomes active (not grayed out) when you highlight a device in the System Status window.
Badge		Monitors or traces alarms for a specific badge.
Controller		Monitors or traces alarms for the selected access panel/controller. An access panel/controller is a device that acts as the focal point for a group of card readers. The **Controller** menu option or toolbar button becomes active (not grayed out) when you highlight an access panel/controller or any device under a given access panel/controller in the System Status window. **Note:** Access panel/controller traces are recursive, meaning all events occurring on that access panel/controller are included.
Device		Monitors or traces alarms for the selected device. The **Device** menu option becomes active (not grayed out) when you highlight a device in the System Status window. This menu option is displayed through the Trace icon drop-down. **Note:**

Configure menu

Menu option	Function
Alarm Filter	Displays a checklist of alarm types to monitor. The **Alarm Filter** menu option becomes active (not grayed out) when you display an alarm window.
Columns	Displays a list of columns from which to display. The **Columns** menu option becomes active (not grayed out) whey you display an alarm window.
Hardware Status Frequency	Determines how often background updates are performed. The choices are “No Updates”, 10, 15, 20, 30 and 60 minute intervals.
System Status Options	Displays the System Status Options window which is used to specify how the System Status window displays information and what devices are included.

Control menu

Menu option	Toolbar button	Function
Update All Hardware Status		Updates the status of all controllers in the monitoring zone.
Set All Controller Clocks		Sets the clocks in all according to the machine on which the driver is running.

Control menu (Continued)

Menu option	Toolbar button	Function
"Current Device"		This menu option is dynamic, meaning the name of this menu option changes according to the device highlighted in the System Status window. Each "Current Device" menu option also has sub-menu options. For more information refer to the Control menu - "Current Device" sub-menu table on page 44.
Guard Tour		Allows Operators to launch or view a guard tour. Guard tour provides a guard (a cardholder who has been specifically chosen to conduct a tour) with a defined set of tasks that must be performed within a specified period of time. Typical tasks include swiping a card at a checkpoint access reader or turning a key connected to an alarm panel input. To use guard tour the Linkage Server must be properly configured. For more information, refer to the System Options Folder chapter in the System Administration or ID CredentialCenter User Guide.

Control menu - "Current Device" sub-menu

Sub-menu option	Toolbar button	Function
Note: The "Current Device" sub-menu options that are available depend on the type of device listed as the "Current Device" in the **Control** menu. The type of device listed as the "Current Device" in the **Control** menu depends on the device highlighted in the System Status window.		
Current Status		Displays current status of device.
Acknowledge		Acknowledges the selected alarm.
Trace		Traces the selected device.
Update Hardware Status		Polls currently selected access panel/controller and updates the hardware status. If a downstream device is selected, the update hardware status is done for the controller associated with that device.
Properties		Displays access panel/controller properties.
Open Door(s)	🚪	Pulses open any door associated with selected access panel/controller or reader. To activate the Open Door(s) toolbar button you must select an access panel/controller or reader, otherwise the option is grayed out.
Set Controller Clock		Sets selected access panel/controller clock to current time. If a device other than an access panel/controller is selected, this option sets the clock on the access panel/controller to which the device is attached.
Reader Access Modes		Updates the reader mode of every reader associated with selected access panel/controller or reader.

Control menu - “Current Device” sub-menu (Continued)

Sub-menu option	Toolbar button	Function
Reader Biometric Verify Mode		Enables/disables verify mode for access control readers with an associated biometric reader. • When verify mode is enabled, the normal card and/or pin access is and a biometric match is required. • When verify mode is disabled, only the card and/or pin access is required.
Reader First Card Unlock Mode		Enables/disables the Reader First Card Unlock Mode. The Reader First Card Unlock Mode is a qualifier for online Reader Mode. When enabled, the online Reader Mode is in effect until the first (qualified) access granted with entry occurs. When the first access granted with entry occurs, the online Reader Mode changes to unlocked. Whenever a Reader enters or leaves First Card Unlock Mode, an event transaction is logged in the database and displayed in Alarm Monitoring. **Note:** The Reader First Card Unlock Mode can also be enabled/disabled via the Reader folder/window in System Administration, via local timezone control in the RKP-2000 and as part of the Reader Mode or Reader Group Mode action used in the Scheduler and Global I/O. **Note:** Reader First Card Unlock Mode is only supported on the RKP-2000 controller. However, first style unlock behavior can be configured for use with any access controller through Bosch’s Global I/O Support.
Activate		Activates the selected alarm output.
Deactivate		Deactivates the selected alarm output.
Pulse		Pulses an output device.
Mask		Masks an input device. The System Status window displays `masked` beside the selected device.
UnMask		Unmasks an input device.
Receiver account information		A *receiver* is a piece of hardware used to receive events from multiple accounts in multiple formats. Downstream devices connect to receivers via phone lines, direct wire connections and LAN connections. The receiver account information displays information about a specific receiver.
View Map		Displays a map associated with the selected device (if one exists). If more than one map exists, the user is prompted to select a map.
Launch Video		Displays video for the selected device if a camera is associated with the device.
Download Firmware		Downloads firmware to the following downstream devices: Dual Interface Rdr1 readers, RKP-1100 and RKP-1200 alarm panels, and RS-485 command keypads. **Note:** It is not possible to download firmware to a single reader interface.
Download Database		Downloads the database to the access panel/controller.
Reset Use Limit		Resets the number of times a badge can be used on a particular access panel/ controller.

Control menu - "Current Device" sub-menu (Continued)

Sub-menu option	Toolbar button	Function
Connect		Connects the access panel/controller via a dialup/modem connection.
Disconnect		Disconnects the access panel/controller via a dialup/modem connection.
Execute Custom Function		Executes a custom function associated with the Bosch Intrusion Controller. This menu option is only available with Bosch Intrusion Controllers.
Bypass		Term used to indicate that the zone has been masked. If a zone is bypassed the controller ignores any tamper or alarm condition for the zone.
Unbypass		Similar to bypass, this command unmasks the zone so that any tamper or alarm will be reported.

Options menu

Menu option	Function
Mute Sound	Disables the audio portion of the system when selected (checked).
Font	Selects the font used in Alarm Monitoring.
Save Alarms on Exit	Saves all currently displayed alarms at the end of a session, when selected (checked).
Save Settings on Exit	Saves screen characteristics at the end of a session, when selected (checked). The following settings will be saved for the current user's profile: 1. Window positions, sizes, and minimized states 2. Matrix or player mode 3. Window arrangement setting 4. Scale factor 5. List of live and recorded video windows **Note:** Windows playing video from a file will not be saved. When the user logs back in, all the video windows previously saved will automatically be launched. Recorded video windows will be launched as live video, since recorded video time is typically not relevant later.
Save Settings Now	Saves screen characteristics immediately.
Ascending Time/ Date	Lists alarms in ascending order of time and date (i.e., oldest first), when selected (checked).
Descending Time/ Date	Lists alarms in descending order of time and date (i.e., newest first), when selected (checked).
Display Seconds	Includes seconds in the displayed alarm times, when selected (checked).

Options menu (Continued)

Menu option	Function
Auto Cardholder Display for Access Alarms	Displays the cardholder associated with an incoming alarm whenever the alarm deals with a badge id. • If selected (checked), Alarm Monitoring displays the cardholder associated with access alarms. • If not selected (unchecked), Alarm Monitoring does NOT display the cardholder associated with access alarms.
Automatic Map Display	Automatically displays a map when the alarm arrives, if selected (checked) and if the associated device exists on a map. If the device exists on multiple maps, the first one found will be displayed. This feature must also be configured in System Administration **Monitoring** > **Alarm Configuration** menu, Alarm Definitions tab/form.
Automatic Cardholder Display	Applies to alarms for which the **Show Card Holder** check box is selected in the System Administration software. To locate this check box select the **Monitoring** menu and then select **Alarms**. Click the Alarm Definition tab. • If selected (checked), the corresponding cardholder view automatically displays when the alarm arrives if the alarm is related to a badge id. • If the cardholder view is already displayed when a new alarm arrives, the new cardholder associated with the alarm is searched for and displayed. • If not selected (unchecked), the corresponding cardholder view does not automatically display when an alarm occurs.
Automatic Video Verification	Applies to alarms for which the **Video Verification** check box is selected in the System Administration software. To locate this check box select the **Monitoring** menu and then select **Alarms**. Click the Alarm Definition tab. • If selected (checked), the corresponding video verify view automatically displays when the alarm occurs. • If not selected (unchecked), the corresponding video verify view does not automatically display when the alarm occurs.
Automatic Visual Notification	Causes breakthrough alarms to occur. By default, this menu choice is selected (checked) in Alarm Monitoring. • If selected (checked), breakthrough alarms cause the Monitoring application and the Main Alarm View to be brought to the foreground when an alarm occurs. • If not selected (unchecked), breakthrough alarms occur in the background. Automatic visual notification must be configured for individual alarms in System Administration. From the **Monitoring** menu select **Alarm Configuration**. Click the Alarm Definition tab. Highlight the appropriate alarm, click the [Modify] button, select the **Visual Notification** check box. Click the [OK] button. In the Alarm Monitoring application be sure to refresh the Alarm configuration through the **Options** menu.
Automatic Live Video Display	Displays live video automatically when an alarm occurs, if selected (checked).
Launch Video for Active Alarm	Displays the video for the active alarm. When the video is launched from a restored alarm the start time of the video clip will be the actual alarm time minus the pre-roll time.

Options menu (Continued)

Menu option	Function
PTZ Options	Displays the PTZ Options dialog which is used to specify locking options, the default PTZ mode, and step mode options.
SkyPoint Options	Displays the SkyPoint Options dialog which is used to specify full screen or windowed display, window resolution, and monitor that will be used for the application. **Note:** This dialog is only available if you have the SkyPoint application installed.
Display Status On Maps	Displays the status of all device icons on graphical maps. • If selected (checked), the status of every device icon on a graphical map is displayed (e.g. online/offline, occupancy number). • If not selected (unchecked), the status will only be displayed for a given device as a tool tip when the mouse pointer is over the device icon.
Highlight Entire Row	Highlights the entire row of an alarm when selected (checked).
Disable Command Verification	Displays "successful configuration" messages when commands to hardware, E-mail and pages are successfully sent. • If selected (checked), Alarm Monitoring will NOT display "successful configuration" messages. • If not selected (unchecked), Alarm Monitoring displays "successful configuration" messages. Errors display in message boxes regardless of this setting.
Execute Command on Single Click of Icon	Specifies commands to be executed on a single click. This setting may be configured for each user and saved along with other user settings. • If selected (checked), then a single click executes the default command for the device configured in System Administration. • If not selected (unchecked), then the default command executes on a double-click.
Display Controller Capacity	Displays available memory, free memory, the maximum number of cardholders, current cardholders stored in a controller, maximum number of biometric templates and the current number of biometric templates set in a controller. This information is displayed in the System Status window and is mainly used for diagnostic purposes. By default, this option is unchecked. • If selected (checked), the controller capacity information displays. • If not selected (unchecked), the controller capacity information is NOT displayed.

Options menu (Continued)

Menu option	Function
Display Device Firmware Versions	Displays firmware version (major and minor) for downstream devices. The minor firmware version number displays as the last two digits. The firmware version of controllers and gateways displayed regardless of this option. **Note:** The firmware version is that of the interface board. • If selected (checked), the current firmware version displays for devices including single interface readers, dual interface Rdr1 readers, RKP-1100 and RKP-1200 alarm panels, cameras and RS-485 command keypads. • If not selected (unchecked), the firmware version displays as part of the status when the mouse pointer is over the device icon. However the firmware version of controllers and gateways always displays, regardless of this option.
Display Device Serial Numbers	Displays the serial number of most devices. The serial numbers are displayed in the System Status Tree for all devices that report a serial number. **Note:** Bosch Dual Interface Rdr 2 readers and biometric readers do not report serial numbers. and biometric readers do not report serial numbers. • If selected (checked), the serial number information displays. • If not selected (unchecked), the serial number information is NOT displayed.
Refresh Alarm Configuration	Causes alarm configuration information to be refreshed.

Window menu

Menu option	Function
Cascade	Places all open windows in an overlapping arrangement with the active window displayed on top.
Tile Horizontally	Places all open windows in a horizontal, non-overlapping arrangement.
Tile Vertically	Places all open windows in a vertical, non-overlapping arrangement.
Arrange Icons	Places all minimized windows (title icons) in a row.
Close “options”	There are several menu options to close different windows in the Alarm Monitoring application (e.g. Close All Windows, Close System Status Windows).
Numbered choices	Lists all open windows. The active (topmost) window is indicated by a checkmark.

Help menu

Menu option	Function
Contents	Displays online help for the currently displayed window.
Send Feedback	Displays the Send Feedback form. From here you can launch a web feedback form and send feedback directly to Bosch.
Index	Displays the online help table of contents.
About Alarm Monitoring	Displays version and copyright information.

Cardholder menu

Menu option	Function
Note: This menu is only available after you select **View** > **Badge Info** from the menu options.	
Show Unassigned Assets	If selected, both assets that currently are and assets that once were (but have since been unassigned) assigned to the selected cardholder will be displayed in the listing window on the Assets form. If not selected, only assets that are currently assigned to the selected cardholder will be displayed.
MobileVerify	When selected, displays the MobileVerify Options window where the gate assigned to the current MobileVerify workstation can be changed, or the system's Force Protection Setting can be overridden. For this option to be available, the following conditions must be met: • The user must have the MobileVerify Workstation Options permission, which is set on the MobileVerify sub-tab of the System Permission Groups form in the Users folder. • A recommendation label must have been added to the Cardholder form using FormsDesigner. (The recommendation label may be on a new separate tab or on the Cardholder form.) • The current workstation must have a gate configuration assigned to it. This is done on the Gate Configuration sub-tab of the Workstations form in the Workstations folder.
Keyboard Wedge Settings	When selected, displays the Wedge Scanner Settings window where you can configure how the ReadykeyPRO system interprets the information it receives from a wedge reader. You must have administrative rights to the workstation when setting these options. These settings are set per workstation.
View Options	When selected, displays the View Options window from where you can choose cardholder search attributes.
One Free Pass	If selected, allows the selected cardholder to violate anti-passback rules one time.
APB Move Badge	When selected, displays the Area Move Badges window from where you can move a badge to a new area.
Display Global APB Areas	When selected, displays the Cardholder Global Anti Pass Back (APB) Areas window. This window lists the global APB areas that the selected cardholder is currently located in.
Show Last Granted Location	If selected, the **Last access** field will display information about the most recent valid access by the selected cardholder, including the triggered event, date, time and reader name.
Show Last Attempted Location	If selected, the **Last access** field will display information about the most recent access attempt (whether access was granted or not) by the selected cardholder, including the triggered event, date, time and reader name.
Bulk	Provides a sub-menu of options that can be applied to a select group of cardholder records.
First Record	Displays the first matching cardholder record.
Rewind	Jumps back 10 matching cardholder records.
Previous Record	Displays the previous matching cardholder record.
Next Record	Displays the next matching cardholder record.
Fast Forward	Jumps forward 10 matching cardholder records.
Last Record	Displays the last matching cardholder record.

Cardholder menu - Bulk sub-menu

Menu option	Function
Note: The **Bulk** sub-menu is only available when the **Cardholder** menu is available. **Note:** The **Bulk** sub-menu options are available when a cardholder record is displayed in the Cardholders folder/ window.	
Assign Access Levels	Allows you to assign access levels to a select group of cardholder records.
Remove Access Levels	Allows you to remove access levels from a select group of cardholder records.
Modify Badges	If selected, displays the Bulk Modify Badges window from where you can choose to update one or more of the following fields in the Cardholders folder/window: **Activate Date**, **Deactivate Date**, **Badge Status** and **Use Limit**. You can apply a filter as to which badges you want to update, based on status and/or type. Note that when updating the **Badge Status** field, you must select a badge status filter. **Note:** When bulk changing the **Use Limit** field and enter no value it will automatically be set to 255 (unlimited).
Change Cardholder Segments	When selected, the Bulk Segment Change window opens from where you can change a selected group of cardholder record's segment assignment.
Change Cardholder Replication	When selected, the Change Cardholder Replication window opens from where you can select a new replication setting. **Note:** This menu option applies only to Enterprise systems.
Delete Cardholders in Search	Allows you to delete cardholders to a select group of records.
Destroy ALL Cardholder Data	Allows you to destroy all cardholder data.
View Log	Displays the Log Viewer window from where you can view a log of bulk events.

Asset menu

Menu option	Function
Note: This menu is only available after you select **View** > **Asset Info** from the menu options.	
First Record	Displays the first matching asset record.
Rewind	Jumps back 10 matching asset records.
Previous Record	Displays the previous matching asset record.
Next Record	Displays the next matching asset record.
Fast Forward	Jumps forward 10 matching asset records.
Last Record	Displays the last matching asset record.
Asset Groups and Classes	Displays the Asset Groups and Classes Management folder/window.

Asset menu (Continued)

Menu option	Function
Asset Types and Subtypes	Displays the Asset Types and Subtypes Management folder/window.
Show Assignments X Days Past	Displays the Filter Out Assignments After X Days window, which allows you to specify the number of days you want to view.
Bulk Add Mode	Enables you to quickly enter multiple Scan IDs for the same type of asset (e.g. enter multiple Scan ID's for 10 portable PCs). To display the **Bulk Add Mode** menu option an asset record must be open in the Assets folder/window.

Toolbar Procedures

How to Use the Toolbars

Alarm Monitoring utilizes one standard Windows toolbar.

If you want to:	Procedure:
Display the name of a toolbar button	Point to the toolbar button with the mouse (without clicking).
Use a toolbar button to perform a command or function	Click the toolbar button with the left mouse button.
Change the toolbar from "anchored" to "floating" Change the toolbar from "floating" to "anchored"	Double-click an empty area of the toolbar.
Hide or display the toolbar	From the **View** menu select **Toolbar**. A checkmark appears next to the toolbar if it is not hidden. Toggle the toolbar to display or hide.

Alarm Monitoring Status Bar

The Alarm Monitoring status bar, located in the lower portion of the screen provides different information, depending on what window is displayed.

The Main Alarm Monitoring window displays the following information in the status bar:

- **Selected alarm:** the name of the selected alarm, if any. If multiple alarms are selected simultaneously, the last one that was selected is indicated here.
- **Sort criteria:** the information by which the list of alarms is currently sorted.
- **Pending:** the number of alarms that are currently pending. Pending alarms include all existing normal or initiating alarms marked as "Active" that are still displayed in the main alarm view and have not been acknowledged.
- **Total:** the total number of alarms currently in the window.
- **Verified mode enabled:** an access control reader that has an associated biometric reader, is in verify mode.

System Administrator Procedures

Chapter 3: System Administrator Procedures

The Alarm Monitoring application is not only designed to monitor alarms and events, but it can also be used for a variety of administrative tasks such as adding cardholders or visitors, printing badges, adding assets to the database and assigning assets to cardholders. Depending on how the System Administrator sets the cardholder and system permissions, users with access to Alarm Monitoring can add, modify and delete cardholder, badge and asset information as well as capture images and perform bulk operations.

This chapter assumes that an Alarm Monitoring Station has been physically set up and focuses on the procedures the System Administrator should complete to enable procedures to be performed by Alarm Monitoring Operators. Refer to the ReadykeyPRO release notes to determine the PC requirements for an Alarm Monitoring Station (client or server) and refer to the Digital Video Hardware Installation Manual for physically setting up the hardware.

Note: Additional System Administrator procedures may be included in the Advanced Operator Procedures on page 127.

Administrative Procedures Checklist

The administrative procedures are completed via the **Administration** menu in the System Administration application. Instructions can be found in the Administration section of the System Administrator User Guide.

- **Create card formats** - card formats (asset, magnetic, smart card, etc.) are required to configure a reader
- **Create badge types** - (employee, visitor, etc.)
  - printing/encoding badge options
  - required cardholder fields
  - badge ID allocation for generating ID numbers
  - guest defaults (extended strike/held times, passage mode, deadbolt override)
- **Add directories** - required for single sign-on
- **Set system, cardholder, monitor and field/page permissions**
- **Add users**
  - user name
  - internal account and password
  - directory account
  - segment access
  - area access manager levels
- **Add Alarm Monitoring workstations** - workstations are required to configure hardware devices
  - add dot matrix printer via workstations folder

  - connect a printer locally (directly to the Alarm Monitoring workstation).
- **Set general system options**
  - log on authorization warning
  - strong password enforcement
  - number of days to save queued events
  - Linkage Server host
  - DataExchange server host
- **Set cardholder options and visits**
  - maximum number of badges per cardholder
  - ability to create/save photo thumbnails
  - badge PIN types (4, 6 or 9-digits)
  - PIN code generated (random or manual)
  - precision access mode
  - use or lose badge feature (change badge status to lost or returned after a specified amount of time)
  - visits options
  - cardholder, visitor and visit search result options
- **Configure global output devices**
  - SMTP server settings to use when sending e-mail
  - GOS paging device
  - recipients of e-mail and page messages
- **Configure e-mail and paging notification**
  - fields and display order for e-mails and paging
  - fields and/or directories to check when determining who to send an e-mail notification to
- **Add segments to your installation**
  - enable segmentation
  - segment options
- **Create list options** (using List Builder)
- **Set up archiving parameters**

Access Control Procedures Checklist

This portion of the chapter focuses on the procedures the System Administrator should complete to enable access control and monitoring procedures to be performed by Alarm Monitoring Operators.

Note: Be sure to complete the administrative procedures listed at the beginning of this chapter before attempting any access control and monitoring procedures. Several access control and monitoring procedures require that certain administrative procedures be completed first. For example you must configure a workstation before you can configure most hardware devices.

All System Administrator access control procedures are completed via the **Access Control** or **Additional Hardware** menu in the System Administration application. Instructions can be found in the Access Control section of the System Administration User Guide, as well as the Additional Hardware section. A separate Intrusion Detection User Guide also exists if you are going to configure intrusion detection devices.

- **Configure hardware devices**
  - dialup modem
  - access panels
  - readers
  - alarm panels
- **Additional access control configurations**
  - timezones (specify holidays, assign readers and modes of operation)
  - access levels
  - anti-passback areas (normal, safe and hazardous areas for mustering)
  - alarm mask groups (un/mask multiple alarm inputs simultaneously)
  - device groups (input/output readers)
  - local and/or global inputs and outputs
- **Configure additional hardware**
  - fire panels
  - intercom devices
  - personal safety devices
  - receivers
  - intrusion detection devices

Intrusion Detection Alarm Definitions

See the Alarm Definitions appendix in the Intrusion Detection User Guide for information on alarm definitions in references to customizing intrusion detection alarms.

Alarm Monitoring Operator Procedures

These procedures are used to handle intrusion detection events in Alarm Monitoring. For specifics see the Alarm Monitoring Operator Procedures chapter in the Intrusion Detection User Guide.

Intrusion Detection Device Statuses

See the Intrusion Detection Device Statuses appendix in the Intrusion Detection User Guide for more information.

Monitoring Procedures Checklist

System Administrator monitoring procedures are completed via the **Monitoring** menu in the System Administration application. Instructions can be found in the Monitoring section of the System Administration User Guide.

- **Customize alarms, instructions, acknowledgment notes and acknowledgment actions**
  - alarm mask groups
  - customize and configure alarms
  - text instructions
  - audio
  - acknowledgment notes
  - automatic acknowledgment actions
- **Configure monitor zones**
  - event routing group
  - monitor zones
  - monitoring station assignments
- **Set up guard tours**
  - checkpoint actions
  - messages and checkpoint events
  - monitoring stations
  - link camera devices to the checkpoints
  - special instructions
- **Set Monitoring Options**
  - associate a command with a device or area icon (enables operators to execute a command with a single and double left-click in the system status tree and map view)

Video Procedures Checklist

All the video procedures are completed via the **Video** menu in the System Administration application. Instructions can be found in the Video section of the System Administration User Guide.

- **Configure video**
  - matrix switcher
  - video devices (recorders and cameras)
  - link hardware devices to a camera
  - alarm-video configurations
  - add a video recorder to a monitoring zone
- **Configure video verification**
  - CCTV Controller associated with a workstation
  - CCTV Command (located on **Access Control** > **Readers** > Control tab)

Operator Procedures

Chapter 4: Set Alarm Monitoring Display Options

Several windows in Alarm Monitoring can be configured to display according to user preference. These views are recreated every time the user logs into the application.

The following is a list of user-defined display options that are set from the **Configure** or **Options** menu.

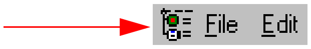
- Select Event Types to Monitor
- Select Column Configuration
- Set Automatic Display Options
- Select Hardware View Options

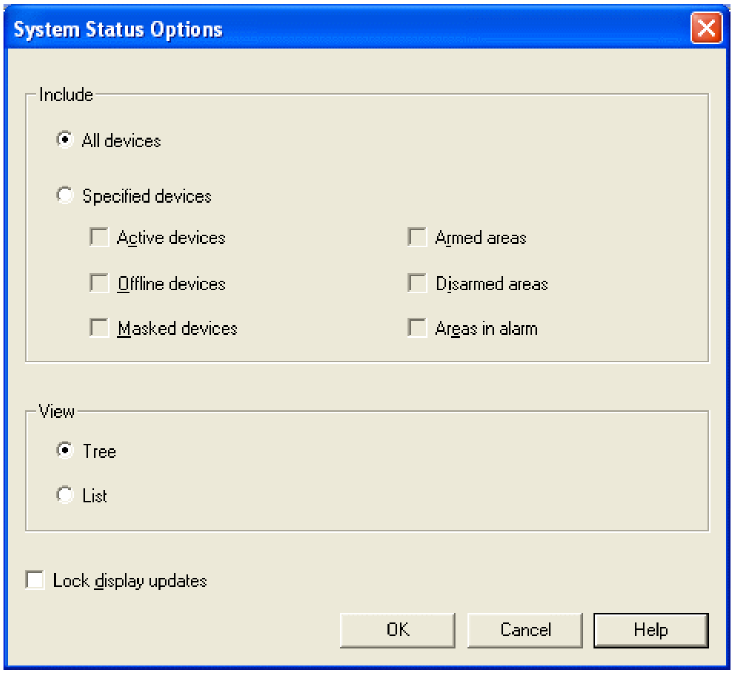
Note: The Select Hardware View procedure displays the System Status Options Window.

System Status Options Window

The System Status Options window is displayed from the System Status window. Verify you are in the System Status window, then select **Configure** > **System Status Options** from the menu.

You can also display the System Status Options window by clicking the System Status icon that displays to the left of the **File** menu (when you open the System Status window).




System Status Options

Include

● All devices

○ Specified devices

□ Active devices □ Armed areas

□ Offline devices □ Disarmed areas

□ Masked devices □ Areas in alarm

View

● Tree

○ List

□ Lock display updates

Button/field	Description
All devices	Displays all the devices (active, offline) in the System Status window.
Specified devices	Displays specific types of devices including: **Active devices** Displays only active devices in the System Status window. **Offline devices** Displays only offline devices in the System Status window. **Masked devices** Displays only masked devices in the System Status window. **Armed areas** Displays only armed areas in the System Status window. An *area* is a separately configured section of an Intrusion Detection Panel, sometimes referred to as a *partition*. To arm an area means to “turn on” the protection for an area. **Disarmed areas** Displays only disarmed areas in the System Status window. **Areas in alarm** Displays only areas that have an active alarm triggered. **Note:** If one or more of the specified device selections are made, only devices matching those criteria display in the view.

Button/field	Description
View	Displays information about devices in one of two formats: **Tree** Displays information in a hierarchical fashion, also called a tree or branching arrangement. Each entry in the list represents one device. Panels have the leftmost entries and any device connected to a panel listed below the panel and indented to the right. You can search this or any tree by focusing on the list window and clicking “Ctrl+F”. To proceed through the search, press F3 on your keyboard. **List** Lists the following information about devices in the system: • Device (Name) • Parent Device (Name) • Current Device Status
Lock display updates	Prevents items from being added or deleted from the display window. When the **Lock display updates** check box is selected an indicator on the status bar displays “LOCKED.” Devices cannot be added to or deleted from the display window. The status of devices currently in the window update as their status changes. Then if the status of devices not in the window change, they are not added to the display window. When the **Lock display updates** check box is not selected, the status bar indicator is blank. Devices are added to and removed from the display window automatically as their device status changes. For example, if an input becomes active and the view is displaying active devices, the input will be added to the view. If the input is now restored, it will be removed from the view.
OK	Accepts the settings and closes the window.
Cancel	Closes the window without saving any changes made to the settings.
Help	Displays help for this topic.

Display Option Procedures

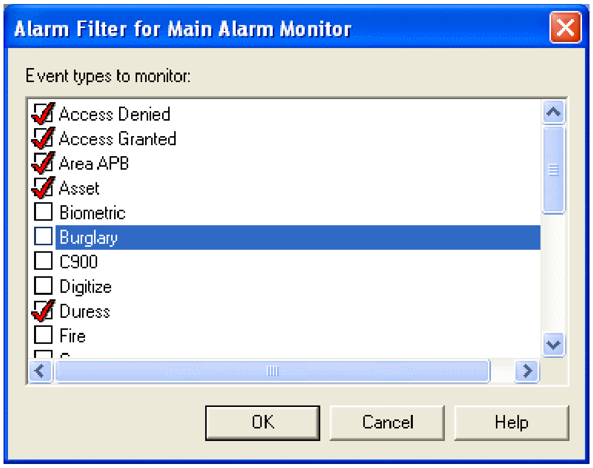
Select Event Types to Monitor

If you have permission to edit alarm filters, you can apply an alarm filter to each view in Alarm Monitoring, including the main alarm view, pending alarm view, video verification view and any trace view. Each of these views can be configured to filter out alarms independent of each other, however, only the main alarm view filter is saved from session to session.

The alarm filter determines which alarms display based on the type of event the alarm is associated with.

For example, you may wish to display every alarm for a specific reader’s trace window but you may not wish to display “Access Granted” alarms in the Main Alarm Monitoring window. You can apply both of these filters to the different views, but when the session ends, only the filters applied the main window are saved.

1. Open the window from which you want to select the events displayed. Verify this window is the active (topmost) window.
2. From the **Configure** menu select **Alarm Filter**. The Alarm Filter window displays.



Alarm Filter for Main Alarm Monitor

Event types to monitor:

☑ Access Denied
☑ Access Granted
☑ Area APB
☑ Asset
☐ Biometric
☐ Burglary
☐ C900
☐ Digitize
☑ Duress
☐ Fire

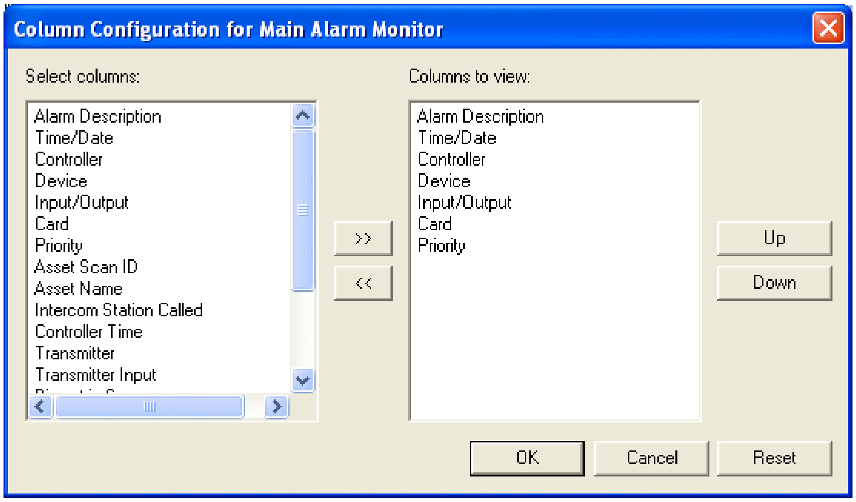
3. By default, all event types are selected (have a checkmark). If you do not want to display a particular category of events, click that option to deselect it (remove the checkmark). Click the option again to select it.
4. Click [OK] to close the Alarm Filter window

Select Column Configuration

You can rearrange the order of the columns in any window as well as add or remove columns that display. This is done independently for each type of window. For example, if the column configuration is changed for an alarm window, this becomes the default for all alarm windows of the same type. If the column configuration is changed for a given trace, this will become the default configuration for all traces.

1. Open the window from which you want to configure the columns displayed. Verify this window is the active (topmost) window.

2. From the **Configure** menu select **Columns**. The Column Configuration window displays.



Select columns:

Alarm Description
Time/Date
Controller
Device
Input/Output
Card
Priority
Asset Scan ID
Asset Name
Intercom Station Called
Controller Time
Transmitter
Transmitter Input

Columns to view:

Alarm Description
Time/Date
Controller
Device
Input/Output
Card
Priority

3. In the **Select columns** display field, click/highlight the name of a column, then click [>>]. The column name appears in the **Columns to view** display field.

4. Arrange the column names in the order you want them to appear. Click/highlight a column name in the **Columns to view** display box. Then use the [Up] and [Down] buttons to change the column's relative position.

Note: The order the column names appear in the **Columns to view** display field is the same order the columns will display in the window which you are configuring the columns for.

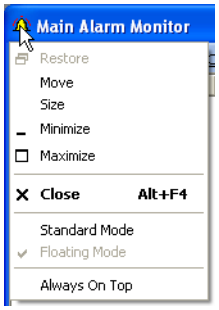
5. Click [OK] and the window displays the new column configuration.

Set Automatic Display Options

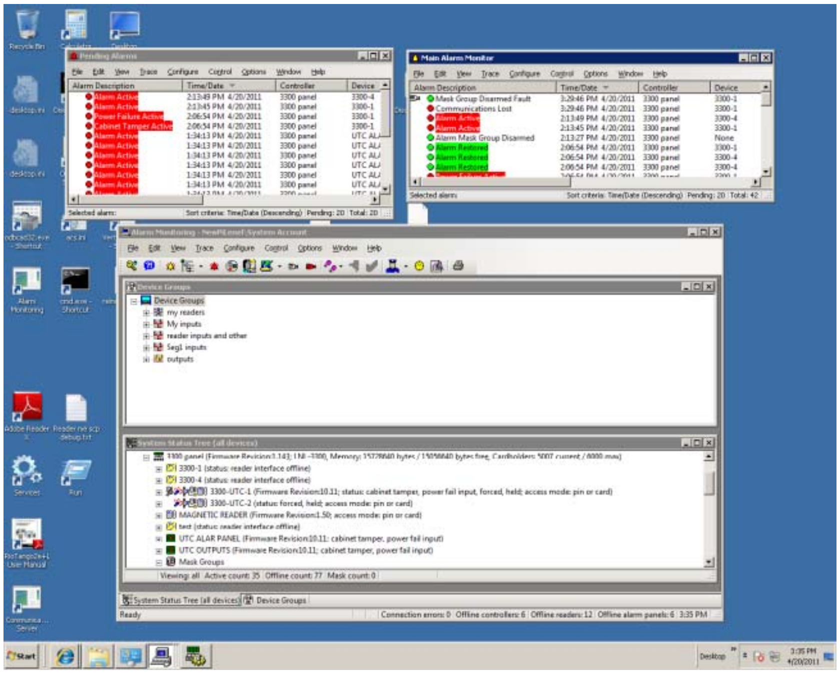
Several display options are available from the **Options** menu. To activate an option select it (place a checkmark beside it). To deactivate an option select it again to remove the checkmark. For information on the options available from the **Options** menu, refer to Chapter 2: Main Alarm Monitoring Window on page 39

Toggle Window Display Modes

In Alarm Monitoring, you can use the following options from a window’s shortcut menu to switch between the window display modes. (Open the shortcut menu by left-clicking on the icon in the window’s title bar.)



- **Standard Mode -** This is the default window display mode. When this mode is selected, the window cannot be moved outside of the main Alarm Monitoring window. For more information, refer to Display Multiple Windows in the Main Window on page 69.
- **Floating Mode -** When this mode is selected, the window is independent of the main Alarm Monitoring window, and can be moved (dragged) outside the main window onto one or more monitors:



Floating windows contain the main window menu bar and appear in the Windows taskbar. In addition, the **Always on top** menu option is available for floating windows. When **Always on top** is selected, the window remains in view when you switch to a different window.

The following windows can display in the floating mode:

– Main Alarm Monitor

- Pending Alarms
- Trace Monitors
- System Status
- Map views
- Cardholder Verification
- Video Verification
- Video Monitoring

Display Multiple Windows in the Main Window

For windows in the standard display mode, complete the following steps:

1. Open the desired windows using the toolbar buttons or menu options.
2. From the **Window** menu select one of the following:
   - Cascade
   - Tile Horizontally
   - Tile Vertically
3. Using the mouse, click and drag each window to resize and relocate it.

Select Hardware View Options

Hardware view options include list or tree view as well as the type of devices displayed. Users can display every device or select devices that meet a specific criteria such as active, offline and/or masked devices as well as armed areas, disarmed areas and/or areas in alarm.

1. Verify you are in the System Status window, then select **Configure** > **System Status Options** from the menu.
2. The System Status Options window displays.
   a. Select the type of device you would like to display by clicking either the **All devices** or **Specified devices** check box. If you selected the **Specified devices** check box, select the desired device by clicking the appropriate radio button (active, offline or masked devices).
   b. Select the **Tree** radio button to view the system hardware in a tree or branching format.
   c. Select the **List** radio button to view a list of devices, their current status and parent device.
   d. Select the **Lock display updates** check box if desired.
3. Click [OK].

Chapter 5: Monitor Devices

The System Status window and Device Groups window are used to monitor devices.

System Status Window

The System Status window lists every access control device, area or action group defined in System Administration for a specific segment. Other configuration settings are listed in parenthesis after each device.

Displayed by:

The System Status window can be displayed several ways:

- Click the triangle on the System Status button and select an existing window or open a new one.

Note: Clicking the System Status button (not the triangle) brings up a new System Status window if there is none present. If a System Status window is already open, clicking the System Status button causes the default (first) window to display.

- From the **View** menu, select **System Status** and then the window you want to display.
- Choose one of the numbered options under the **Window** menu.
  - Though rare, if more than nine (9) System Status windows are open, the **More Windows** menu option will be available. Choose a window from the list and click [OK] to bring it to the foreground.

Device Groups Window

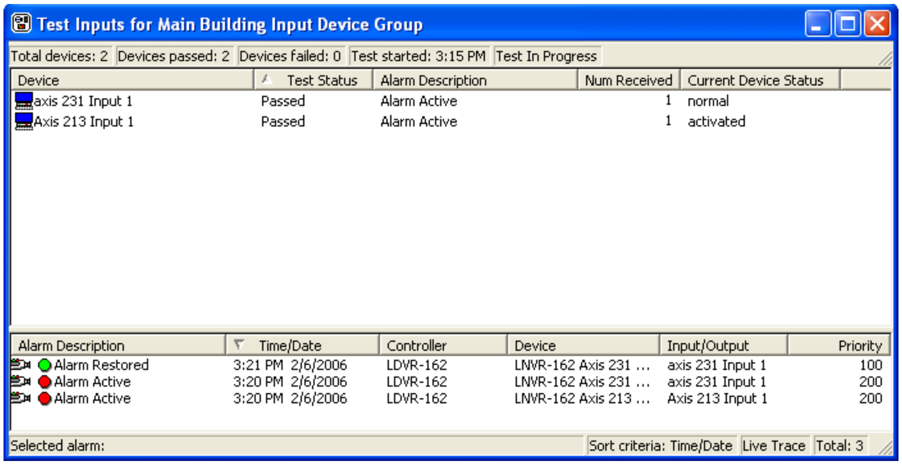
The Device Groups window displays the currently configured device groups within a monitoring zone and is expandable in the tree view. The Device Groups window allows operators to view, test and change the status of devices (cameras, remote monitors, readers, inputs and outputs).

Toolbar Shortcut

To display the Device Groups Window, click the View Device Groups toolbar button or select **Device Groups** from the **View** menu

Device Group Test Mode Window

Similar windows display for the test access grants, test forced open and test inputs for device groups. The example below is a Test Inputs for an input device group.



Test Inputs for Main Building Input Device Group

Total devices: 2 | Devices passed: 2 | Devices failed: 0 | Test started: 3:15 PM | Test In Progress

Device	Test Status	Alarm Description	Num Received	Current Device Status
axis 231 Input 1	Passed	Alarm Active	1	normal
Axis 213 Input 1	Passed	Alarm Active	1	activated

Alarm Description	Time/Date	Controller	Device	Input/Output	Priority
● Alarm Restored	3:21 PM 2/6/2006	LDVR-162	LNVR-162 Axis 231 ...	axis 231 Input 1	100
● Alarm Active	3:20 PM 2/6/2006	LDVR-162	LNVR-162 Axis 231 ...	axis 231 Input 1	200
● Alarm Active	3:20 PM 2/6/2006	LDVR-162	LNVR-162 Axis 213 ...	Axis 213 Input 1	200

Selected alarm: | Sort criteria: Time/Date | Live Trace | Total: 3

Field	Description
Upper status bar	Displays information about the upper display window and includes the total number of devices tested, the number of devices that pass and fail, what time the test started and the current status of the device test.
Upper display window	Displays the device name, test status, alarm description, number of inputs or requests received and the current device status. The information displayed in this window can be sorted by any column.
Lower display window	Displays a variety of user-defined columns that can be sorted. Users can select whether the following columns display: Alarm Description, Time/Date, Controller, Device, Input/Output, Card, Priority, Asset Scan ID, Asset Name, Intercom Station Called, Controller Time, Transmitter, Transmitter Input, Biometric Score, Account Group, Badge Type, Text, Line Number and Intrusion Area. For more information, refer to Select Column Configuration on page 66.
Lower status bar	Displays information about the lower display window and includes the name of the currently selected alarm, sort criteria, trace type and the total number of alarms listed.

Device Group Icons

The table below identifies the different icon groups available.

Icon	Description
🖥	ReadykeyPRO System
▣	Alarm Mask Group

Icon	Description
	Camera Group
	Reader Group
	Alarm Input Group
	Alarm Output Group
	Monitor Group

Hardware Device Icons

The table below identifies the different icons available. To view a list of icons and icon groups available in your database, as well as add or modify icons, open MapDesigner and select **Edit** > **Icon Library**.

Icon	Description
	Access Panel
	Access Panel with selective cardholder download enabled.
	Alarm/Camera/Reader Input
	Alarm/Camera/Reader Output
	Alarm Panel
	Camera **Note:** The Camera icon flashes when there is motion detected with the associated camera. The CCTV Camera icon turns green when there is sound with the associated camera.
	CCTV Monitor
	CCTV Panel
	Facility Utilization Gate
	Fire Panel
Func	Function List
	IntelligentVideo Application

Icon	Description
	IntelligentVideo Server
	Intercom Exchange
	Intercom Station
	Intercom Station Analytics Event
	Intercom Station Call Connected
	Intercom Station Line Error
	Intercom Station Queued
	Intrusion Area
	Intrusion Door
	Intrusion Offboard Relays
	Intrusion Onboard Relays
	Intrusion Panels
	Intrusion Zones
	Matrix Switcher
	DataConduIT Device
	DataConduIT Source
	DataConduIT Sub-Device
	PC Panel
	Personal Safety Device Panel
	Reader
	Receiver
	Remote Monitor
	Remote Monitor Video Cell
	Segment (only if your system is segmented)

Device Status

Alarm Monitoring is the only application that displays the status of hardware devices. Alarm Monitoring obtains the status of a device from the Communication Server, which in turn obtains the device status from hardware controllers.

Status icons are located to the left of hardware device icon. There may be one icon or a combination of icons, depending on the hardware status.

The status of the device is displayed after the entry in parentheses. If viewing the icons on a map, the device status is displayed in parentheses after the icon or as a tool tip when the mouse pointer is over the device icon. This is determined by whether the **Display Status on Maps** option in the **Options** menu is checked.

Note: To view a list of current hardware status icons in your database, as well as add additional icons, open MapDesigner and select **Edit** > **Icon Library.**

Runaway Devices

When configured conditions cause a device to enter a “runaway” state, an alarm is generated and the status information displayed next to the device icon is updated to indicate it is a runaway device. A runaway device is characterized by multiple alarms of the same type coming from the device during a user-defined time interval. While the device is in the runaway state, the Communication Server stops sending the runaway events to Alarm Monitoring stations.

When the configured conditions for the runaway state are no longer true, a restored event occurs and the status information for the device is updated to normal in the hardware tree.

Runaway device conditions are configured on the System Options > Runaway Detection tab in System Administration.

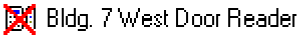
Offline Hardware Devices

Important: The Communication Server must be running in order for the proper offline status to be reported in Alarm Monitoring.

Devices can be marked offline for two reasons: The connection may be broken or it can intentionally be set offline. In Alarm Monitoring a different color “X” is used to differentiate those items that are intentionally taken offline to those that have a broken connection.

Broken Connection

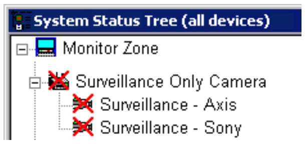
A red “X” through an icon indicates a broken connection, meaning that the software cannot communicate to the device. For example:



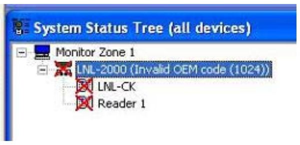
Bldg. 7 West Door Reader

If a child device is offline then the parent device is examined. If both child and parent are found to be offline then a red “X” is used for both devices. If only the child device is offline then a yellow “X” is used for just the child device.

Although surveillance-only cameras are not associated with a physical video recorder, they are assigned to a virtual “surveillance-only recorder” to maintain consistency in the user interface. For example, the Alarm Monitoring hardware tree below shows two surveillance-only cameras assigned to a virtually surveillance-only recorder which serves only as a placeholder to group cameras.



A 16-bit OEM code can be programmed into the device which allows for a check to occur in Alarm Monitoring. If the OEM code doesn’t match the hardware, an Invalid ID transaction is generated and the device will not come online. The system status tree will show the status as offline and list the invalid OEM code.


System Status Tree (all devices)
Monitor Zone 1
LNL-2000 (Invalid OEM code (1024))
LNL-CK
Reader 1

Marked Offline

Many items can be marked offline intentionally in System Administration. When items are marked offline, a black “X” appears on those items in Alarm Monitoring. A black “X” also appears for those items that are deleted from the system. Deleted items are also marked with text that reads “deleted.”

A list of items that can be marked offline are: Alarm inputs, Cameras, Camera Inputs, Camera Outputs, Elevator Dispatching Panels, Fire panels, Intercom devices, Intrusion Detection Devices, Lenel access panels, OPC Connections, Personal Safety Devices, POS Devices, Receivers, SNMP Managers, and Video Recorders.

Items that show a black “X” if their parent device has been marked offline include: Alarm inputs, Alarm Mask Groups, Alarm outputs, Alarm panels, Anti-passback areas, Camera Inputs, Camera Outputs, Cameras, Elevator dispatching terminals, Fire Devices, Fire Inputs/Outputs, Intercom stations, Intrusion Areas, Intrusion Doors, Intrusion Onboard/Offboard relays, Intrusion zones, Local function lists, OPC Sources, POS Register, Readers, Reader Inputs, and Reader Outputs.

Map items need to be configured in MapDesigner to use the current state of the device rather than a default icon for the proper icons to be shown on the map.

Video Failover Status

IP camera icons in the System Status Tree display the status of the primary and secondary recorders if failover is enabled.

Procedures for Monitoring Devices

Update the Hardware Status

Hardware status information displays in several Alarm Monitoring windows. When alarms and actions occur in the system, ReadykeyPRO software updates the status information "live" for the affected hardware. Operators can also choose to have the status updated on demand.

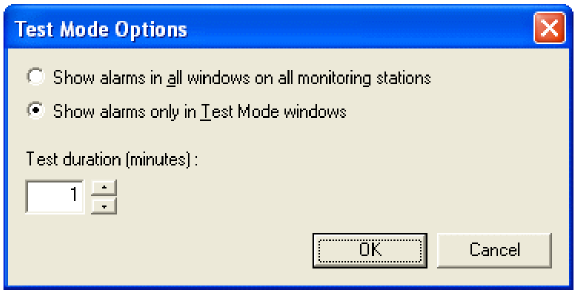
1. Select **Update All Hardware Status** from the **Control** menu or by right-click an alarm, access panel, alarm panel, alarm input, relay output or reader.
2. The update all hardware status feature polls the currently selected device and updates the hardware status of the associated devices. A message displays when the update is complete.

Note: Hardware Status Update Frequency can be used to set automatic updates. You can set the frequency to No Updates, 10, 15, 20, 30 or 60 minutes (by selecting **Hardware Status Frequency** from the **Configure** menu).

Perform a Device Test

Operators can perform a test on various devices in the system. A special test mode operation is available for Input Groups, Reader Groups (Door Forced) and Reader Groups (Access Grants). Performing this test allows you to see which devices generated alarms and which ones did not.

1. Display the Device Groups window by selecting **View** > **Device Groups**.
2. Right-click the device group and select the **Test Inputs**, **Test Door Forced** or **Test Access Grants**. If you select **Test Access Grants**, skip to step 7.
3. A dialog box appears:



Test Mode Options

○ Show alarms in all windows on all monitoring stations

● Show alarms only in Test Mode windows

Test duration (minutes): 1

4. You have two choices. Choose **Show alarms only in Test Mode windows** if you do not want the results to show up on any Monitoring Station. Otherwise choose **Show alarms in all windows on all Monitoring Stations**.
5. Type in the duration (in minutes) of the test. This option is available only if you selected **Show alarms only in Test mode windows**.
6. Click [OK] to initiate the test.

7. A Test Mode window launches. The top portion of the window lists all the devices being tested and their current status (whether the test was successful/ unsuccessful). Devices that failed the test flash in red. The bottom portion of the window displays a trace of the related alarms.
8. When the test is finished, all the windows and monitoring stations resume their normal display of alarms.

Note: Device status is not available for Matrix Switchers or Account Panels.

Locate or Search for a Device

Operators can locate or search for a device in any window in Alarm Monitoring.

1. Display any Alarm Monitoring window.
2. Verify your cursor is in the window.
3. Begin typing the name of the device. The system automatically scrolls to the first occurrence of those letters in column one.

View the Last Connection Time for Dialup Panels

The Last connect time status is displays in parenthesis after each dialup panel. It reflects the time of the panel's last "Communications Restored" event and is updated every time you disconnect from the panel.

To view a dialup panel's Last connect time within Alarm Monitoring, locate the dialup panel in the System Status window. In parenthesis after the name of the dialup panel, the Last connect time is listed.

Last Connection Time Guidelines

The following are guidelines for the Last connect time status:

- If a dialup panel has never connected, the Last connect time for it is "Never".
- If a dialup panel connects while Alarm Monitoring is not running, the Last connect time for it is retrieved from the database when Alarm Monitoring starts up again.
- When a dialup panel is disconnected, the System Status window immediately reflects the new Last connect time regardless of whether the "Communications Lost" alarm is acknowledged or not.
- When a dialup panel and Alarm Monitoring station are in different time zones, the Last connect time displays both the local time and the panel time.

Download the ReadykeyPRO Database or Firmware

Operators can download the ReadykeyPRO database and/or firmware to devices via Alarm Monitoring. Devices include access panels (RKP-500, RKP-1000, and RKP-2000), dual interface Rdr1 readers, alarm panels, RS-485 command keypads and cameras.

Notes: It is not possible to download firmware to single reader interfaces.

It is only possible to download firmware to RKP-1320 version B dual reader interfaces through the primary reader.

It is only possible to download firmware to RKP-CK command keypads connecting directly via RS-485 interface cable.

It is only possible to download firmware to RKP-500B gateways communicating to Handkey and Bioscrypt Fingerprint Biometric readers (number 0 only).

Toolbar Shortcut

1. Open Alarm Monitoring and display the System Status window by selecting **View** > **System Status** and then the desired window.
2. Right-click the device in the hardware view and select **Download Database, Download Firmware** or **Download Reader Firmware**.

View the Controller Properties

The type of firmware a controller has is indicated in the firmware revision reported in the Alarm Monitoring hardware view. It can also be found in the diagnostic tab of the access panels folder in System Administration and in the main window of the Controller Encryption Configuration Utility, which can be found in the ReadykeyPRO directory.

Note: If the firmware on the LNL-500, LNL-1000, and LNL-2000 controllers is not up to the latest version that is in the release a “[Not current]” tag will be noted on the firmware version string.

The flash chip size is indicated in the Alarm Monitoring controller properties dialog box, which you get to by right-clicking on the controller and selecting properties. It can also be found in the diagnostic tab of the access panels folder in System Administration.

Note: If the current firmware revision in the controller is older then 3.041 the controller will not report its flash size and it will not be indicated in any utility.

The current DIP switch settings for a given controller are indicated in the Alarm Monitoring controller properties dialog box, which you get to by right-clicking on the controller and selecting properties. It can also be found in the Diagnostic tab of the access panels folder in System Administration.

RKP-2000 and RKP-3000 boards show the Communications Path Status, which indicates which of their dual path connections are active. The value of this status can be either Primary or Secondary/Failover. The secondary connection is only used when a problem with the primary problem has occurred. This status can also be seen in the System Status Tree of the controller.

There is an additional property, Selective Cardholder Download, which is either enabled or disabled in the controller properties of an Access Panel. If you update the selective download configuration in System Administration, you can perform an Update Hardware Status in Alarm Monitoring to see the changes.

View Notes

Some hardware devices may have notes that were entered in System Administration. This is available for access panels, fire panels, intercom devices, personal safety devices, receivers, intrusion panels, Crestron PLC, POS devices, SNMP managers, readers, elevator dispatching devices, video recorders, and cameras.

To view the device notes:

1. Select the device and right-click on it. Or, if there is an alarm, right-click on the alarm.
2. A popup menu is displayed. If there are no notes, the option will be disabled and labeled with **(None)**. Otherwise, there are a few possible menu options:
   a. Select the **View Controller Notes** option from the popup menu (for devices that are access panels, fire panels, intercom devices, personal safety devices, receivers, intrusion panels, Crestron PLC, POS devices, SNMP managers, video recorders, or elevator dispatching devices).
   b. If the device you selected is a reader, select **View Reader Notes**.
   c. If the device you selected is a camera, select **View Camera Notes**.
   d. If you selected an alarm, select **View Device Notes**. If there are associated devices containing notes, they will be shown in a new popup window. Select a device to show the corresponding notes.
3. The Notes window is displayed. These notes are read-only. Click [OK] when you are done to exit.

Chapter 6: Trace Alarms and Events

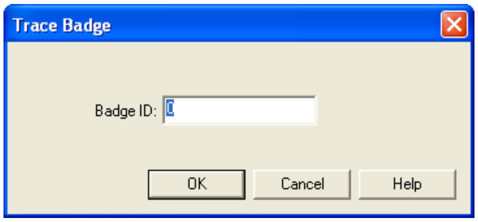
ReadykeyPRO allows you to trace the alarms and events associated with a monitor zone, controller, device, badge, asset or area. This includes events from third party DataConduIT sources.

Note: Trace permissions for a Monitor Permission Group are set in System Administration or ID CredentialCenter in **Administration** > **Users** > Monitor Permission Groups tab > Monitor sub-tab.

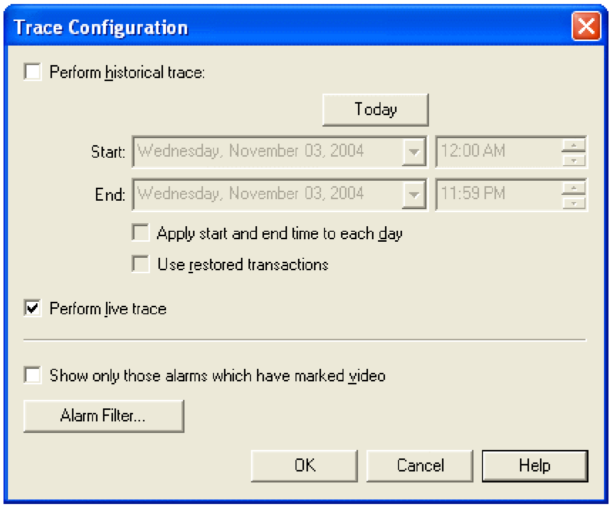
Trace Configuration Window Overview

The Trace Configuration window performs live and historical traces of events and is displayed by:

- Selecting the **Trace** menu and then the type of device you wish to trace. Click [OK] when ReadykeyPRO prompts you to verify the name of the device to be traced.
- Right-clicking an alarm and selecting **Trace** and then the device you wish to trace.
- If tracing a badge you are first introduced with the following dialog box. Type the badge ID you wish to trace and click [OK].



Trace Configuration Window



Trace Configuration

☐ Perform historical trace:

Start: Wednesday, November 03, 2004 12:00 AM

End: Wednesday, November 03, 2004 11:59 PM

☐ Apply start and end time to each day

☐ Use restored transactions

☑ Perform live trace

☐ Show only those alarms which have marked video

Trace Configuration Window

Field	Description
Perform historical trace	If the check box is selected, the trace will include events that occurred between the **Start** and **End** date/times you specify.
Today	When clicked, the **Start** and **End** fields populate with the following: • Start and End date: the current day’s date • Start time: 00:00 on the current date • End time: 23:59 on the current date
Start	The first date/time combination that the trace displays events for
End	The last date/time combination that the trace displays events for
Apply start and end time to each day	If the check box is selected, the time range is applied to each day within the date range. For example: A trace has a **Start** date/time of 12/1/2003 9:00 and an **End** date/time of 12/9/2003 17:00. • If the **Apply start and end time to each day** check box is checked, then the trace will include only those events that occurred during the hours of 9:00 a.m. through 5:00 p.m. on the days December 1st through December 9th, 2003. • If the **Apply start and end time to each day** check box is not checked, then the trace will include all events that occurred from 9:00 a.m. on December 1st until 5:00 p.m. on December 9th.
Use restored transactions	This option is applicable only when a historical trace is performed. • If the check box is selected, restored transactions will be included in the historical trace. • If the check box is not selected, normal transactions from the EVENTS table will be used for the historical trace.

Trace Configuration Window (Continued)

Field	Description
Perform live trace	Controls whether new events are displayed or not • If the check box is selected, the trace displays new events. • If the check box is not selected, live tracing is disabled and new events are excluded from the trace.
Show only those alarms which have marked video	Controls whether alarms (events) that have marked video are displayed or not. • If the check box is selected, live tracing shows events that are new AND are configured (in the System Administration application) to have video marked for them. The marking is not instant, so the trace may not show the 🎥 icon in front of the event right away. • When the **Show only those alarms which have marked video** check box is checked and the **Perform historical trace** check box is checked, the trace will show events which have video marked for them, regardless of the current alarm-video configuration in the System Administration application. This means that a video-only trace may exclude some alarms seen in the main alarm view with a 🎥 icon in front of them.
Alarm Filter	Enables you to configure the type of events that will be displayed for a trace. When clicked, the Alarm Filter window opens.
OK	Performs the trace using the settings selected and closes the Trace Configuration window. A Trace Monitor window will open, which looks identical to the Main Alarm Monitoring window, but displays only those alarms that are associated with the trace criteria specified.
Cancel	Cancels the pending requested action.
Help	Displays help for this topic.

Procedure for Tracing

Trace Alarms and Events

ReadykeyPRO allows you to trace the alarms and events associated with a monitor zone, controller, device, badge, asset or area. This includes events from third party DataConduIT sources.

1. Select (highlight) an alarm, event or device you want to trace.
2. Do one of the following:
   - Right-click and select **Trace**. Then select **Controller**, **Device**, **Badge**, **Asset** or **Area**.
   - From the **Trace** menu select **Controller**, **Device**, **Badge**, **Asset** or **Area**.
   - Click the toolbar button that corresponds to what you want to trace. Choices include:

	Traces a Controller

	Traces a Device (including alarm outputs, reader aux inputs and reader aux outputs)
	Traces a Badge

Note: If you are tracing a badge the Trace Badge window displays asking you to verify the Badge ID. Click [OK].

3. The Trace Configuration window displays.
4. To perform a historical trace, select the **Perform historical trace** check box and select the **Start** and **End** dates.
   - **Optional** - You can also select the **Apply start and end time to each day** or the **Use restored transactions** check box.
5. To perform a live trace, select the **Perform live trace** check box.
   - **Show only those alarms which have marked video** check box unchecked
6. To view only alarms with video select the **Show only those alarms which have marked video** check box.
7. Click [Alarm Filter] to select the types of events that will be displayed for this trace.
8. In the Alarm Filter window, select (place a checkmark beside) the alarm types you want displayed.
9. Click [OK].
10. In the Trace Configuration dialog, click [OK].
11. ReadykeyPRO will open a new Trace Monitor window that looks identical to the Main Alarm Monitoring window, but only displays alarms that are associated with the trace.

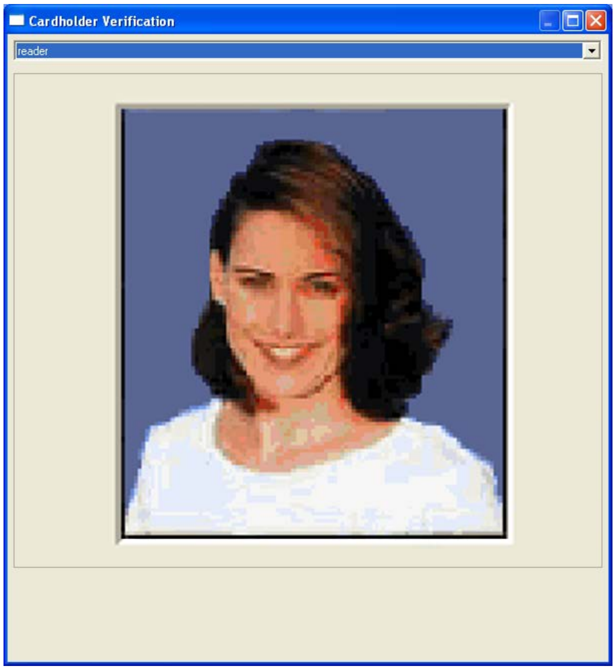
Chapter 7: Cardholder Verification

Cardholder verification is the process of viewing a cardholder's photo "live" (as the cardholder is badging through a reader). When a cardholder swipes a badge through a reader, that user's photo is displayed in the Cardholder Verification Configuration window. You can use cardholder verification to compare the cardholder's photo to that of the person using the reader.

The Cardholder Verification window can be displayed by clicking **View** > **Cardholder Verification**.

If the Cardholder Verification window is open when the Alarm Monitoring application is closed then the Cardholder Verification window will open automatically next time the application is launched.

Cardholder Verification Window



Form element	Comment
Reader drop-down box	Choose a reader from this drop-down box to view the cardholder images from the badge being used.

Cardholder Verification Procedures

The following procedures explain how to set up Cardholder Verification.

Set up Cardholder Verification

1. In Alarm Monitoring, click **View** > **Cardholder Verification**. The Cardholder Verification window opens.
2. In the drop-down box, select the reader whose cardholders you would like to view.
3. As the cardholder badges through the selected reader their photo will appear in the Cardholder Verification window.
4. Repeat steps 1-3 to open multiple Cardholder Verification windows to cover multiple readers at once.

Chapter 8: Control Devices and Areas

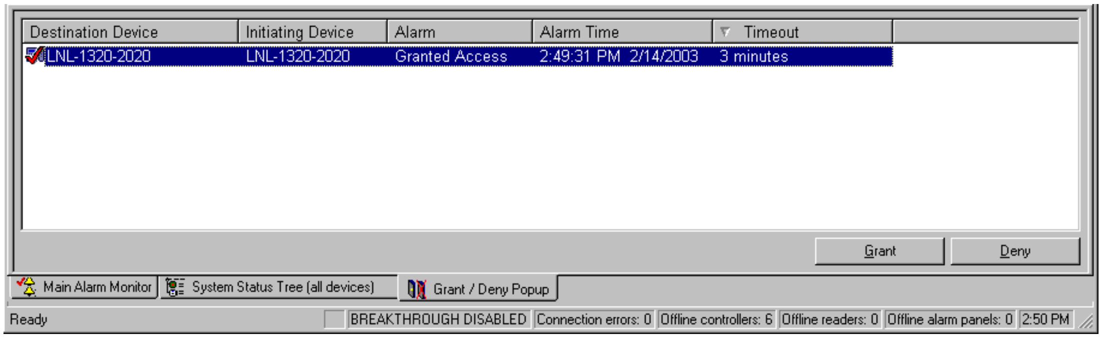
Permissions for control device groups can be given or restricted through System Administration. From the **Administration** menu select **Users**. On the Monitor Permission Groups sub-tab there is a Control Device Groups sub-tab with which you can control access to device groups.

Grant / Deny Pop-up Window

Your System Administrator can configure any input event for any device to execute an output action that launches a grant/deny pop-up window associated with a door/reader. Alarm Monitoring operators with the correct permissions can either grant or deny access through the door/reader. When a grant is issued the door is pulsed open. When a deny is issued, no command is sent.

Note: For configuration procedures refer to the Global I/O Folder chapter in the System Administration User Guide.

Alarm Monitoring stations and operators monitoring the same zone the input device/event and output device/event are configured for are notified when the input event occurs.



Destination Device	Initiating Device	Alarm	Alarm Time	Timeout
LNL-1320-2020	LNL-1320-2020	Granted Access	2:49:31 PM 2/14/2003	3 minutes

Ready | BREAKTHROUGH DISABLED | Connection errors: 0 | Offline controllers: 6 | Offline readers: 0 | Offline alarm panels: 0 | 2:50 PM

Field	Description
Display area	Displays any and all active requests. The display window contains the following columns: • **Destination Device** - The door/reader the output action will affect. • **Initiating Device** - The device the request is coming from. **Note:** Both the initiating device and destination device must be in the same monitor zone. • **Alarm** - The input event that is linked to an output action. • **Alarm Time** - The time the request was initiated. • **Timeout** - The total amount of time the operator has to either grant or deny the request. The timeout value is user-defined with a default value of 3 minutes. This field does not refresh. To determine the amount of time remaining the operator must also refer to the Alarm Time column. The current time located in the status bar determines when the request was initiated.
Grant	Grants the request (pulses open the door) and removes the request from the Grant / Deny pop-up window.
Deny	Denies the request (no command is issued to the hardware) and removes the request from the Grant / Deny pop-up window.

Grant / Deny Pop-up Window Procedures

Grant or Deny Access

1. Verify the Communication and Linkage Server are running. To do this, click the Start button then select **Programs** > **ReadykeyPRO Unlimited** > **Communication Server** or **Linkage Server**.
2. To grant access, complete one of the following when the Grant / Deny pop-up window displays:
   - Double-click a request.
   - Right-click a request and select **Grant**.
   - Select (highlight) a request and click [Grant].

Note: You must have the open door user permission in order to issue a grant. Contact your System Administrator to set up this permission or refer to the Users Folder chapter in the System Administration User Guide for procedures.

3. To deny access, complete one of the following when the Grant/Deny pop-up window displays:
   - Let the timeout value expire by doing nothing.
   - Right-click a request and select **Deny**.

- Select (highlight) a request and click [Deny].

Note: A user transaction is logged when a grant or deny occurs.

Right-click Options to Control Devices and Areas

You can control devices and areas through a wide variety of right-click and left-click menu options available in Alarm Monitoring. You can right-click and left-click icons in map view, right-click alarms, right-click device groups as well as right-click and left-click hardware in the System Status window. The menu options available when you right-click or left-click depend on the window you are in and the device or area you are clicking on.

Some right-click and left-click menus contain sub-menus. To execute commands you must first select the device from the right-click or left-click menu. A sub-menu of options displays to control that device.

Note: Many of the right-click and left-click options are also available as options from the main menu.

General Right-click Options

These right-click options can be available for alarms as well as multiple devices/ hardware.

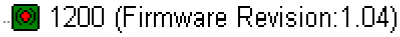
- **Acknowledge** - acknowledges the currently selected alarm.
- **Trace** - traces the selected device.
- **Update Hardware Status** - polls currently selected access panel/controller and updates the hardware status. If a downstream device (like a reader) is selected, the update hardware status is done for the controller associated with that device.
- **View Map** - displays a map associated with the selected device (if one exists). If more than one map exists, the user is prompted to select a map.
- **Launch Video** - displays video for the selected device if a camera is associated with the device.

Monitor Zone Right-click Options

- **Update All Hardware Status -** updates the display to show the currently status of all devices.
- **Set All Controller Clocks** - sets all clocks to the current system time.
- **Trace Monitor Zone** - traces a monitor zone.

Access Panel and Alarm Panel Right-click Options

- **Properties** - available for access and intrusion panels.
- **Open Door(s)** - opens the door(s) associated with the selected access panel. If using Recognition Source readers this option will not be available, because these specific readers are not in constant communication with the PIM devices.
- **Set Controller Clock** - sets selected access panel/controller clock to current time. If a device other than an access panel/controller is selected, this option sets the clock on the access panel/controller to which the device is attached.
- **Reader Access Modes** - updates the reader mode of every reader associated with selected access panel/controller or reader.
  - **Card and Pin**: Sets the reader to card and pin mode.
  - **Card Only**: Sets the reader to card only mode.
  - **Pin or Card**: Sets the reader to pin or card mode.
  - **Cipher Lock Emulation**: Sets the reader to cipher mode requiring a master combination or “cipher code”.
  - **Facility Code Only**: Sets the reader to facility code only mode.
  - **Locked**: Locks the reader.
  - **Unlocked**: Unlocks the reader.
  - **Default**: Sets the reader to the default online mode that it is configured for in the database.
  - **Lock Door -** NGP only. Select to lock both the in and out reader.
  - **Unlock Door -** NGP only. Select to unlock both the in and out reader.
  - **Reinstate Door -** NGP only. Select to put both the in and out reader into a locked state until the proper credentials are presented putting the reader into the last known access mode.
- **Reader Verify Mode** - used to enable or disable verify mode for access control readers with an associated secondary reader. When verify mode is enabled, access to both the primary and secondary reader is required. When verify mode is disabled, only access to the primary reader is required.
- **Activate** - activates the outputs associated with the selected access panel.
- **Deactivate** - deactivates the outputs associated with the selected access panel.
- **Pulse** - pulses all outputs associated with the selected access panel.
- **Mask** - masks inputs or alarms for the currently selected reader.
- **UnMask** - unmasks inputs or alarms for the currently selected reader.
- **Download Firmware** - downloads firmware to the selected controller, RKP-1100 or RKP-1200 alarm panel or RS-485 command keypads. Controllers and gateways display firmware revision numbers using three decimal places, while downstream devices display the firmware revision number using two.



1200 (Firmware Revision:1.04)

- **Download Database -** downloads the database to the access panel/controller.
- **Download Encryption Keys -** downloads the encryption keys to the panel and from the panel to any connected devices over an RS-485 connection. Encryption keys can only be transferred over an encrypted connection. This option is available for RKP-3300 and RKP-2220 panels only.

- **Reset Use Limit -** resets the number of times a badge can be used on a particular access panel/controller.
- **Connect -** connects the access panel/controller via a dialup/modem connection.
- **Disconnect -** connects the access panel/controller via a dialup/modem connection.

Intrusion Area Right-click Options

- **Disarm** (all intrusion controllers) - Disarms the area.
- **Perimeter Arm** (Detection Systems only) - Arms the perimeter of an area.
- **Arm Entire Partition** (Galaxy and Detection Systems only) - Arms the perimeter and interior points of an area.
- **Partial Arm** (Galaxy only) - Arms only the zones marked for partial set in the controller.
- **Master Arm Delay** (Bosch only) - Arms the perimeter and interior points with exit and entry delays.
- **Master Arm Instant** (Bosch only) - Instantly arms both the perimeter and interior points.
- **Perimeter Delay Arm** (Bosch only) - Arms the perimeter with exist and entry delays.
- **Perimeter Instant Arm** (Bosch only) - Instantly arms the perimeter points.

Intrusion Panel Right-click Options

In addition to the acknowledge, trace, update hardware status, properties and set controller clock right-click options, intrusion panels and relays can also have the following right-click option.

- **Execute Custom Function** - executes a custom function associated with the Bosch Intrusion Controller. This menu option is only available with Bosch Intrusion Controllers.

Intercom Right-click Options

- **Place Call** - displays a dialog box where you enter the station number you are calling to.
- **Call Intercom** - places a call using the intercom station configured in **System Administration > Monitoring > Monitor Zones**, and then selecting the **Monitor Stations** tab.

Note: Calls made using the Call Intercom function are always assigned Low Priority or Priority 0.

- **Cancel Call** - cancels the intercom call.
- **Badge Information -** displays badge information associated with the intercom event; who placed the call and/or who received the call. If an intercom event has two intercom stations associated with it (the station that placed the call and the station that received the call) a dialog displays,

allowing alarm monitoring operators to select the intercom station(s) they want to base the cardholder search on.

Note: The Badge Information right-click option is only available for intercom stations linked with the customized cardholder field, Cell number. For more information, refer to the Cardholder Options folder - Automatic Lookup form in System Administration.

Ericsson MD110 Intercom Right-click Options

Note: The Ericsson MD110 allows calls to be queued. If a call is queued, a Call Queued alarm is sent to Alarm Monitoring.

- **Place Call** - displays a dialog box where you enter the station number you are calling to.
- **Cancel Call** - cancels the intercom call.
- **Cancel all Calls** - cancels all calls.
- **Block Station** - blocks the station from receiving a call.
- **Unblock Station** - lets the station receive calls again.
- **Divert This Call** - for a call that has been queued. Displays a dialog box that allows you to divert the call to another station. That station will then receive a ringing alarm, which you then handle as normal.

Intrusion Door Right-click Options

Bosch is the only intrusion controller that supports doors.

- **Open Door** - Opens the door for the selected intrusion panel.
- **Door Mode** - Changes the current door mode.
  - **Lock -** Locks a door and requires a proper user ID to allow access.
  - **Unlock -** Unlocks the door allowing free access to everyone.
  - **Secure -** Locks the door prohibiting access for anyone.

Intrusion Relay Right-click Options

The information in this section applies to both onboard and offboard relays except where noted otherwise.

- **Activate** - Activates the outputs associated with the selected intrusion panel.
- **Deactivate** - Deactivates the outputs associated with the selected intrusion panel.
- **Toggle** - Puts the output in the opposite state of the current state. For example, if the output is currently set to activate then this command will set the output to deactivate. This command is available for Bosch Offboard relays only.

Intrusion Zone Right-click Options

- **Bypass** - Masks the zone from reporting alarm or tamper activity.
- **Unbypass** - Unmasks the zone so that any tamper or alarm activity for the zone will be reported.

Reader Right-click Options

In addition to several options listed in Access Panels and Alarm Panels, right-click options for readers also include:

- **Download Reader Firmware** - downloads firmware to the selected dual interface Rdr1 reader. Displays the major and minor firmware revision number. The minor firmware revision number displays as the last two digits.
- **Reader Biometric Verify Mode** - enables/disables verify mode for access control readers with an associated biometric reader. When verify mode is enabled, the normal card and/or pin access and a biometric match is required. When verify mode is disabled, only the card and/or pin access is required.
- **Reader First Card Unlock Mode** - enables/disables the Reader First Card Unlock Mode. The Reader First Card Unlock Mode is a qualifier for online Reader Mode. When enabled, the online Reader Mode is in effect until the first (qualified) access granted with entry occurs. When the first access granted with entry occurs, the online Reader Mode changes to unlocked.

Note: Reader First Card Unlock Mode is only supported on the RKP-2000 controller. However, first style unlock behavior can be configured for use with any access controller through Bosch’s Global I/O Support.

Reader Group Right-click Options

- **Secure All** - locks all doors in the reader device group and sets all readers to the locked mode.
- **Unsecure All** - unlocks all doors.in the reader device group that were previously secured, and sets all readers to the unlocked mode.
- **Reader Access Modes** - sets all readers in a reader device group to a specified reader access mode.

Note: Only reader access modes which are supported by the entire group will be available.

For example, Unlocked and Card Only will be the available modes for the following group of readers:

- Reader 1 (Unlocked, Card Only, Secured, Unsecured)
- Reader 2 (Unlocked, Card Only, Card and Pin, First Card Unlock)
- Reader 3 (Unlocked, Card Only, Secured, Unsecured)

Alarm Mask Group Right-click Options

- **Group Mask** - masks inputs or alarms for the currently selected reader.
- **Group Unmask** - unmasks inputs or alarms for the currently selected reader.

Intrusion Mask Group Right-click Options

- **Disarm/Reset** - Disarms the Intrusion Mask Group. If the intrusion mask group is armed it will transition to be disarmed if no alarm is made. If the intrusion mask group was in an alarm state, it will transition into an alarm cancelled state until the same command is executed again to transition it into a disarmed state.
- **Arm Away** - Arms all points of the mask group. Any point activation will either trigger an alarm or start the entry or exit delays. Exit delays start at the time arming occurs, and allows exit through trigger points for the user set duration.
- **Arm Stay** - Arms the perimeter points of the mask group but does not arm the points defined as interior. This mode allows movement inside the protected area, but will trigger an entry delay and subsequent alarm if any perimeter point is activated. Exit delays start at the time arming occurs, and allows exit through trigger points for the user set duration.
- **Arm Stay Instant** - Arms the perimeter points of the mask group but does not arm the points defined as interior. This mode allows movement inside the protected area but will trigger an entry delay and subsequent alarm if any perimeter point is activated. There is no exit delay.
- **Restore All Points** - Removes bypass settings for all points in the intrusion mask group.

Function List Right-click Options

Function Lists are keypad - activated commands that are programmed into an access panel. Function lists can be accessed by assigning them to specific keypad sequences.

- **Execute: True** - sets the logic term to true.
- **Execute: False**- sets the logic term to false.
- **Execute: Pulse** - temporarily sets the logic term to true.

Action Group Right-click Options

In addition to the view map option, action groups also include execute as a right-click option.

Note: Action groups will display if the logged in user has the segment access to the action group along with permissions to execute all of the actions in the action group.

Anti-Passback Area Right-click Options

These right-click options are unique to areas and area alarms. There are other right-click options available for areas and they are listed in General Options.

- **Update Area Status** - updates the status of both safe and hazardous areas so that operators can have a current view of cardholder locations.
- **Occupancy Report** - provides a current report of the cardholders currently in a safe area.
- **Move Badges** - enables an operator to manually move all the badges from one area to another.
- **Mustering Report** - provides a current report of the cardholders currently in a hazardous area.
- **Start Muster Mode** - initiates Muster mode. The Start Muster Mode window displays and provides an area to enter comments.
- **Reset Muster Mode** - ends Muster mode. The Reset Muster Mode window displays and provides an area to enter comments.

Guard Tour Right-click Options

These right-click options are available if Guard Tour is set up in your system.

- **Launch Tour** - starts a guard tour.
- **View Tour** - displays the guard tour live tracking window for a specific tour.
- Remote Monitor Right-click options

In addition to several options listed in Access Panels and Alarm Panels, right-click options for Remote Monitors also include:

- **Launch Video** - launches the local monitor window in Alarm Monitoring.
- **Download Database** - synchronizes the RM with the camera channels assigned in Alarm Monitoring.
- **Remove All** - removes all video from the RM.
- **Matrix** - switches the RM to matrix view.
- **Single** - switches the RM to single player mode.
- **Next** - in single player mode, selects the next video cell in the list.
- **Prev** - in single player mode, selects the previous video cell in the list.
- **Live** - changes to live video on each video cell in the RM.
- **Recorded** - changes to recorded video on each video cell in the RM.
- **Pause** - pauses the video playback on each video cell.
- **Play** - resumes the video playback on each video cell.
- **Stop** - stops the video playback on each video cell.
- **Frame Advance** - advances one video frame on each video cell.
- **Fast Forward End** - fast forwards to the end on each video cell.

Remote Monitor Video Cell Right-click Options

In addition to several options listed for Remote Monitors, these right-click options are available for video cells assigned to Remote Monitors (RM):

- **Launch Video** - launches video on the RM and the local monitor window in Alarm Monitoring.
- **Remove** - removes the video cell from the RM.
- **Select** - in matrix view, changes to single player mode with the selected video cell.

Elevator Terminal Right-click Options

These right-click options are available if elevator dispatching is configured in your system:

- **Set Allowed Floors** - updates which floors and doors are accessible via the elevator terminal without supplying security credentials.
- **Elevator Terminal Modes** - updates the elevator terminal's operational mode for interacting with the cardholder.
  - **Default Floor Only:** When the cardholder presents a valid badge to the elevator reader, or enters a valid PIN code or floor number on the DEC (elevator terminal), the system calls the default floor.
  - **Access to Authorized Floors:** When the cardholder presents a valid badge to the elevator reader, and then selects an authorized floor, the system calls the authorized floor.
  - **User Entry of Destination Floor:** The cardholder has the option to select a floor with or without presenting their badge to the elevator reader. If the selected floor is an allowed floor, the system calls the floor. If the floor is a non-allowed floor, the cardholder is requested to present their badge.
  - **Default Floor or User Entry of Destination Floor:** When the cardholder presents a valid badge to the elevator reader, the system calls the cardholder's default floor. Within a configurable timeout period, the cardholder can override the default floor call by entering another floor number.

Single and Double Left-click Mode

Each Alarm Monitoring operator can set their options so that commands are executed with a single left-click or a double left-click of an icon in the system status view or map view. The default setting is to execute commands with a double left-click.

Furthermore, if that command was previously available as a right-click menu option, then the command will be listed in bold when the device is right-clicked. For some menus, the default command may be in a sub-menu of the context menu. The example that follows shows the **Reader Auxiliary Output # 2** in bold. This is the command that will be executed when the operator single or double left-clicks the controller icon, depending on how they have set their options.

Note: Using the System Administration application your System Administrator can associate commands with a device or area icon so that when the icon is single or double left-clicked in Alarm Monitoring, the command is executed. For information on how to associate a command with a device or area icon, refer to the Monitoring Options Folder Chapter in the System Administration User Guide.

Activate Single or Double Left-click Mode

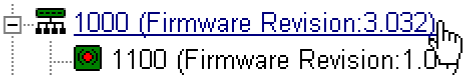
Single or double left-click mode is configurable per user. To activate single left-click mode select (place a checkmark beside) the **Execute Command on Single Click of Icon** in the **Options** menu of Alarm Monitoring. While in this mode you can single left-click an icon in the Alarm Monitoring system status and map view to execute the command configured for that device or area.

To activate double left-click mode deselect (there is no checkmark beside) the **Execute Command on Single Click of Icon** in the **Options** menu of Alarm Monitoring.

Select a Device in Single or Double Left-click Mode

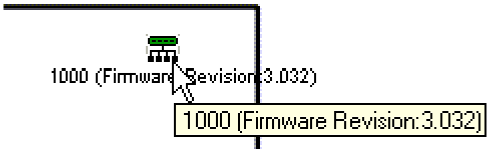
Single Left-click Mode

In single left-click mode you can select a device, by placing or hovering the cursor near the device without left-clicking. The system status list and tree view identifies a selected device by underlining and/or highlighting the device.



1000 (Firmware Revision:3.032)
1100 (Firmware Revision:1.0

The map view identifies a selected device by displaying the tool tip.



1000 (Firmware Revision:3.032)
1000 (Firmware Revision:3.032)

Double Left-click Mode

To select a device in double-click mode, left-click the device.

Execute a Command in Single or Double Left-click Mode

Single Left-click Mode

To execute a command in single left-click mode, left-click the device. Clicking the expand symbol in tree view does not execute the command.

Double Left-click Mode

To execute the command, double left-click the device.

Note: If you are in double left-click mode in the System Status view, not only do you execute the command when you double left-click a device, but you also expand or collapse the hardware list.

Chapter 9: Monitor Alarms

When an alarm occurs, it displays in the Main Alarm Monitoring window. Each alarm displays in its own row and is preceded by a colored dot. If alarms are configured in the System Administration software so that they do not automatically delete after they are acknowledged, an alarm icon will also display beside the colored dot after it is acknowledged.

Alarm Icons

The following table is a list of the different types of alarm icons.

Icon	Description
✓	Alarm acknowledged without notes.
📝	Alarm acknowledged with notes.
🟢	Green colored dot indicates a restored alarm.
🟢🟢	Two green colored dots indicate a restored alarm from a secondary channel connection.
🔴	Red colored dot indicates an active alarm.
🔴🔴	Two red colored dots indicate an active alarm from a secondary channel connection.
🟦	Outstanding acknowledgment action is associated with the alarm. An *acknowledgment action* is an action that will automatically be carried out when the alarm is acknowledged.
📹	Camera is associated with the device that the alarm occurred on/for. Therefore you can pull up live video via the **Launch Video** right-click menu option.
✓📹	Alarm acknowledged without notes and a camera is associated with the device.
📝📹	Alarm acknowledged with notes and a camera is associated with the device.
🟦📹	An outstanding acknowledgment action is associated with the alarm and a camera is associated with the device.
📹	Digital video associated with the alarm has been marked.
✓📹	Alarm acknowledged without notes and has archived video.

Icon	Description
🎥	Alarm acknowledged with notes and has archived video.
🎥	Outstanding acknowledgment actions and archived video.
✓	Alarm marked in progress.

Pending Alarms Window

The Pending Alarms window is similar to the Main Alarm Monitoring window in that it has the same menu options and toolbars. However, the Pending Alarms window only displays *pending alarms,* which are alarms that are configured to require an operator to take action. Pending alarms are highlighted in the Main Alarm View and cause Alarm Sprites to be shown on graphical maps for the devices associated with those pending alarms.

Alarms are configured to be pending alarms in the Alarm Definitions Form in System Administration. If events configured here are set to be “active” then their corresponding alarm will be highlighted in Main Alarm Monitoring window. For more information see the Alarm Configuration Folder chapter in System Administration.

An example of a pending alarm can be anything depending on the configuration done in System Administration. Commonly though, higher need alarms such as a door being forced open are reserved for this type of immediate action.

An initiating alarm is automatically deleted upon arrival of its corresponding canceling alarm. (e.g. Door Forced Open/Door Forced Open Cancelled).

If the Pending Alarms Window is left open, the window automatically updates itself. For example, when a pending alarm is acknowledged in the Main Alarm Monitoring window, it immediately ceases to display in the Pending Alarms window.

If a pending alarm is an initiating alarm that becomes physically restored and must be acknowledged, it continues to display as a pending alarm until it is acknowledged. If a pending alarm is an initiating alarm that becomes physically restored but does not require acknowledgment, the alarm ceases to be a pending alarm.

Like the Main Alarm Monitoring window you can determine the type of information displayed about alarms through the **Configure** > **Columns** menu option. However, you cannot filter the type of alarms displayed through the **Configure** > **Alarm Filter** menu option. That is because the Pending Alarms window is intended to summarize ALL pending alarms.

Toolbar Shortcut

🔔

To display the window, select the **Pending Alarms** option from the **View** menu or click the View Pending Alarms toolbar button.

To view tables of the menu items and toolbar options, refer to Menus and Toolbars on page 39.

Procedure for Monitoring Alarms

Sort Alarms

Alarms are listed in the order indicated by the sort criterion. To determine the current sort criterion locate “Sort criteria” in the status bar (lower right side of the screen).

You can rearrange the order of existing and new alarms using either of these two methods:

- Clicking a column heading
- Selecting **View** > **Sort by** from the Main Alarm Monitoring menu.

The choices available in the **Sort by** submenu are:

Column name	Description
Alarm Description	Lists alarms alphabetically by alarm description.
Account Group	Lists alarms in order of receiver account group (panels). Receiver accounts are used to represent panels in a receiver setup.
Asset Name	List alarm alphabetically by asset name.
Asset Scan ID	Lists alarms in order of asset scan ID.
Associated Text	Indicates (Yes or blank) whether there is additional text associated with the alarm.
Badge Type	Displays the badge type associated with the alarm.
Biometric Score	Lists alarms in order of biometric score. A biometric score is based on how well a biometric access control reader matches a template in the database. By default, this sort option is not enabled. To enable this sort option, the “Biometric Score” column must first be added via the **Configure** > **Columns** menu option in Alarm Monitoring.
Card	Lists alarms numerically by the card number (badge ID), if the alarm is associated with a cardholder.
Controller	Lists alarms alphabetically by name of the controller with which the alarms are associated.
Controller Time	Lists alarms in order of controller time. The time includes the hour and minute and the date includes the month, day and year. The display is based on the time zone setting selected in the Control Panel of your computer. Typically the display is adapted to the country in which you are located.
Device	Lists alarms alphabetically by name of the device associated with the alarm. If the alarm originates at a video recorder, the recorder name displays.
Input/Output	Lists alarms alphabetically by name of the alarm input, if the alarm is generated at an alarm input.
Intercom Station Called	Lists alarms in order of intercom station called.

Column name	Description
Intrusion Area	Indicates the name of the area associated with the alarm. This is only displayed when the controller reported an area number along with the alarm.
Line Number	Displays alarms in order of line number.
Priority	Lists highest priority alarms at the top of the list, followed by medium priority alarms, with low priority alarms placed at the bottom of the list.
Time/Date	Lists alarms in chronological order. Within a given date (month, day and year) the alarms are sorted by time, which include hours and minutes and optionally seconds. • To view time in seconds go to the **Options** menu and select (place a checkmark beside) **Display Seconds**. • To view the most recent alarms at the bottom of the list, go to the **Options** menu and select (place a checkmark beside) **Ascending Time/Date**. To view the most recent alarms at the top of the list select (place a checkmark beside) **Descending Time/Date**.
Transmitter	Lists alarms in order of transmitter. *Transmitters* are devices that generate either an RF or IR (or both) signal that Visonic SpiderAlert receivers can receive. There are three types of transmitters: fixed, portable (hand-held) and man-down. For more information refer to the Personal Safety Devices Folder chapter in the System Administration User Guide.
Transmitter Input	Lists alarms in order of transmitter input.

For any sort, the second level sort criterion is always **Priority** and the third level criterion is always **Time/Date**. For example:

- If you sort by **Controller**, all alarms associated with the same controller will be sorted by **Priority** then by **Time/Date**.
- If you sort by **Priority**, all alarms with the same priority will be sorted by **Time/Date**.
- If you sort by **Time/Date**, alarms with the same time (to the second)/date will be sorted by **Priority**.

The sort criterion applies to the current window only. You can have one Main Alarm Monitoring window and various Trace windows, each with a different sort criterion. When you open a new Main Alarm Monitoring window, it is initially sorted by Priority.

Chapter 10: Acknowledge Alarms

When you acknowledge an alarm, you provide a software response to it. Your system administrator can configure alarms so they have to or do not have to be acknowledged before they are deleted from the Main Alarm Monitoring window. Furthermore, your System Administrator can associate actions with an alarm so when the alarm is acknowledged an action or group of actions is automatically triggered.

Alarms can be acknowledged from the Main Alarm Monitoring window, the Trace Monitor window, the Pending Alarms window, or the Video Verification window.

Note: An *action* is any task performed by software as a result of an event or schedule.

Alarm Acknowledgment Window

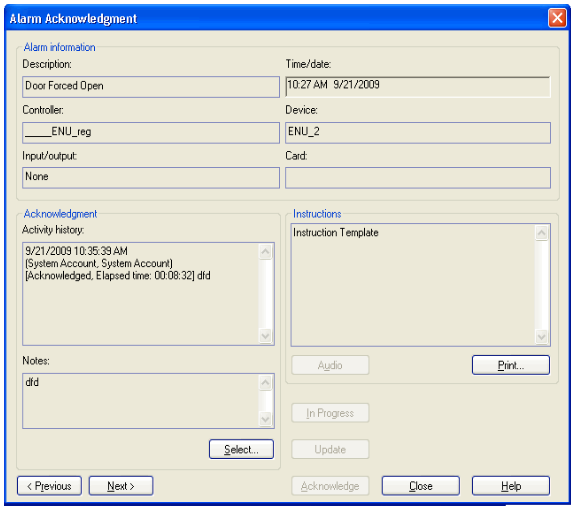
The Alarm Acknowledgment window enables you to:

- Respond (in the software) to an alarm.
- View or listen to stored instructions for a specific alarm.
- Print information pertaining to an alarm.
- Enter or select notes pertaining to an alarm.

The Alarm Acknowledgment window can be displayed several ways:

- Double-click an alarm
- Highlight an alarm entry and from the **Edit** menu select **Acknowledge**

- Right-click an alarm entry and select **Acknowledge**



Alarm Acknowledgment

Alarm information

Description: Door Forced Open

Time/date: 10:27 AM 9/21/2009

Controller: ____ENU_reg

Device: ENU_2

Input/output: None

Card:

Acknowledgment

Activity history:

9/21/2009 10:35:39 AM
(System Account, System Account)
[Acknowledged, Elapsed time: 00:08:32] dfd

Notes: dfd

Instructions

Instruction Template

Alarm Acknowledgment Window

Form Element	Comment
Description	Contains the same name for the alarm as indicated in the Main Alarm Monitoring window.
Controller	Displays the name of the access panel/controller associated with the alarm.
Input/output	If the alarm originated at an input/output device, displays the name of the device.
Time/date	Displays the time and date the alarm occurred.
Device	
Card	
Original notes	Displays any notes carried forward from the associated original alarm.
Notes	Enables you to add your own comments/response to the selected alarm.
Select	Displays a window where pre-configured acknowledgment notes can be selected.
Instructions	Displays pre-configured instructions pertaining to the alarm.
Audio	Plays audio instructions.
Print	Prints the information from this window, including alarm information and any notes entered.
In Progress	Marks the alarm as “In Progress.” This shows that the alarm is currently being checked on but whose source has yet to be determined. If an alarm has been marked in progress, the “Original notes:” control will list the operator that marked the alarm in progress and the date\time this occurred prior to displaying the current notes for that alarm.
Update	Once an alarm has been marked “In Progress” you are able to update the notes for the alarm by clicking [Update] and adding additional notes. Each note is time stamped with the date and time of the update.
Acknowledge	Tells the ReadykeyPRO software to acknowledge the currently selected alarm.

Alarm Acknowledgment Window (Continued)

Form Element	Comment
Previous	Displays information about the previous alarm in the Main Alarm Monitoring window.
Next	Displays information about the next alarm in the Main Alarm Monitoring window.
Close	Closes the Alarm Acknowledgment window.
Help	Displays online assistance for using this window.

Alarm Acknowledgment Procedures

Acknowledge an Alarm

1. Display the Alarm Acknowledgment window by double-clicking an alarm.
2. If the alarm has text instructions associated with it the information displays in the Instructions sub-window. Click [Print] to print the instructions.
3. If the alarm has voice instructions click [Audio].
4. To select pre-configured acknowledgment note(s) click [Select]. The Select Acknowledgment Notes dialog appears. Select the name of the pre-configured note and click [OK].
5. To add notes to the alarm, type your comments and click in the **Notes** sub-window. If this is a canceling alarm, any notes carried forward from the associated initiating alarm gets displayed in the **Original Notes** field.

Note: If your System Administrator has configured the alarm to be marked “in progress” before being acknowledged continue to step 6. If not, move on to step 8.

6. If you are unable to acknowledge an alarm click [In Progress]. This marks the alarm as being “in progress” and acts as a state in between an unacknowledged and acknowledged alarm.
7. One an alarm is marked “In Progress” you are able to update the notes by clicking [Update]. Each update is time stamped with the date and time.
8. Click [Acknowledge] to acknowledge the alarm.
   - If your System Administrator has configured this alarm type for “Require Login On Ack.” you must first log in before this alarm can be acknowledged.
   - If this is an initiating alarm, the corresponding canceling alarm may not be displayed until you acknowledge this alarm. Whether this happens depends upon how your system is set up.
   - Your System Administrator may have set up some types of alarms to be automatically deleted from the Main Alarm Monitoring window after

An initiating alarm is an alarm that ReadykeyPRO automatically deletes when the corresponding canceling alarm occurs.

you acknowledge them. If this is not the case, delete the alarm manually. For more information, refer to Delete an Alarm on page 111.

9. You can acknowledge multiple alarms without closing the Alarm Acknowledgment window. Repeat step 2 through 8 for each alarm you display in the Alarm Acknowledgment window. Use the navigation buttons to move through the list of alarms.

10. To close the Alarm Acknowledgment window, click [Close].

Fast/Group Acknowledge Alarms

The Fast/Group Acknowledge feature allows you to acknowledge a group of alarms simultaneously. This feature can be used without bringing up the acknowledgment dialog box.

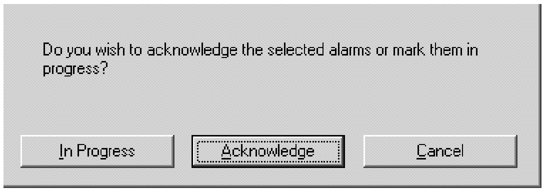
1. Select the alarm(s) that you wish to acknowledge.
    - To choose two or more alarms, hold down the <Ctrl> key while selecting additional alarms.
    - To select all the alarms press <Ctrl> + <F11>.

Toolbar Shortcut

✓

2. Acknowledge the group of alarms by completing one of the following:
    - Choose **Fast/Group Acknowledge** from the **Edit** menu
    - Right-click the selected group of alarms and choose **Fast/Group Acknowledge**
    - Click the Fast/Group Acknowledge toolbar button
    - Press <Ctrl> + <F12>

3. A message displays:



Do you wish to acknowledge the selected alarms or mark them in progress?

4. Click [Acknowledge] to confirm the acknowledgment of the alarms.

Notes: If any of the chosen alarms require notes upon acknowledgment, you will be prompted to enter notes.

If any one of the alarms has already been acknowledged, it cannot be re-acknowledged. A message displays to inform you of how many alarms have been acknowledged. Click [OK] and delete the alarm(s).

The configuration for any given alarm may require that the operator log in upon acknowledging the alarm. If this is the case the user will be prompted to log in.

The configuration for an alarm may also require an acknowledgment password. If this is the case the operator will be prompted only once for the password (for each type of alarm).

Delete an Alarm

1. In the Main Alarm Monitoring window, highlight (click) the alarm you wish to delete.
2. Complete one of the following:
   - Press the <Delete> key.
   - From the **Edit** menu select **Delete**.
3. A confirmation message displays. Click [Yes].

Note: You can also right-click the alarm and select **Delete**. When the confirmation message displays click [Yes].

Delete All Alarms

Depending on how your System Administrator configured alarms, some alarms cannot be deleted until they have been acknowledged. ReadykeyPRO will alert you if this is the case.

1. To delete all of the alarm entries from the current alarm view, select **Delete All** from the **Edit** menu.
2. A confirmation message displays. Click [Yes]. All entries will be removed from the Main Alarm Monitoring window.

Note: You can also delete multiple alarms in the Main Alarm Monitoring window using the <Shift> or <Ctrl> keys and right-clicking. Select the **Delete** option. A confirmation message displays. Click [Yes].

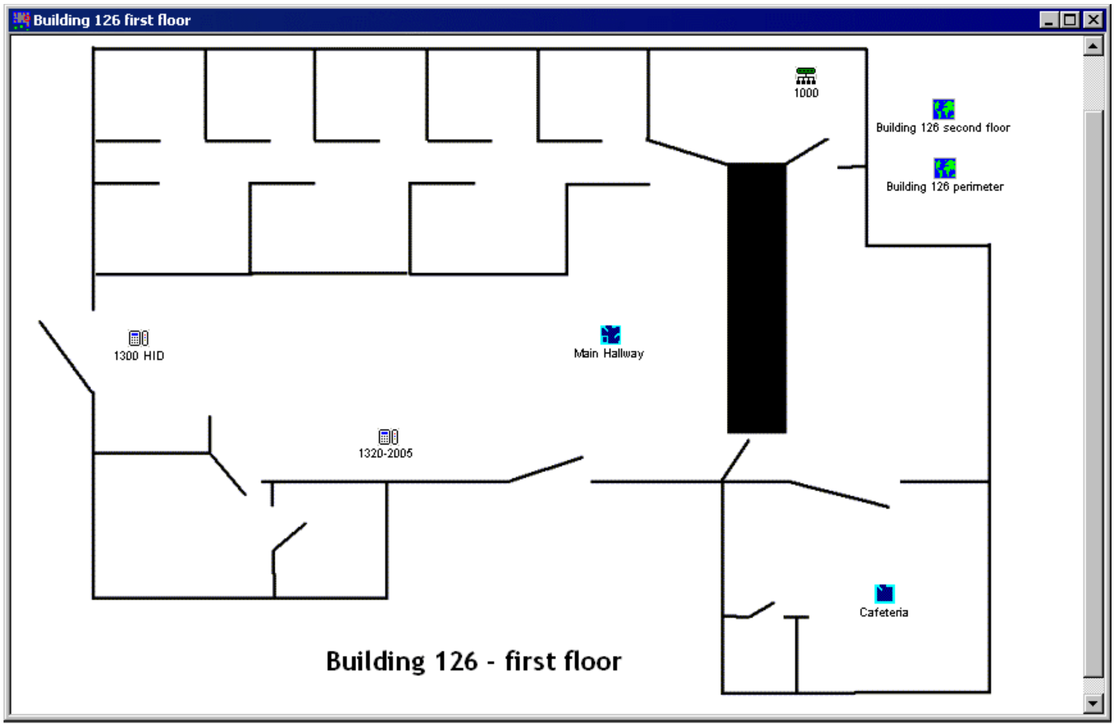
Display a Map

A *monitoring map* is a graphical representation of a facility or area monitored by the ReadykeyPRO system. You can manually view maps associated with an alarm or you can set your display options to automatically display maps when an alarm occurs.

1. To manually display a map, open Alarm Monitoring.
2. If alarms are displayed in the Main Alarm Monitor window, right-click an alarm that has a map associated with it and select **View Map**. Otherwise, with the alarm selected choose **Map** from the **View** menu.
3. If no alarms are displayed in the Main Alarm Monitor window, select **Map Selection** from the **View** menu. Select the desired map and click [OK].

Note: If the selected device has multiple maps associated with it you will be prompted to select a map from a list provided. Do so and click [OK].

Example of a Map



Graphical symbols on the map indicate the location of devices. Using your mouse, scroll over each symbol to view the device status and any text associated with the device. For information on associating text with map icons refer to the MapDesigner User Guide.

Right-click a device symbol to perform a variety of operations depending on the type of device you select.

The word "ALARM" blinks, indicating an alarm's location on the map.

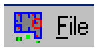
- The blinking alarm displays only if there is one or more alarm designated as an “Active Alarm” in the System Administration software and if these alarms are unacknowledged/undeleted.
- An alarm sprite is a small bitmap image used as an icon. It disappears once the alarm has been acknowledged.
- The alarm sprite disappears if the alarm has been deleted without acknowledgment (as in the case of an initiating alarm that is automatically replaced by a canceling alarm).
- The alarm sprite is not used for canceling alarms.

View Linked Maps

Several maps can be linked to each other using the MapDesigner software application. For more information refer to the “Place Icons on a background” section in the MapDesigner User Guide.

To view linked maps do one of the following:

- If the map that is currently displayed has a link to another map, you can double-click the icon or right-click and select **Switch Map**.
- With a map currently displayed, click the map icon beside the **File** menu option. If you have previously brought up more than one map, a **Back 1 Map** menu option displays. If you go back one map, a **Forward 1 Map** menu option displays.



- From the **View** menu select Map Selection. Highlight a new map and click [OK].

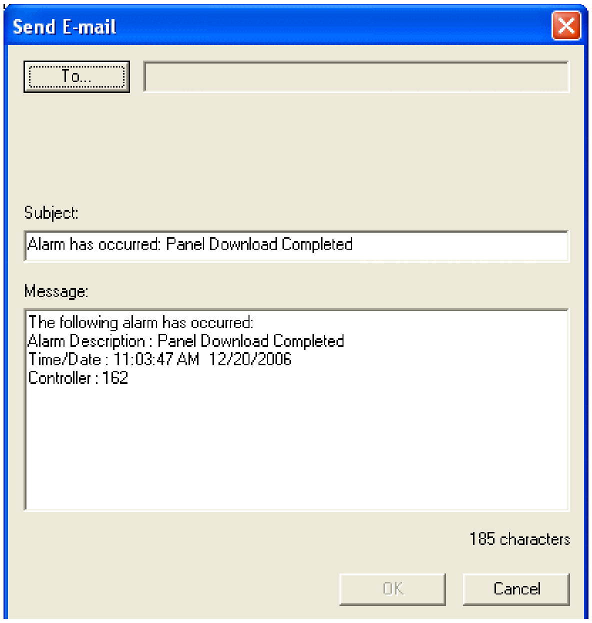
Send an E-mail

Using ReadykeyPRO software you can automatically or manually send electronic mail with alarm information. Contact your System Administrator to automatically send electronic mail for specific alarms.

To manually send an e-mail using Alarm Monitoring:

1. Verify the Global Output Server is running by clicking Start and selecting **Programs** > **ReadykeyPRO Unlimited** > **Global Output Server**.
2. Right-click an alarm and select **Send Email**. The Send Email window opens.
3. Click [To] and select (place a checkmark beside) the desired e-mail addresses. Use the <Ctrl> or the <Shift> key to select multiple addresses.
4. The subject and body of the message are automatically populated with information that describes the alarm. Click in either field to make any changes.

5. Click [OK].



Subject:

Alarm has occurred: Panel Download Completed

Message:

The following alarm has occurred:
Alarm Description : Panel Download Completed
Time/Date : 11:03:47 AM 12/20/2006
Controller : 162

185 characters

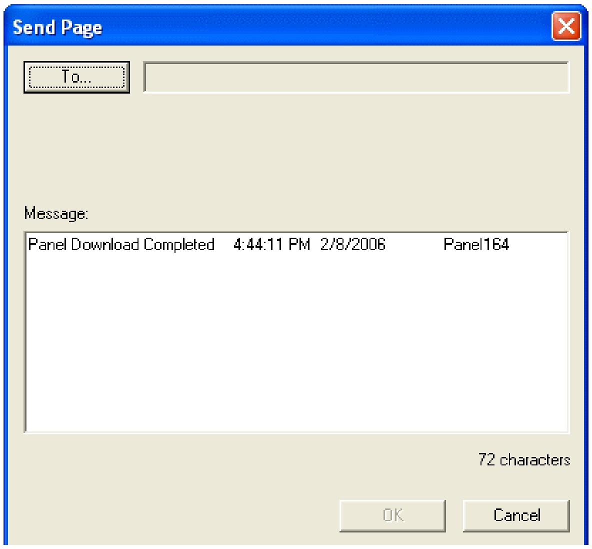
Field/button	Description
To	Allows you to select an e-mail address that is already in the database.
Subject	Displays the subject of the message. By default, the description of the alarm that has occurred is displayed. To change it, type over the text.
Message	Displays the body of the message being sent. By default, information pertaining to the alarm is displayed. To change it, type over the text.
OK	Once you are done, click the [OK] button to send the message and exit the window.
Cancel	To exit the window without sending an e-mail message, click the [Cancel] button.

Send a Page

Using ReadykeyPRO software you can send a page to a recipient with alarm information.

1. Verify the Global Output Server is running by clicking Start and selecting **Programs** > **ReadykeyPRO Unlimited** > **Global Output Server**.
2. Right-click an alarm and select **Send Page**. The Send Page window opens.
3. Click [To] and select (place a checkmark beside) the pager number of the recipient.
4. The message field is automatically populated with an alarm description, the time and date on which it occurred and the location (which reader/alarm panel).

5. Click [OK] to send the page.



Panel Download Completed   4:44:11 PM 2/8/2006   Panel164

Field/Button	Description
To	Allows you to select pager number that is already in the database.
Message	Displays the body of the message being sent. By default, information pertaining to the alarm is displayed. To change it, type over the text.
OK	Once you are done, click the [OK] button to send the message and exit the window.
Cancel	To exit the window without sending a page, click the [Cancel] button.

Chapter 11: Muster Mode

Mustering is a licensed feature that identifies all cardholders in a hazardous location during an incident. When an incident occurs (triggers an alarm) ReadykeyPRO automatically goes into muster mode. System operators can also manually initiate muster mode if necessary.

An *incident* is any situation/emergency where everyone in a hazardous area must evacuate and convene at designated safe locations. Safe locations are defined by exit and entry readers called muster readers. These readers are used purely for registration purposes and not to actually gain access into the safe location.

When an incident occurs a muster report can be generated listing all personnel within a hazardous location. During an incident cardholders must register in a safe location by entering the safe location via a designated muster readers. Registering in a safe location removes the cardholder from the muster report. In this way the muster report becomes a report of all those who are on-site and have failed to register in a safe location.

At the end of an incident system operators can remove all cardholders from the safe locations; this is referred to as a *muster reset*.

Overview of Hazardous / Safe Locations

Hazardous and safe locations are defined in System Administration as a special type of global APB (Anti-PassBack) area. *APB* is the prevention of a badge from gaining entry in an access control system when that badge has either recently entered the same reader or area (timed APB) or is not considered to be in the proper area required to gain entry into a new area (area APB). *Global APB* is APB enforced at a system level; areas span across multiple controllers.

Global APB can be soft APB or hard. *Soft APB* allows badges to enter areas that would normally be denied due to APB violations whereas Hard APB does not.

Hard APB in Hazardous Locations

Soft global APB is required for hazardous locations but it is strongly recommended that hard global APB be used when ever possible, because soft global APB can invalidate the accuracy of muster reporting. For example the accuracy of muster reporting will be compromised if a person swipes into a hazardous location that they are already considered to be in or swipes out of a hazardous location when they are not considered to be in it.

Note: Soft global APB is required for **hazardous locations** but it is **strongly recommended** that **hard global APB** be used when ever possible.

Soft APB in Safe Locations

Soft APB must be applied to safe locations. It is assumed that readers entering safe locations are used purely for registration purposes and not to actually gain access into the safe location. In other words it is not expected that a badge will be presented to a reader to register at a safe location except during a muster mode. Since readers entering safe locations are used purely for registration purposes and not to gain access, any card transaction at a reader entering a safe location that contains a badge ID will be used to register that badge as being in a safe location. This includes granted with entry, granted with no entry, and access denied transactions.

Note: **Soft Global APB** is required for **safe locations**.

Enable Global APB

Hazardous and safe locations are segmented and can only belong to one segment at any time. **In order to enable mustering functionality in a given segment, Global APB support must be enabled in that segment.**

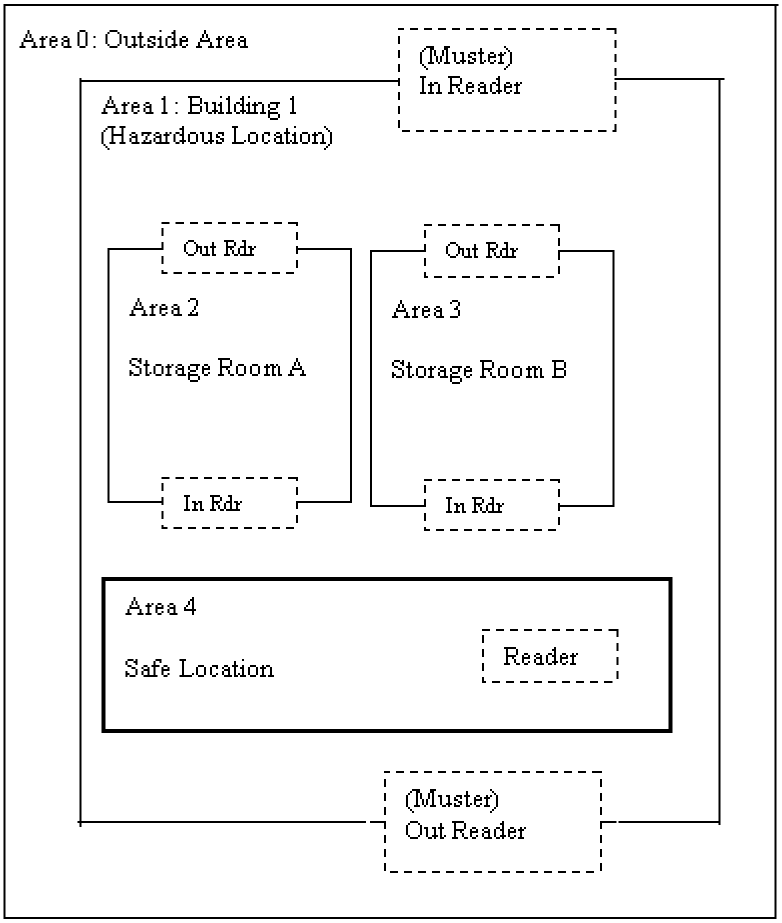
To enable global APB:

- In a segmented system, open System Administration or ID CredentialCenter and select the **Global Anti-Passback** check box on the Anti-Passback sub-tab of the Segments form in the Segments folder.
- In a non-segmented system, open System Administration or ID CredentialCenter and select **Administration** > **System Options**. Select the **Global Anti-Passback** check box on the Anti-Passback form.

Mustering Inside Hazardous Locations

For every hazardous location there must be at least one safe location associated with it, although multiple safe locations can be specified. In addition, multiple

APB areas can be defined as hazardous, and safe locations can exist within these hazardous locations. Refer to the example below.



This site wants to do mustering inside of a hazardous location. They also want to use APB within area 1 (hazardous location) and the two storage rooms (area 2 and area 3). To have APB control within the two storage rooms, area 2 and area 3 must be defined as separate areas.

When a Badge enters “Storage Room B”, the system will consider it to be area 3. As far as APB goes, that person is not considered to be in area 1 (the hazardous location). To function properly in this situation APB will not allow the badge to re-enter area 1 through any reader other than a reader leaving area 3.

However, for purposes of mustering, a person in “Storage Room B” (area 3) or in “Storage Room A” (area 2) needs to be considered as being in a hazardous location since everything inside of Building 1 except the safe location (area 4) is in the danger zone.

How can both of these be achieved? The answer is by considering the hazardous location to be a combination of area 1 + area 2 + area 3. When determining who is in the hazardous location, mustering will report anybody who is currently in any one of those areas.

Only normal APB areas can be configured as being contained in a hazardous location. Safe locations cannot, even though they may physically reside inside the hazardous location. This is because Badges recorded in a safe location should not be considered as being contained in the hazardous location.

General Constraints of Muster Mode

- When controllers go offline, ReadykeyPRO is not able to provide accurate muster and safe location reports since ReadykeyPRO will be unaware of access activity and safe location registration that occurs while a controller is offline. When the controller comes back online, ReadykeyPRO will be able to synchronize as long as the controller queued up all event transactions while it was offline.

Note: It is recommended that dual path panels and communications be deployed to help avoid offline panel situations.

- For the case of safe areas outside of hazardous areas, the muster exit readers are unlocked providing free access into and out of the hazardous area. Therefore access into and out of hazardous areas during an incident cannot be accurately tracked. Registration at the safe locations is what is accurately tracked.

Note: For the case of safe locations inside of hazardous areas, entry and exit readers are locked.

Recommendations for Optimal Reliability

- The operators main concern during an incident is to change the mode of muster exit readers to unlocked or locked and to run the muster and safe location reports.
- If a reader entering or leaving a hazardous location is configured with an offline mode of “unlocked” or “facility code only” and that reader goes offline with the controller, badges will be able to enter and/or exit the hazardous location without a record being made. If an incident occurs before these badges are swiped again (thus self-correcting the record of their location), the muster report will not be correct. It may list badges as being in hazardous locations when they are no longer there. Furthermore, it may not list badges that are still in the hazardous location as being there.

  The same issues can occur if, during normal times, badges are not forced to swipe at muster readers to gain entry into and out of hazardous areas or if physical barriers are not present to enforce one and only one physical entry per card swipe.

Bosch recommends the following during normal times, at muster entry and exit readers:

- Require that all access to hazardous locations be performed through the Access Control System. Utilize physical barriers such as full turnstile and vehicle gates to enforce one and only one physical entry per card swipe.
  This implies that a scenario should not be allowed where people freely enter a hazardous location and are then issued an access control badge once inside. If an incident occurs just after they have entered the hazardous location, there will be no record of them being in the hazardous area. If personnel, such as visitors, must enter hazardous locations without being issued a physical badge, they should first be issued a “virtual” badge in the system and the interface to manually place their badges inside of the hazardous location should be used. When they visitors physically leave the hazardous location, the same interface should be used to manually take them out of the hazardous location. It is likely going to be simpler and more reliable to actually issue real visitor badges that are used for access into and out of the hazardous locations.
- Utilize Hard APB enforcement into and out of hazardous locations.
- Configure reader offline modes to be “Locked”. If personnel must enter/exit the hazardous areas through doors whose readers are currently offline with their ISC, record the badge movement via the interface for manually moving a badge into a specific area.
  Note, however, that if free access is required through muster exit readers during muster mode, that the door strikes must be physically overridden during muster mode via an external source to ensure free exit during muster mode when readers are offline with their ISC’s.

Additionally, all host computers running ReadykeyPRO Communication Servers that are communicating with Access Controllers in the same Global APB Segment, must be time synchronized.

- ReadykeyPRO will not automatically change the mode of muster exit readers to unlocked or locked during an incident and back to a card mode at the end of an incident. It is assumed an external override will be used to override door strikes and physical barriers. For example if a fire system and access control system are installed at a site, the access control system is typically not depended upon to unlock the doors during a fire; the fire system overrides the door strike.
- Registration at safe locations is required after muster mode occurs even if personnel are already in the safe location at the start of the incident.

Muster Mode in Main Alarm Monitoring Window

In muster mode, the Main Alarm Monitoring window displays a muster mode start alarm. Right-clicking the alarm and selecting the area in muster mode displays a sub-menu of options. These options are also available by right-clicking a hazardous or safe area icon in a map or in the System Status window.

Note: In certain situations some right-click options listed below may not be available because they are location and/or mode (normal or muster) dependant.

Right-click Muster mode alarm sub-menu options

Option	Description
Update Area Status	Updates the status of both safe and hazardous areas so that operators can have a current view of cardholder locations.
View Map	Displays a map associated with the alarm. If several maps are associated with an alarm, the operator is prompted to select a map.
Move Badges	Enables an operator to manually move all the badges in one area to another.
Occupancy Report	Provides a current report of the cardholders currently in a safe area with information such as: the badge ID, the cardholder name, the time entered, and how the area was entered. **Note:** The occupancy report can also be run for a hazardous area. The occupancy report for a hazardous area is the similar to the muster report except it does not report the last attempted location.
Muster Report	Provides a current report of the cardholders currently in a safe area with information such as: the badge ID, the cardholder name, the time entered, and the area/last attempted location. **Note:** The muster report cannot be run for a safe area.
Start Muster Mode	Initiates muster mode. The Start Muster Mode window displays and provides an area to enter comments.
Reset Muster Mode	Ends muster mode. The Reset Muster Mode window displays and provides an area to enter comments.

Hazardous / Safe Locations in System Status Window

Hazardous and safe location icons display in the System Status window under the Global Anti-Passback Areas and Mustering section. Alarm monitoring operators can right-click hazardous or safe area icons and view all or some of the options available in the Right-click Muster mode alarm sub-menu options on page 122 table, depending on the area selected.

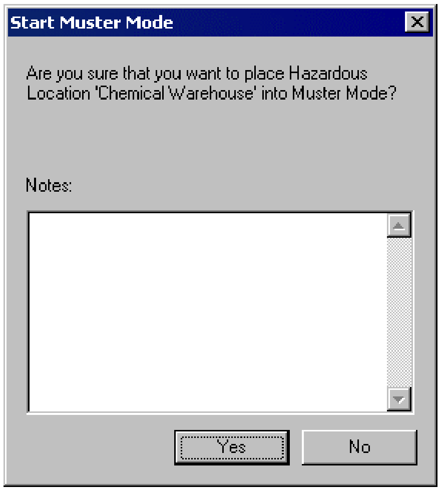
Muster Mode Procedures

Initiate Muster Mode

Muster mode is manually initiated via the Main Alarm Monitoring window, System Status window or map view.

Depending on how your System Administrator configures hazardous locations, muster mode initiation may automatically remove all cardholders from a safe location.

1. Using the Alarm Monitoring application, do one of the following:
   - From the Main Alarm Monitoring window **-** Right-click the Muster Mode Start alarm and select the hazardous location in muster mode. A sub-menu displays. Select **Start Muster Mode**.
   - From the System Status window - Right-click an area and select **Start Muster Mode**.
   - From the **View** menu select **Map** - Right-click a hazardous area and select **Start Muster Mode**.
2. The Start Muster Mode window displays.



Start Muster Mode

Are you sure that you want to place Hazardous Location 'Chemical Warehouse' into Muster Mode?

Notes:

3. Enter any notes relating to why muster mode is being activated, and click [Yes] to activate muster mode.
4. A warning message displays. Click [OK]. Muster mode is initiated.

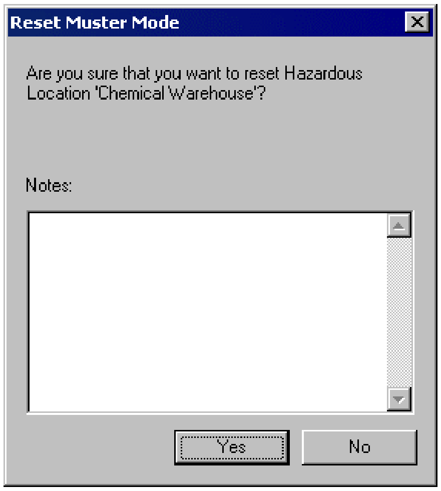
Reset Muster Mode

Muster reset is a manual operation that takes a hazardous area out of muster mode. Muster reset will not automatically remove personnel in hazardous locations. If a person really does remain in a hazardous area, you want to keep a record of them being there.

1. Using the Alarm Monitoring application, do one of the following:
   - From the Main Alarm Monitoring window - Right-click the Muster Mode Start alarm and select the hazardous location in muster mode. A sub-menu displays. Select **Reset Muster Mode**.
   - From the System Status window - Right-click an area and select **Reset Muster Mode**.

- From the **View** menu select **Map**. Right-click a hazardous area and select **Reset Muster Mode**.

2. The Reset Muster Mode window displays. Enter any notes and click [Yes] to reset muster mode.



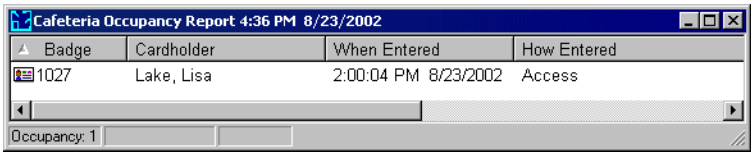
Are you sure that you want to reset Hazardous Location 'Chemical Warehouse'?

3. A warning message displays. Click [OK] and muster mode is initiated.

Reports

Several reports are available with mustering:

- **Muster mode report** - lists the badge IDs, cardholder name, time entered, how entered, and their last attempted location for a specific hazardous area. The status bar of the report displays the total occupancy for that area and the words MUSTER MODE. The title of the report displays the name of hazardous location and the time and date the report was initiated.
- **Occupancy report** - list badge IDs, cardholder name, time entered, and how entered. The status bar displays the total occupancy for that area. The title of the report displays the name of the safe location and the time and date the report was initiated. The occupancy report is sometimes referred to as the Safe Location report.



Badge	Cardholder	When Entered	How Entered
1027	Lake, Lisa	2:00:04 PM 8/23/2002	Access

Occupancy: 1

Run Muster and Occupancy Reports

Operators can run the muster and occupancy reports from the Main Alarm Monitoring window or System Status window. They can also right-click a hazardous or safe icon in map view to run reports.

1. Display either the Main Alarm Monitoring window or the System Status window.
2. Do one of the following:
   - From the Main Alarm Monitoring window - Right-click the Muster Mode Start alarm, select the device (in this case it would be the hazardous location in muster mode.) A sub-menu displays. Select **Muster Report** or **Occupancy Report**.
   - From the System Status window - Right-click an area and select **Muster Report** or **Occupancy Report**.

Notes: Muster reporting automatically refreshes every two minutes. However the user can manually refresh a report at any time.

Automatic reporting ends when the number of personnel in the muster report becomes zero.

Report right-click options

Both the muster and occupancy report (via right-click options) allow operators to move one or several badges from an area as well as select a cardholder and bring up their badge information.

Moving Badges

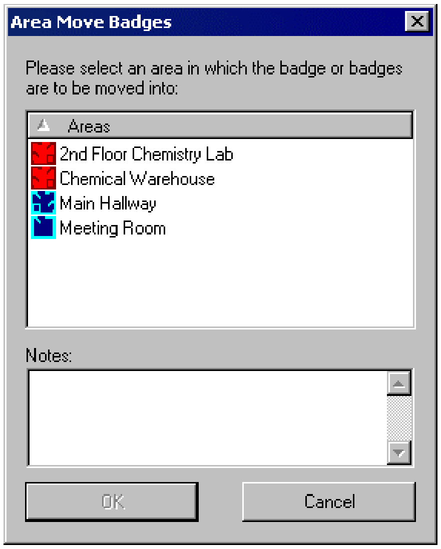
Specific user permission is required to move badges.

The focus of muster mode is to account for all personnel in hazardous locations. The muster report provides this information. If an operator verifies that personnel recorded as being in the hazardous location are physically outside the hazardous area they can manually move the badge to a different area.

Move All Badges from an Area

1. You can move every badge from a safe or hazardous area via several windows:
   - From the Main Alarm Monitoring window right-click the muster mode Start alarm, select the hazardous area and then select **Move Badges**.
   - From the System Status window right-click an APB area and select **Move Badges**.
   - From a map view right-click an APB area and select **Move Badges**.
2. When prompted to confirm your request. Click [Yes].

3. The Area Move Badges window displays. Select the desired area (a checkmark displays beside the area), enter any notes and click [OK].



Area Move Badges

Please select an area in which the badge or badges are to be moved into:

- 2nd Floor Chemistry Lab
- Chemical Warehouse
- Main Hallway
- Meeting Room

Move a Single Badge from an Area

Operators can also move a single badge from a safe or hazardous area; this can only be done through the occupancy or muster report.

1. Run the occupancy or muster report. For more information, refer to Run Muster and Occupancy Reports on page 125.

2. From the occupancy or muster report right-click and select **Move Badge to APB Area**.

Note: You can also move multiple badges from an area; this can be done by highlighting the desired badges, right-clicking and selecting **Move Badge to APB area**.

Advanced Operator Procedures

Chapter 3: Cardholders Folder

The Cardholders folder contains forms with which you can:

- Add, modify and delete cardholder and visitor records.
- Assign cardholders or groups of cardholders to different segments.
- Create badge records for cardholders and visitors.
- Assign access levels to active badges for cardholders and visitors.
- Assign one or more Precision Access groups to a badge (if Precision Access is used on your system).
- Search for and display cardholders and visitors biometrics records.
- Search for cardholders and visitors visit records.
- Assign and track assets to cardholders and visitors.
- Link directory accounts to cardholders and visitors.
- Assign a cardholder as a tour guard.
- Assign security clearance levels to tour guards.
- Create and print reports containing cardholder information.

the ILS Authorization form, In Visitor Management, the Cardholders folder can contain up to nine forms: the Cardholder/Visitor form, the Badge form, the Segments form (if segmentation is enabled), the Access Levels form, the Biometrics form, the Precision Access form (if in use), the Visits form, the Directory Accounts form, and the Reports form.

Toolbar Shortcut

The Cardholders folder is displayed by selecting **Cardholders** from the **Administration** menu, or by selecting the Cardholders toolbar button.

The forms in the Cardholders folder are visually divided into four sections; the right section, the upper-left section, the middle-left section and the bottom section.

Several of the form elements in these sections are common to every form in the cardholders folder. Refer to the following table for descriptions of the common form elements.

Notes: This documentation refers to cardholder data fields that are shipped as the default by Bosch. If you have used the FormsDesigner application to customize your cardholder data, the elements on your Cardholders folders will be different.

The Segments form is only available if segmentation is enabled on your system

The availability of certain forms and fields in the Cardholders folder is subject to licensing restrictions.

Cardholders Folder

Form Element	Comment
Common form elements - right section	
Photo display	Displays the cardholder's photo as it appears on their badge.
Signature display	Displays the cardholder's signature as it appears on their badge.
Last access	If **Show Last Granted Location** is selected in the **Cardholder** menu, displays information about the most recent valid access by this cardholder, including the triggered event, date, time and reader name. If **Show Last Attempted Location** is selected in the **Cardholder** menu, displays information about the most recent access attempt (whether access was granted or not) by this cardholder, including the triggered event, date, time and reader name.
Badge ID	Displays the numeric identifier assigned to the cardholder's active badge.
Issue code	Displays the issue code assigned to the cardholder's active badge.
Prints	Displays the number of times the active badge has been printed.
Activate	Displays the date when the badge becomes valid.
Deactivate	Displays the date when the badge becomes invalid.
Common form elements - upper-left section	
Last name	Indicates the cardholder's last name.
First name	Indicated the cardholder's first name.
Middle name	Indicates the cardholder's middle name.
Cardholder ID	Indicates the cardholder's ID number. **Note:** This field is not displayed on the Visitor form.
Badge type	Indicates the cardholder's badge type. Badge types are configured in the Badge Types folder. For more information refer to the Badge Types Folder chapter in the System Administration User Guide.
Common form elements - bottom section	
Search	Displayed in view mode on every form in the Cardholders folder. This button is used to search for existing cardholder records.

Cardholders Folder (Continued)

Form Element	Comment
Add	Enabled in view mode on the Cardholder/Visitor and Badge form and is used to add a record. **Note:** This button is displayed but not enabled on the Segments form, the Access Levels form, the Precision Access form, the Biometrics form, the Visits form, the Guard Tours form and the Reports form because these records are not added in the Cardholders folder.
Modify	Displayed in view mode on every form in the Cardholders folder. **Note:** This button will be displayed but will not be enabled on the Directory Accounts form and the Reports form, because directory account and report records cannot be modified.
Delete	Enabled in view mode on the Cardholder/Visitor and Badge form and is used to delete a record. **Note:** This button is displayed but not enabled on the Segments form, the Access Levels form, the Precision Access form, the Biometrics form, the Guard Tours form and the Reports form because these records are not deleted in the Cardholders folder.
Print	Displayed in view mode on every form in the Cardholders folder. When selected, displays the **Badge Printing** window from where you can print the active badge for the current record, or the active badges for all records found in a search. You can also log and print errors encountered during the print operation. **Note:** When you select this button on the Reports form, the **Print Report Options** window is displayed. For more information, refer to Chapter 7: Print Report Options Window on page 181.
Encode	Displayed in view mode on every form in the Cardholders folder. When clicked, displays the **Encode Badge** window from where you can encode the badge configurations selected for the cardholder onto a smart card. or more information refer to the Card Formats Folder chapter in the System Administration User Guide.The availability of this button is subject to licensing restrictions.
Replication	**Note:** This field only appears on Enterprise systems. The value in this field determines where the cardholder record gets propagated. On a Master server, this option is grayed out, and "All Regions" is selected. This is because when cardholder records are added at a Master server, they must be propagated to ALL Regional servers. On a Regional server: • If "All Regions" is selected, the cardholder record is sent to the Master server when replication occurs, and the record is then sent to ALL Regional servers when they replicate. • If "Local Regions Only" is selected, the cardholder record is stored on the local Regional server where it was added. The record is also sent to the Master server.
⏮	Displayed in search mode on every form in the Cardholders folder. When selected, moves to the first record that matches your search criteria.

Cardholders Folder (Continued)

Form Element	Comment
◀◀	Displayed in search mode on every form in the Cardholders folder. When selected, by default moves 10 matching records back. You can change the number of records moved back by modifying the value in the **Number of records to scroll for fast forward and rewind** field on the **View Options** window. The View Options window is displayed by selecting **View Options** from the **Cardholder** menu.
◀	Displayed in search mode on every form in the Cardholders folder. When selected, moves to the previous record that matches your search criteria.
▶	Displayed in search mode on every form in the Cardholders folder. When selected, moves to the next record that matches your search criteria.
▶▶	Displayed in search mode on every form in the Cardholders folder. When selected, by default moves 10 matching records forward. You can change the number of records moved forward by modifying the value in the **Number of records to scroll for fast forward and rewind** field on the **View Options** window. The View Options window is displayed by selecting **View Options** from the **Cardholder** menu.
▶|	Displayed in search mode on every form in the Cardholders folder. When selected, moves to the last record that matches your search criteria.
OK	Displayed in search or modify mode on every form in the Cardholders folder. When selected, saves the changes made to the current record, or begins the requested search.
Cancel	Displayed in search or modify mode on every form in the Cardholders folder. When selected, cancels the pending requested action.
Clear	Displayed in search or modify mode on every form in the Cardholders folder. When selected, clears all current record information that can be cleared from the current form.
Clear All	Displayed in search or modify mode on every form in the Cardholders folder. When selected, clears all current record information that can be cleared from *all* forms in the folder.
Capture	Displayed in add or modify mode on the Cardholder/Visitor form, the Segments form, the Badge form, the Access Levels form, the Precision Access form and the Biometrics form. Displayed in modify mode on the Visits form. When selected, opens Multimedia Capture. **Note:** The availability of Multimedia Capture is subject to licensing restrictions.
Last Search	Displayed in search mode on every form in the Cardholders folder. When selected, retrieves the same group of records that was found by the most recent search operation.
Record count	Displayed in view mode on every form in the Cardholders folder and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.
Person type	In search mode, select the type of record you want to search. Choices are: • All - when selected, your search will locate both Cardholder and Visitor records • Cardholders - when selected, your search will only locate cardholder records • Visitors - when selected, your search will only locate visitor records

Cardholders Folder Procedures

The following procedures pertain to every form in the Cardholders folder unless otherwise noted.

Cardholder Search Capabilities

Before you begin searching cardholders you must have cardholder search permissions enabled. For more information, refer to Cardholder Permission Groups Form (Cardholder Sub-tab) in the System Administration or ID CredentialCenter user guide.

In search mode, you can search on any combination of fields in the Visits folder, including the Status search, Visit and Details forms. On the E-mail and Reports forms, you can only search for the host name or visitor name.

Comparison Operators

Comparison operators are symbols that represent specific actions. You can refine your search by prefixing search fields with a comparison operator. Refer to the following table to identify the comparison operators you can use with different fields.

Comparison operator	Description	Text field	Numeric field	Drop-down list
=	Equal to	Yes	Yes	Yes
!= or <>	Not equal to	Yes	Yes	Yes
>	Greater than	Yes	Yes	NA
<	Less than	Yes	Yes	NA
>=	Greater than or equal to	Yes	Yes	NA
<=	Less than or equal to	Yes	Yes	NA
%	Contains	Yes	NA	NA

Notes: “Equal to” is the default comparison operator for numeric and drop-down list fields.

If you type an equal to sign “=” in a field and nothing else, ReadykeyPRO will search for records that have an empty value for that field. For example, typing an “=” in the Department field will find every record that does not have an assigned department.

Search Fields Using “Begins With”

For text and drop-down list fields you can search records whose values begin with specific characters by entering those characters in the field. For example, when searching by last name, a filter of “L” will find “Lake”, “Lewis”, etc. A filter of “Lake” will find “Lake”, “Lakeland”, etc.

Note: The default comparison operator for text fields is “begins with”.

Search Multiple Fields

When you search multiple fields, the search criteria for each field is combined. For example, typing “A” in **Last name** field and “B” in **First name** field will find all people whose last name begins with “A” and whose first name beings with “B”.

One *exception* is searching access levels, which uses an “or” comparison for multiple selections. For example, selecting both “Access Level A” and “Access Level B” will find all cardholders with either “Access Level A” or “Access Level B” assigned.

Note: If you want to search for a range of Badge IDs, take advantage of the two Badge ID fields on the Badge form. One field is located in the middle-left section of the form and the other field is located in the right section of the form. Note, the form must be in modify mode to see both fields. Type “>= 100” in one field and “<= 200” in the other to find all badges with IDs between 100 and 200 (inclusive).

Search for a Cardholder Record

1. In Alarm Monitoring, select **Badge Info** from the **View** menu. In all other applications, select **Cardholders** from the **Administration** menu.
2. The Cardholders folder opens. Click [Search].
3. If you are searching for a cardholder or visitor, select the type of person you are searching for in the **Person type** drop-down list (in the lower right). This field may not display due to licensing restrictions.
4. Specify your search criteria by typing full or partial entries in any enabled field on any of the tabs.
5. Click [OK].
6. ReadykeyPRO retrieves and displays the first matching record. Use the navigational buttons (in the lower right) to look at additional matching records.

   ⏮ ⏭ **First record/Last Record** - Displays the first/last matching record.

   ⏪ ⏩ **Rewind/Fast Forward** - Moves backward/forward ten matching records. To modify the number of records moved, refer to the View Options window, which is accessed from the **Cardholder** menu.

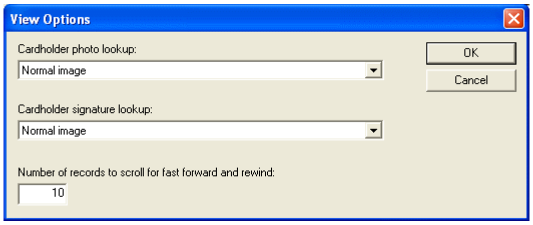
   ◀ ▶ **Previous record/Next record** - Displays the previous/next matching record.

Retrieve the Most Recent Search Results

1. Display the Cardholders folder or Visits folder by completing one of the following:
   - To display the Cardholders folder in Alarm Monitoring, select **Badge Info** from the **View** menu. For all other applications, select **Cardholders** from the **Administration** menu.
   - To display the Visits folder in Alarm Monitoring, select **Visits** from the **View** menu. For all other applications, select **Visits** from the **Administration** menu.
2. Click [Search].
3. Click [Last Search]. The criteria you selected from the most recent search operation will be inserted into the appropriate fields.
4. You can optionally modify your search criteria.
5. Click [OK].
6. ReadykeyPRO retrieves and displays the first matching record. Use the navigational buttons to look at additional matching records.

Change the Cardholders Folder View Options

1. Select **View Options** from the Cardholder menu. The **View Options** window opens.



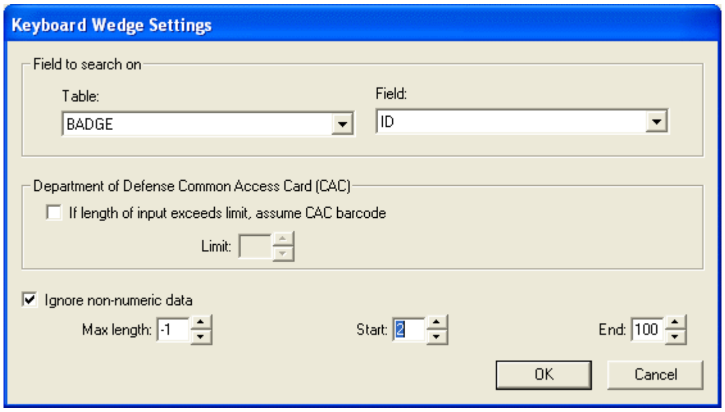
Cardholder photo lookup:
Normal image

Cardholder signature lookup:
Normal image

Number of records to scroll for fast forward and rewind:
10

2. From the **Cardholder photo lookup** drop-down list, select the image type you want displayed in **Photo** display (located in the right section of the Cardholders folder forms).
   Choices include:
   - **None** - no image will be displayed
   - **Normal image** - a photo image will be displayed as it was originally captured
   - **Normal image with chromakey** - a photo image will be displayed, but without its background
   - **Thumbnail** - This option is only displayed if the **Create/save photo thumbnails** check box in **Administration** > **Cardholder Options** > General Cardholder Options is selected. A smaller thumbnail version of the photo is displayed.
3. From the **Cardholder signature lookup** drop-down list, select the type of signature you want displayed in **Signature** display (located in the right section of the Cardholders folder forms).
   Choices include:
   - **None** - no signature will be displayed
   - **Normal image** - a signature will be displayed
4. In the **Number of records to scroll for fast forward and rewind** field, type in the number of records you want to move backwards and forwards when you select the ⏪ and ⏩ push buttons.
5. Click [OK].

Keyboard Wedge Settings Window



Keyboard Wedge Settings

Field to search on

Table: BADGE

Field: ID

Department of Defense Common Access Card (CAC)

□ If length of input exceeds limit, assume CAC barcode

Limit:

☑ Ignore non-numeric data

Max length: -1

Start: 2

End: 100

A wedge scanner, also sometimes referred to as a wedge reader, is a device that is attached to a keyboard and used to scan badge IDs as direct keyboard input. Wedge scanners can be used with ReadykeyPRO to:

- **Add a badge.** In this scenario, each card entry station has a wedge scanner. The operator clicks [Add] and swipes the badge with the wedge scanner to read the badge ID. This is equivalent to typing in the badge ID at the keyboard. When a wedge scanner is used in this manner, no configuration of the settings on the Keyboard Wedge Settings window is needed.
- **Search for a badge.** The normal way to search for a badge in ReadykeyPRO is to click [Search] and then specify what to search for, such as badge ID or social security number. When a wedge scanner is used, the [Search] button does not need to be clicked; instead, the system specifically searches on one predefined criteria. When a wedge scanner is used in this manner, the settings on the Keyboard Wedge Settings window must be properly configured.

Displaying the Keyboard Wedge Settings Window

The Keyboard Wedge Settings window is displayed by selecting **Keyboard Wedge Settings** from the **Cardholder** menu. (In System Administration, ID CredentialCenter, Visitor Management, and View/Edit Only the **Cardholder** menu is only displayed after selecting **Cardholders** from the **Administration** menu. In Alarm Monitoring, the **Cardholder** menu is displayed after clicking the toolbar button.)

CAC Barcodes

A common access card (CAC) is a military-issued ID card that is issued to active duty personnel, selected reservists, Department of Defense civilian employees, eligible contractors, and some foreign nationals. Retirees, family members, and inactive reservists are not currently issued a CAC card.

Configuring ReadykeyPRO to Read CAC Barcodes

To set the ReadykeyPRO system up to read CAC cards, the **If length of input exceeds limit, assume CAC barcode** check box on the Keyboard Wedge Settings window must be selected. A limit also needs to be specified. If only CAC cards will be read, then the **Limit** can be set to 0. However, most systems will also need to have the ability to read other cards in addition to CACs, so the limit will need to be set to an appropriate value.

For example, a military base that assigns badge IDs to the people on its base may want to be able to read those badge IDs as well as CACs because visitors from other bases will only have a CAC. In this case, the limit would need to be set to an appropriate number. If the badge IDs were all nine digits long, then an appropriate limit would be ten because CAC barcodes are much longer than ten digits.

Scanning Barcodes with a Wedge Scanner

When an ID is scanned, ReadykeyPRO determines the length of the number that was scanned. If the number of digits exceeds the limit, then the number is treated as a CAC number, and the social security number is decrypted and searched up.

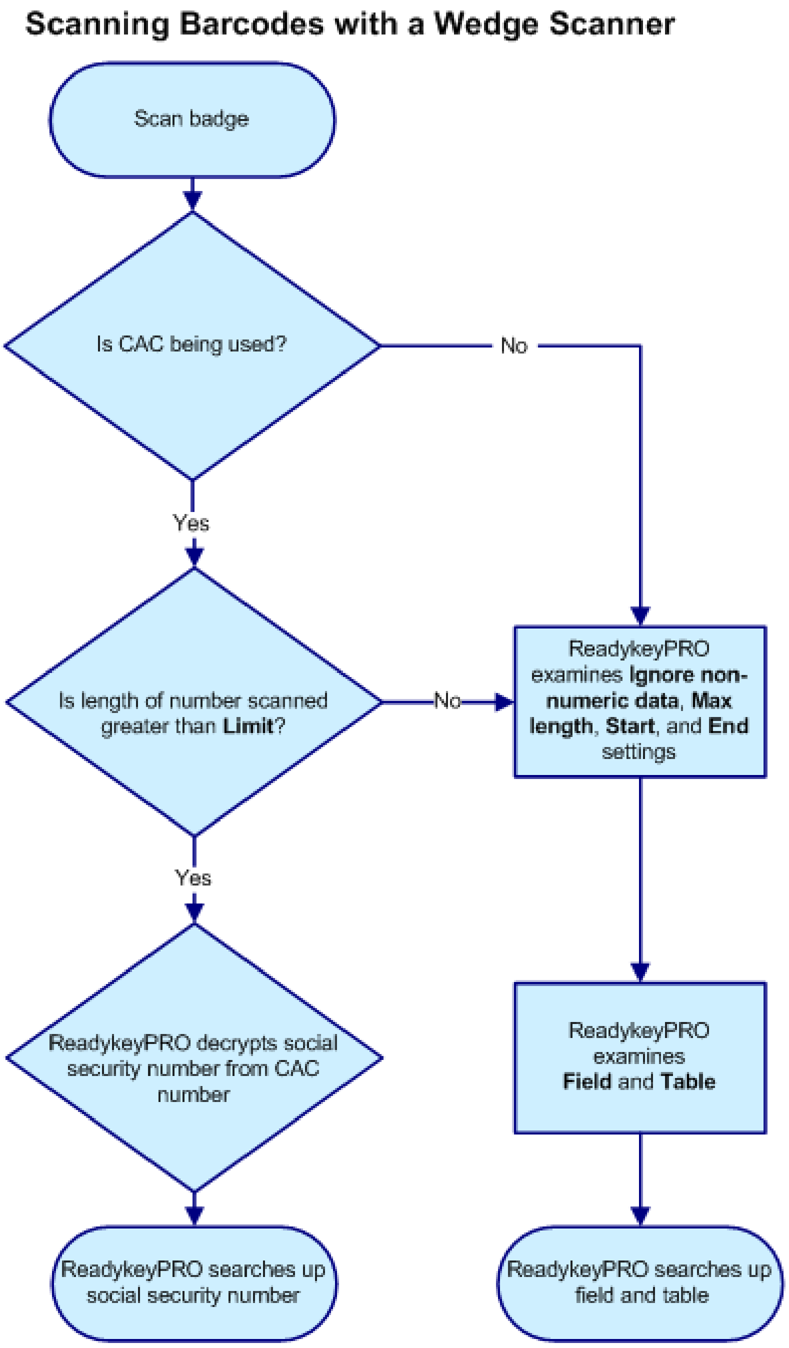
If the number of digits is less than the limit, then the maximum length, start, and end settings are applied to the string and used to extract the search criteria (typically badge ID or social security number).

After those settings are examined, the system then examines the **Table** and **Field** and searches that information up. The **Table** and **Field** specified depend on what information is encoded on the card that will be read in addition to the CAC. Common options include:

- **Badge ID**. If searching on Badge IDs, select the BADGE table and the ID field.
- **Social security number**. If searching on social security numbers, select the EMP table and the SSNO field.

- **User-defined field.** If searching on a user-defined field, select the desired table and field. For example, a company may wish to search on a table and field that is unique to their system, such as an employee number.

The following flowchart describes what happens when a barcode is scanned with a wedge scanner:


Scanning Barcodes with a Wedge Scanner
Scan badge
Is CAC being used?
No
Yes
Is length of number scanned greater than **Limit**?
No
Yes
ReadykeyPRO examines **Ignore non-numeric data**, **Max length**, **Start**, and **End** settings
ReadykeyPRO decrypts social security number from CAC number
ReadykeyPRO examines **Field** and **Table**
ReadykeyPRO searches up social security number
ReadykeyPRO searches up field and table

Keyboard Wedge Settings Window

Form Element	Comment
Table	Select the table in the ReadykeyPRO database that you wish to search on when keyboard input is detected. If searching for badge ID numbers, select the BADGE table, and if searching for social security numbers, select the EMP table. **Note:** If CAC is being used and an ID is scanned that has more than the specified **Limit** of digits, then the **Table** and **Field** will be ignored.
Field	Select the field in the selected table in the ReadykeyPRO database that you wish to search on when keyboard input is detected. If searching for badge ID numbers, select ID (in the BADGE table), and if searching for social security number, select SSNO (in the EMP table). **Note:** If CAC is being used and an ID is scanned that has more than the specified **Limit** of digits, then the **Table** and **Field** will be ignored.
If length of input exceeds limit, assume CAC barcode	If selected, CAC (Common Access Card) barcodes can be used. This allows military code 3of9 barcodes to be scanned and decoded into the cardholder's social security number. If you do not wish to use this feature, leave this check box deselected. If this check box is selected, you must specify an appropriate **Limit**. When this check box is selected and an ID is scanned, the number of digits will be examined. • If the number of digits is less than or equal to the **Limit**, then the system will search on the **Table** and **Field**. • If the number of digits is greater than the **Limit**, then the system will assume the ID was a CAC, decrypt the social security number, and search the social security number up.
Limit	The **Limit** field is only enabled when the **If length of input exceeds limit, assume CAC barcode** check box is selected. If the **Limit** is set to zero, then only CAC can be read. Setting a limit greater than zero enables the system to recognize two different formats. When an ID is scanned, the number of digits will be examined. • If the number of digits is less than or equal to the **Limit**, then the system will search on the **Table** and **Field** using the **Max length**, **Start**, and **End** settings. • If the number of digits is greater than the **Limit**, then the system will assume the ID was a CAC, decrypt the social security number, and search the social security number up.
Ignore non-numeric data	If selected, non-numeric data is removed and not counted as a placeholder. This is important for scans that include dashes in the social security number. For example, if an ID is scanned that has 123-45-6789 encoded, the system will search for 123456789.
Max length	A maximum length must be provided if the wedge scanner does not automatically provide a line feed carriage return. This allows the wedge scanner to be used as long as the length of the scan is always the same (i.e., social security number). If 0 or -1 is specified, then the whole string will be read in.

Keyboard Wedge Settings Window (Continued)

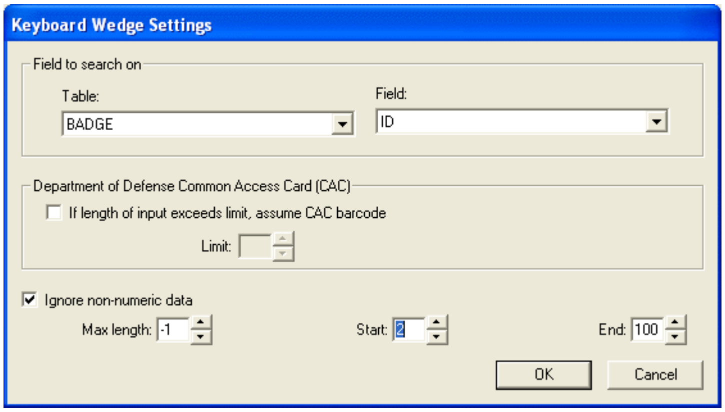
Form Element	Comment
Start	The **Start** field works in combination with the **End** field. When an ID is scanned, a string of numbers are read. As long as the ID is not a CAC, that string of numbers typically contains the actual badge ID or social security number. For a CAC, that string of numbers doesn't contain the actual social security number, but ReadykeyPRO does "decrypt" the social security number from the string. The **Start** position is important because the string of numbers may contain other numbers in addition to what is being searched for; it is the first position in the string of numbers that contains a digit of what is being searched for. The **End** position is the last digit of what is being searched for. The **End** position should be greater than or equal to the **Start** position. Take for example the string 123456789. If 4 is the **Start** position and 7 is the **End** position, then the ReadykeyPRO system will search on 4567. If you specify an **End** position that is less than the **Start** position, ReadykeyPRO assumes the end is 255. Therefore, for the string 123456789 with 4 as the **Start** and 3 as the **End**, ReadykeyPRO would search on 456789.
End	The **End** field works in combination with the **Start** field. As long as the ID is not a CAC, that string of numbers typically contains the actual badge ID or social security number. For a CAC, that string of numbers doesn't contain the actual social security number, but ReadykeyPRO does "decrypt" the social security number from the string. The **Start** position is important because the string of numbers may contain other numbers in addition to what is being searched for; it is the first position in the string of numbers that contains a digit of what is being searched for. The **End** position is the last digit of what is being searched for. The **End** position must be greater than or equal to the **Start** position. Take for example the string 123456789. If 4 is the **Start** position and 7 is the **End** position, then the ReadykeyPRO system will search on 4567. If you specify an **End** position that is less than the **Start** position, ReadykeyPRO assumes the end is 255. Therefore, for the string 123456789 with 4 as the **Start** and 3 as the **End**, ReadykeyPRO would search on 456789.
OK	Applies the selected wedge scanner settings and closes the Keyboard Wedge Settings window.
Cancel	Closes the Keyboard Wedge Settings window without applying any changes made.

Keyboard Wedge Settings Window Procedures

Configure a Wedge Scanner

How the ReadykeyPRO system interprets the information it receives from a wedge scanner can be configured by doing the following:

1. In System Administration, ID CredentialCenter, Visitor Management, or View/Edit Only, select **Cardholders** from the **Administration** menu. In Alarm Monitoring, click the toolbar button.
2. Select **Keyboard Wedge Settings** from the **Cardholder** menu.
3. The Keyboard Wedge Settings window opens.



Keyboard Wedge Settings

Field to search on

Table: BADGE

Field: ID

Department of Defense Common Access Card (CAC)

☐ If length of input exceeds limit, assume CAC barcode

Limit:

☑ Ignore non-numeric data

Max length: -1

Start: 2

End: 100

a. Specify the **Table** and **Field** you wish to search on when non-CAC input is detected. By default, the system searches on the ID field in the BADGE table. If for example you wanted to search based on social security number instead of badge ID, you would select the SSNO field in the EMP table.

b. If CAC (Common Access Card) barcodes will be used, select the **If length of input exceeds limit, assume CAC barcode** check box and specify the limit. This allows military code 3of9 barcodes to be scanned and decoded into the cardholder’s social security number. If you do not wish to use this feature, leave this check box deselected.

c. Select whether to ignore non-numeric data. By default, the **Ignore non-numeric data** check box is selected. This is important for scans that include dashes in the social security number.

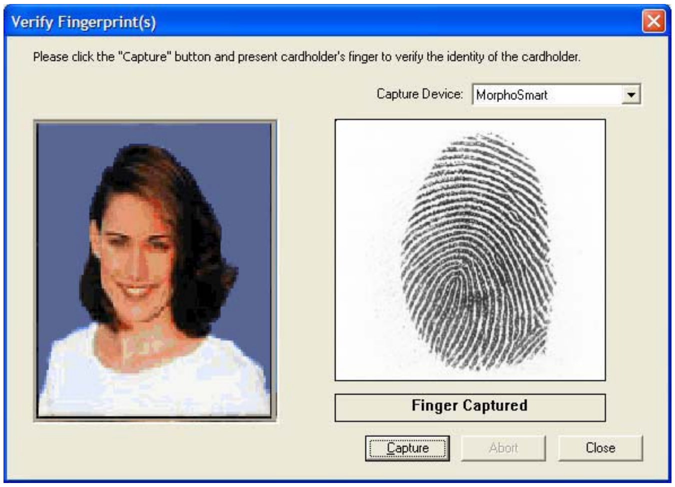
d. Specify the maximum length in the **Max length** field. A maximum length must be provided if the wedge scanner does not automatically provide a line feed carriage return. This allows the wedge scanner to be used as long as the length of the scan is always the same (i.e., social security number).

Note: If 0 or -1 is specified, then the whole string will be read in.

e. Specify the start and end. In a string of numbers that contains a search criteria (typically social security number or badge ID), start and end are the first and last position, respectively, that contain the search criteria.

f. Click [OK].

Verify Fingerprint(s) Dialog


Verify Fingerprint(s)
Please click the "Capture" button and present cardholder's finger to verify the identity of the cardholder.
Capture Device:
MorphoSmart
Finger Captured
Capture
Abort
Close

Fingerprint Verification with PIV Cards

When fingerprint data is imported from PIV cards, the Verify Fingerprint(s) dialog will be displayed allowing you to capture the cardholder's live fingerprint for comparison against the fingerprint encoded on the PIV card. If the PIV card is encoded with a facial image, it is displayed for additional verification.

Important: Fingerprint verification is optional. To verify fingerprints, select the **Verify fingerprints on import** check box on the Cardholder Options Folder > General Cardholder Options form in System Administration.

Verify Fingerprint(s) Dialog

Dialog Element	Comment
Facial image from PIV card	If a facial image is encoded on the PIV card, it is displayed in the left pane of the dialog for verification of the cardholder’s identity.

Verify Fingerprint(s) Dialog (Continued)

Dialog Element	Comment
Capture Device	From the drop-down list, select the fingerprint scanning device you are using to capture the fingerprint.
Live fingerprint	The captured fingerprint is displayed in the left pane. This image is compared against the fingerprints encoded on the PIV card.
Status display	Messages and on-screen prompts are displayed in the status box below the fingerprint image.
Capture	Click this button to begin capturing the fingerprint.
Abort	Click this button to stop the capture operation.
Close	Click this button to close the dialog.

Verify Fingerprint(s) Dialog Procedures

Verify Fingerprints from a PIV Card

1. When the Verify Fingerprint(s) dialog is displayed, follow the on-screen prompts provided in the status box below the fingerprint image. You will be guided through the process of capturing and verifying the fingerprints.
2. From the **Capture Device** drop-down select the device you will use to capture the fingerprints.
3. When prompted, the cardholder presents his/her finger to the capture device.
4. Click [Capture].
5. If the fingerprints match, a successful issuance is registered with ReadykeyPRO. However, if fingerprint verification fails, the card is terminated and recycled.

Note: If the PIV card contains a facial image, it is displayed with the captured fingerprint image for additional verification of the cardholder.

6. To stop the capture operation, click [Abort].

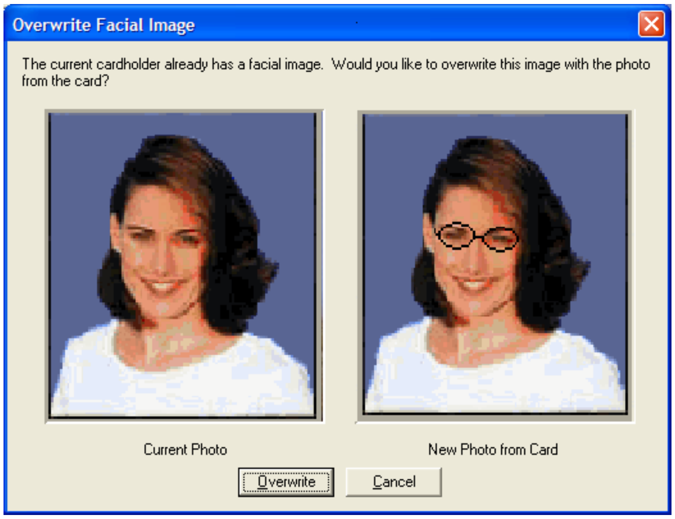
Import Fingerprints from a PIV Card

To import the fingerprints encoded on the PIV card into the database:

Important: Ensure the **Import fingerprints from card into database** check box is selected in the Cardholder Options Folder > General Cardholder Options Form in System Administration.

Note: When importing data from a PIV card after adding, modifying, or searching on a badge (NOT a cardholder), cardholder-specific data that is imported (**Last name**, **First name**, **Middle name**, and **Cardholder ID**) is not overwritten even though it is displayed in the grayed-out fields. However, the cardholder photo is imported if the user confirms replacement of the existing photo.

Overwrite Facial Image Dialog



Overwrite Facial Image

The current cardholder already has a facial image. Would you like to overwrite this image with the photo from the card?

After fingerprint verification, if the cardholder already has a photo, the Overwrite Facial Image dialog is displayed allowing you to import the facial image from the PIV card and overwrite the current cardholder photo with it.

Note: Existing cardholder photos are NOT automatically overwritten. If there is an existing cardholder photo, the Overwrite Facial Image dialog is displayed with the current photo and the photo from the card allowing the user to choose which one to use.

Overwrite Facial Image Dialog

Dialog Element	Comment
Current Photo	Displays the cardholder's current photo.
New Photo on Card	Displays the facial image encoded on the PIV card.
Overwrite	Click this button to replace the current photo with the one on the PIV card.

Overwrite Facial Image Dialog (Continued)

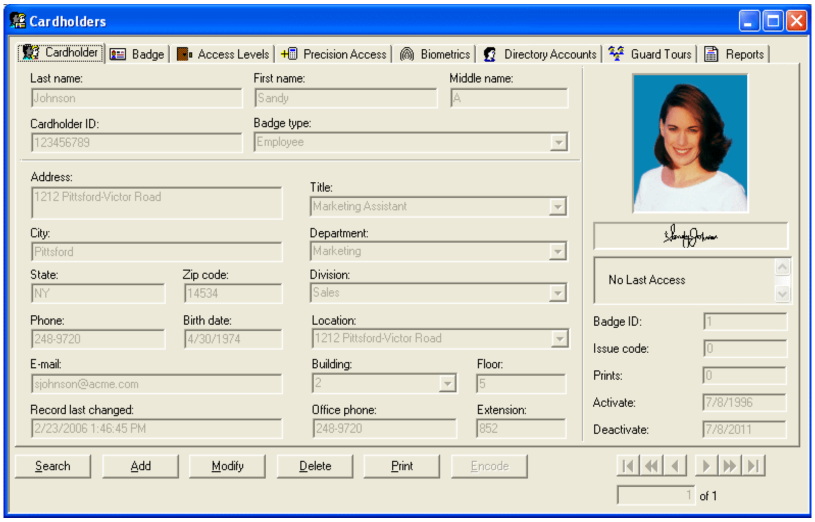
Dialog Element	Comment
Cancel	Click this button if you do not wish to overwrite the current photo.

Overwrite Facial Image Dialog Procedure

Replace Cardholder Photo with Facial Image on PIV Card

1. If the Overwrite Facial Image dialog is displayed, compare the facial image from the PIV card with the current cardholder photo.
2. Click [Overwrite] to replace the current cardholder photo with the one from the PIV card.
3. If you do not wish to replace the current cardholder photo, click [Cancel].

Cardholder Form



Last name:	Johnson
First name:	Sandy
Middle name:	A
Cardholder ID:	123456789
Badge type:	Employee
Address:	1212 Pittsford-Victor Road
Title:	Marketing Assistant
City:	Pittsford
Department:	Marketing
State:	NY
Zip code:	14534
Division:	Sales
Phone:	248-9720
Birth date:	4/30/1974
Location:	1212 Pittsford-Victor Road
E-mail:	sjohnson@acme.com
Building:	2
Floor:	5
Record last changed:	2/23/2006 1:46:45 PM
Office phone:	248-9720
Extension:	852
Badge ID:	1
Issue code:	0
Prints:	0
Activate:	7/8/1996
Deactivate:	7/8/2011

No Last Access

1 of 1

Cardholder Form Overview

In the System Administration and ID CredentialCenter applications, the Cardholder form is used to:

- Define a cardholder.
- Enter or import demographic information into the cardholder record.
- Choose a badge type for the cardholder.
- Access Multimedia Capture (subject to licensing restrictions).

In the Visitor Management application, the Cardholder form is used to search for a cardholder.

Cardholders Folder - Cardholder Form

Form Element	Comment
Cardholder data	Displayed in view mode. When adding or modifying a cardholder record, enter the cardholder's information such as name, address and department into these fields.
Record last changed	Displayed in view mode and indicates the date on which the selected cardholder record was last modified and saved. This date is updated only when cardholder information is changed, not when badge information is changed. The last changed date is saved individually for each badge record as well.

Import Cardholder/Visitor Data

Users can import demographic data stored on business cards, passports, driver's licenses, identification (ID) cards, and smart cards during cardholder/visitor add, modify, or search operations. Refer to the Cardholder/Visitor Import table on page 76 for a summary of the hardware used to import demographic data and the user-defined fields (UDF) that must be mapped in FormsDesigner to import data into the Cardholder form.

Note: Licenses are required to import cardholder data and are based on the number of scanning terminals used.

Prerequisites

System Administrators should complete the following steps in order to prepare ReadykeyPRO to import information:

1. Configure the reader/scanner communication settings including the workstation to which it is connected. Refer to the third column in the Cardholder/Visitor Import table on page 76 to determine if you have to configure the reader/scanner in ReadykeyPRO and if so, what the device type would be. For more information, refer to the Encoders/Scanners form in System Administration.

Note: Some reader/scanners do not need to be configured in the ReadykeyPRO application. Simply load the drivers onto the encoding/scanning workstation.

2. Map the demographic data to the appropriate user-defined fields in Forms Designer. For more information, refer to the FormsDesigner User Guide.
3. For PIV cards:
   a. Configure the fingerprint settings in the General Cardholder Options form. For more information, refer to the Cardholder Options chapter in the System Administration User Guide.
   b. Ensure the PIV card is inserted in the PC/SC encoder/scanner.

Cardholder/Visitor Import

Source	Hardware scanner	License required	Device Type to select in Workstations folder	Import Source to select	UDF
Business card	Corex CardScan scanner	No	NA	Corex CardScan scanner	vCard
Passport	ScanShell 1000-A Terminal	Yes	NA	ID Scan	DMV/ Passport
Driver’s license	ScanShell 800-R Terminal	Yes	NA	ID Scan	DMV/ Passport
	ScanShell 1000-A Terminal	Yes	NA	ID Scan	DMV/ Passport
	ID-Check Terminal	Yes	ID-Check Terminal	ID-Check Terminal	DMV/ Passport
Identification card	ScanShell 800-R Terminal	Yes	NA	ID Scan	DMV/ Passport
	ScanShell 1000-A Terminal	Yes	NA	ID Scan	DMV/ Passport
	ID-Check Terminal	No	ID-Check Terminal	ID-Check Terminal	DMV/ Passport
GSC (iCLASS) smart card	HID iCLASS	Yes	HID (iCLASS) reader/encoder	GSC (iCLASS) smart card	CAC GSC FASC-N
PIV card	PC/SC encoder/scanner	No	PC/SC encoder/ scanner	PIV card	PIV FASC-N

Cardholder/Visitor Import

Source	Hardware scanner	License required	Device Type to select in Workstations folder	Import Source to select	UDF
TWIC card	PC/SC encoder/scanner	No	PC/SC encoder/ scanner	TWIC card PIV card	PIV FASC-N

Corex Business Card Scanner

Using Corex Business Card scanners, users can import demographic data into the Cardholder form from business cards.

The Corex Business Card scanners are not configured in ReadykeyPRO as encoder/scanners. Simply load the drivers onto the encoding/scanning workstation and the Corex CardScan scanner will be an option on the Select Import Source dialog.

Only data that is mapped to the appropriate vCard -UDF or DMV-UDF field in FormsDesigner is imported into the Cardholder form.

GSC (iCLASS) Card

Using HID (iCLASS) readers/scanners, users can import demographic data into the Cardholder form from GSC (iCLASS) smart cards.

Only data that is mapped to the appropriate CAC, GSC, or FASC-N-UDF fields in FormsDesigner is imported into the Cardholder form.

Note: If badge information is stored on the smart card, you will have to assign a badge type during import.

ID Scan

Using the ID Scan scanners, users can import demographic data on driver licenses, identification cards, and passports issued by various Countries and State and Provincial Departments of Motor Vehicles.

Note: Not all the state and provincial DMV’s currently encode their driver’s license and identification cards. Therefore, not all state driver licenses are supported.

Note: Importation of cardholder and visitor data with ScanShell 800-R and ScanShell 1000-A CSS devices is now licensed. This license allows only a certain number of CSS devices, dictated by the license, to be configured through workstations and scanners.

The ScanShell 800-R is the regular scanner that scans driver's licenses and uses OCR to extract data off of them. The ScanShell 1000-A performs the same function plus passport scanning.

Only data that is mapped to the appropriate DMV-UDF fields in FormsDesigner is imported into the Cardholder form.

Data Import

Users will be prompted to select an ID, barcode, or passport during the scanning process. When ID scanning is selected users will have to select the country and the state/region of the driver license. However, when U. S. is selected (as the country), users will have an option to select auto detect (for the state). When auto detect is selected ID scan attempts to detect the state of the driver license that is being scanned.

ID-Check Terminal

Using the ID-Check Terminal scanner, users can import demographic data on driver licenses and identification cards issued by various State and Provincial Departments of Motor Vehicles. These credentials usually use any combination of a 3-track magnetic stripe, 2D barcode, and 1D barcode. Only data that is mapped to the appropriate DMV-UDF field in FormsDesigner can be imported.

Notes: Not all state and provincial DMV's are supported.

ReadykeyPRO supports ID-Check terminals (IDC-1400) version 5.4 and later.

Note: Importation of cardholder and visitor data with the ID-Check Terminal is now licensed. This license allows only certain number of ID-Check Terminal devices, dictated by the license, to be configured.

PIV Card

Using a PC/SC encoder/scanner, users can import data into the Cardholder form from PIV cards.

Only data that is mapped to the appropriate PIV-UDF or FASC-N-UDF fields in FormsDesigner is imported into the Cardholder form.

After selecting the PIV card as the data import source, the user must enter their PIN number to authenticate the process.

Fingerprint Verification and Import

Users will be prompted to verify the cardholder's fingerprint(s) and the photo on the PIV card is presented for further verification. Fingerprints from the card may be imported as well. For more information, refer to Fingerprint Verification with PIV Cards on page 71 and Import Fingerprints from a PIV Card on page 72.

Photo Replacement

If a photo is encoded on the PIV card, the user may elect to replace the current cardholder photo with the one on the card. For more information, refer to Replace Cardholder Photo with Facial Image on PIV Card on page 74.

TWIC Card

Using a PC/SC encoder/scanner, users can import data into the Cardholder form from TWIC cards which contain both TWIC and PIV data.

Only data that is mapped to the appropriate PIV-UDF or FASC-N-UDF fields in FormsDesigner is imported into the Cardholder form.

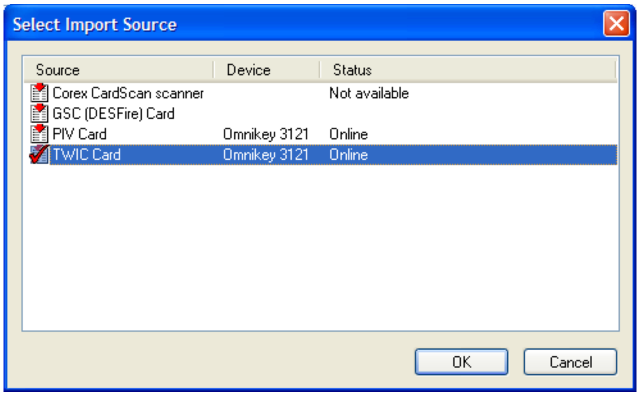
After selecting either the TWIC card or PIV card as the data import source, the user must enter their PIN number to authenticate the process.

Import Cardholder Data

1. Select **Cardholders** from the **Administration** menu for all applications except Alarm Monitoring. (In Alarm Monitoring, select **Badge Info** from the **View** menu.)
2. The Cardholders folder opens. Click [Add].

Note: The Import function is also available if the user searches for or modifies a cardholder/visitor or badge.

3. Click [Import].
4. In the Select Import Source window, select the import source available for this workstation. For more information, refer to the Cardholder/Visitor Import table on page 76.



Source	Device	Status
Corex CardScan scanner		Not available
GSC (DESFire) Card		
PIV Card	Omnikey 3121	Online
TWIC Card	Omnikey 3121	Online

Note: Import devices are configured in System Administration. In System Administration, select **Encoders/Scanners** from the **Workstations** menu.

5. Click [OK].
6. Perform the instructions that display to complete the import data process.

Cardholder Form Procedures

Add a Cardholder Record

Note: This procedure cannot be performed in Visitor Management.

1. Select **Cardholders** from the **Administration** menu. The Cardholders folder opens.
2. By default, the Cardholder form is displayed. Click [Add].
3. From the **Person type** drop-down list, select **Cardholders**.

Note: The **Person type** drop-down list is subject to licensing restrictions. If this field is not displayed, move on to the next step.

4. Enter the cardholder’s name and any additional information in the cardholder data fields.

Note: You can switch to other tabs and modify the other forms at this time.

5. If you want to add a photograph or signature to the cardholder record, click [Capture]. Multimedia Capture opens.
6. Enterprise users only: If you are adding a cardholder on a Regional server, select how the record will be replicated in the **Replication** drop-down list.
   - If you select “All Regions”, the cardholder record will be sent to the Master server when replication occurs, and the record will then be sent to ALL Regional servers when they replicate.
   - If you select “Local Regions Only”, the cardholder record will be stored on the local Regional server where it was added. The record will also be sent to the Master server.
7. Click [OK] to save the record.

Modify a Cardholder Record

Note: This procedure cannot be performed in Visitor Management.

1. Locate the cardholder record you want to change.
2. Click [Modify].
3. Make the changes you want to the record.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Cardholder Record

Note: This procedure cannot be performed in Visitor Management.

1. Locate the cardholder record you want to delete.
2. Click [Delete].
3. Click [OK].

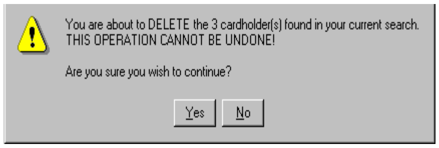
Note: If you delete the cardholder record, all associated records (Badge, Access Levels, Precision Access, Biometrics, Assets, Directory Accounts, Guard Tours and Visits) for the cardholder are also removed from the database.

Delete a Selected Group of Cardholder Records

Warning This is a powerful feature that cannot be undone. Use caution when performing a bulk deletion of cardholders to ensure that you only delete the cardholders you want to eliminate from your database.

Note: This procedure cannot be performed in Visitor Management.

1. Locate the cardholder records you want to delete using the search function. The bulk delete operation will act on **all** cardholders that result from the current search.
2. Select **Bulk** > **Delete Cardholders in Search** from the **Cardholder** menu. The following message is displayed:



You are about to DELETE the 3 cardholder(s) found in your current search.
THIS OPERATION CANNOT BE UNDONE!

Are you sure you wish to continue?

3. Click [Yes].

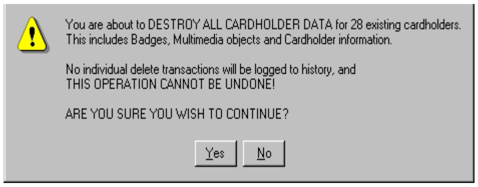
Destroy all Cardholder Data

⚠ **Warning**

This feature will wipe out all cardholder and badge information from the database without any transaction logging and cannot be undone. This function is mainly intended for wiping out data after a system has been installed and tested. For example, when you are first setting up the system and have imported cardholder data but you wish to change and redo the import. This function provides a quick way to wipe out all existing cardholder data.

Note: This procedure cannot be performed in Visitor Management.

1. Select **Bulk** > **Destroy ALL Cardholder Data** from the **Cardholder** menu. The following message is displayed:



You are about to DESTROY ALL CARDHOLDER DATA for 28 existing cardholders.
This includes Badges, Multimedia objects and Cardholder information.

No individual delete transactions will be logged to history, and
THIS OPERATION CANNOT BE UNDONE!

ARE YOU SURE YOU WISH TO CONTINUE?

2. Click [Yes] to confirm the deletion of all cardholder data.

Visitor Form

To provide integration with Visitor Management, visitor records can be searched and viewed in the Cardholders folder. When the current record is a visitor, the first tab in the window changes from Cardholder to Visitor and will display the appropriate fields.

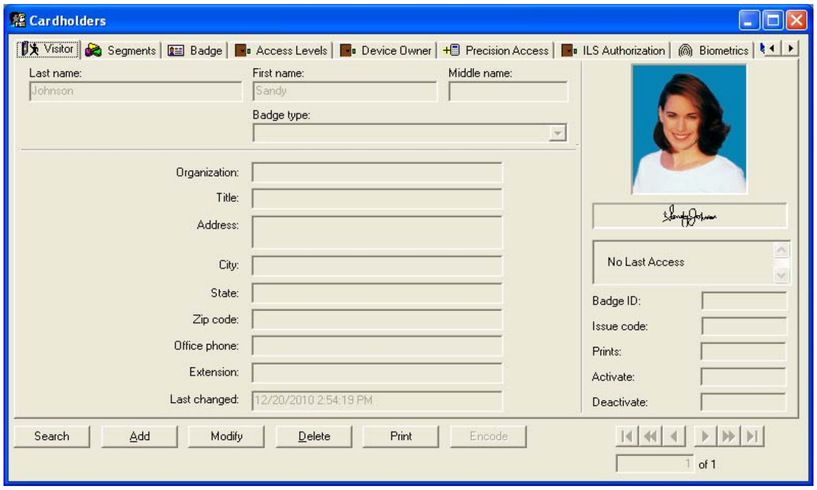
If you select the [Add] button on the Cardholder form, or the [Search] button on any of the forms in the Cardholders folder, the **Person type** drop-down list is displayed in the bottom section of the form.

The drop-down list choices are:

- All - when selected, your search will locate both Cardholder and Visitor records
- Cardholders - when selected, your search will only locate cardholder records
- Visitors - when selected, your search will only locate visitor records

Notes: With the exception of the **Allowed visitors** check box and the [Capture] button (in modify mode only) on the Visits form, visit records cannot be added, modified, or deleted from the Cardholders folder. To add, modify, or delete visits, you must purchase Visitor Management.

The availability of this form is subject to licensing restrictions.



Last name: Johnson

First name: Sandy

Middle name:

Last changed: 12/20/2010 2:54:19 PM

No Last Access

Cardholders Folder - Visitor Form

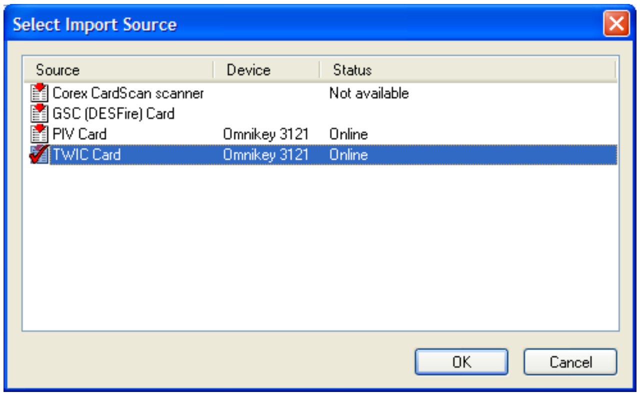
Form Element	Comment
Visitor data	Displayed in view mode. When adding or modifying a visitor record, enter the visitor's information such as name, address and organization into these fields.
Last changed	Displayed in view mode and indicates the date on which the selected visitor record was last modified and saved. This date is updated only when visitor information is changed, not when badge information is changed. The last changed date is saved individually for each badge record as well.

Visitor Form Procedures

Import Visitor Data

For more information, refer to Import Cardholder/Visitor Data on page 75.

1. In Alarm Monitoring, select **Badge Info** from the **View** menu. In all other applications, select **Cardholders** from the **Administration** menu.
2. The Cardholders folder opens. Click [Add].
3. Click [Import].
4. In the Select Import Source dialog, select the import source available for this workstation. Click [OK].



Source	Device	Status
Corex CardScan scanner		Not available
GSC (DESFire) Card		
PIV Card	Omnikey 3121	Online
✓ TWIC Card	Omnikey 3121	Online

Note: Import sources are configured in System Administration under the Workstations folder > Encoders/Scanners form.

5. Follow the instructions that display. They should explain how to scan and execute the import data transaction.

Add a Visitor Record

1. Select **Cardholders** from the **Administration** menu. The Cardholders folder opens. By default, the Cardholder form is displayed.
2. Click [Add].
3. From the **Person type** drop-down list, select **Visitors**.
4. Enter the visitor’s name and any additional information in the visitor data fields.

Note: You can switch to other tabs and modify the other forms at this time.

5. If you want to add a photograph or signature to the visitor record, click [Capture]. Multimedia Capture opens. For more information, refer to Appendix A: Multimedia Capture on page 187.
6. Click [OK] to save the record.

Modify a Visitor Record

1. Locate the visitor record you want to change.
2. Click [Modify].
3. Make the changes you want to the record.
4. Click [OK] button to save the changes, or the [Cancel] button to revert to the previously saved values.

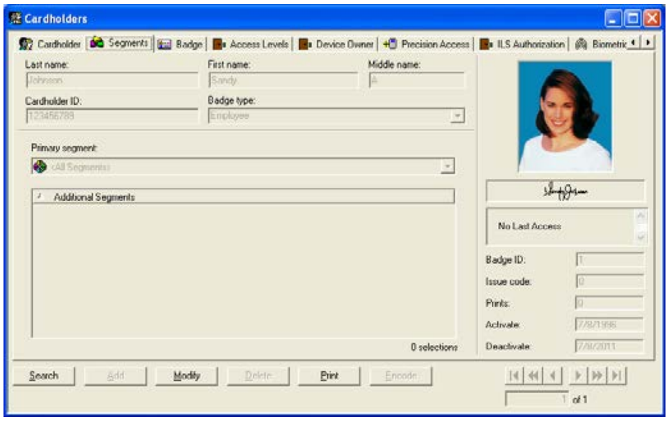
Delete a Visitor Record

1. Locate the visitor record you want to delete.
2. Click [Delete].
3. Click [OK].

Note: If you delete the visitor record, all associated records (Badge, Access Levels, Precision Access, Biometrics, Assets, Directory Accounts, Guard Tours and Visits) for the visitor are also removed from the database.

Segments Form

Note: The Segments tab is only displayed if segmentation is enabled on your system.



Last name: Johnson

First name: Sandy

Middle name: A

Cardholder ID: 123456789

Badge type: Employee

Primary segment: <All Segments>

No Last Access

Badge ID: 1

Issue code: 0

Prints: 0

Activate: 7/8/1998

Deactivate: 7/8/2011

0 selections

Segments Form Overview

With segmentation enabled you may see “Restricted Entry” in the cardholder drop-down boxes. This simply means you do not have the segment permissions to view the currently configured item for cardholder.

The Segments form is used to:

- Modify a cardholder’s segment assignment.
- Change a group of cardholder’s segments.

Cardholders Folder - Segments Form

Form Element	Comment
Primary segment	In modify mode, select which primary segment you want the selected cardholder to be assigned to. A cardholder can be assigned to a primary segment and as well as additional segments.
Additional Segments listing window	Lists all of the segments that have been configured in the system.
Number of selections	Displays the number of segments that have been selected in the **Additional Segments** listing window. For example: 2 selections.

Segments Form Procedures

Modify a Cardholder’s Segment Assignment

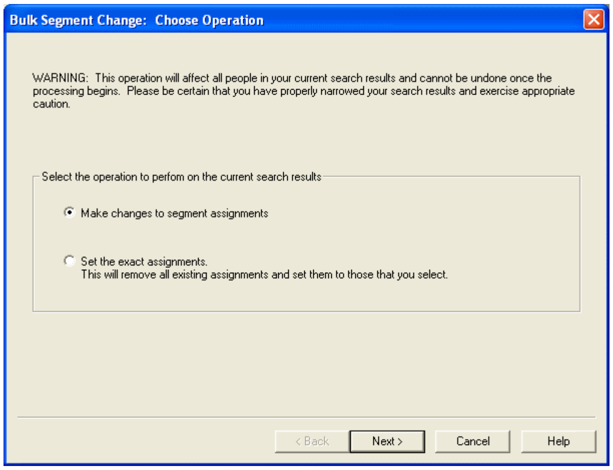
Note: This procedure cannot be performed in Visitor Management.

1. Select **Cardholders** from the **Administration** menu. The Cardholders folder opens.
2. Select the Segments tab.
3. Locate the cardholder record that you want to modify.
4. Click [Modify].
5. From the **Primary segment** drop-down list, select which primary segment you want the selected cardholder to be assigned to.
6. If you want to assign additional segments (if any exist), click on an entry in the **Additional Segments** listing window to select it. You can select multiple entries.
7. Click [OK].

Change a Group of Cardholder's Segments

Note: This procedure cannot be performed in Visitor Management.

1. Locate the group of cardholder records you want to change.
2. Select **Bulk** > **Change Cardholder Segments** from the **Cardholder** menu. The **Bulk Segment Change** window opens.



Bulk Segment Change: Choose Operation

WARNING: This operation will affect all people in your current search results and cannot be undone once the processing begins. Please be certain that you have properly narrowed your search results and exercise appropriate caution.

Select the operation to perfom on the current search results

● Make changes to segment assignments

○ Set the exact assignments.
This will remove all existing assignments and set them to those that you select.

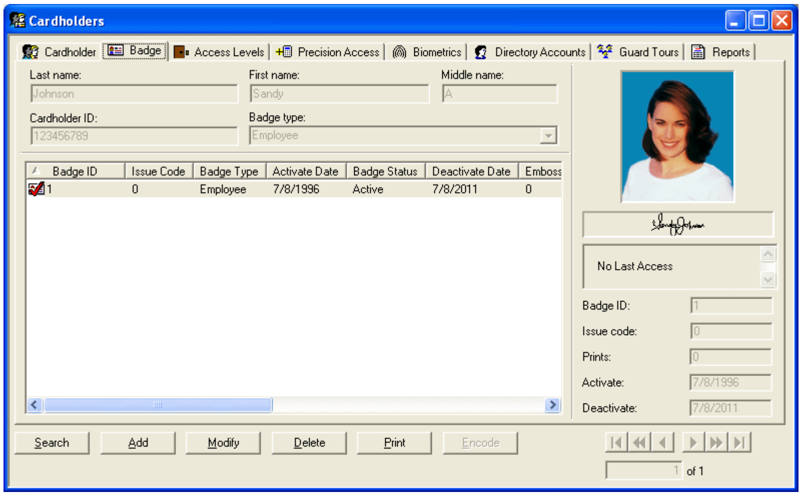
3. Select the **Make changes to segment assignments** radio button or select the **Set the exact assignments** radio button if you want all assignments that

exist for the cardholders in your group to be replaced with the new assignments you select.

4. Click [Next].
5. Select which primary segment you want the selected groups of cardholders to be assigned to.
6. If you selected the **Set the exact assignments** radio button in step 3, and if you want to assign additional segments (if any exist), click on an entry in the **Segments** listing window to select it. You can select multiple entries.
7. Click [Next]. If you selected "All Segments" in step 5, proceed to step 10.
   If you selected the **Make changes to segment assignments** radio button in step 3:
   a. From the **Segments** listing window, select any assignments you want to add in addition to the primary segment.
   b. Click [Next].
   c. If there are segment assignments you want to remove from the group, click on an entry in the **Segments** listing window to select it. You can select multiple entries.
   d. Click [Clear] to remove the assignment.
   e. Click [Next].
8. If you want to perform preliminary validation and be prompted with the results before proceeding, select the **Perform preliminary validation and prompt for confirmation** radio button. Select the **Prompt only if a problem is found** check box if you do not want to a prompt for confirmation if there is no validation problem.
   If you do not want to be prompted, select the **Skip preliminary validation and perform the operation without prompting** radio button.
9. Click [Next].
10. Click [Finish].
    - If you selected the **Skip preliminary validation and perform the operation without prompting** radio button in step 8 or if you selected "All Segments" in step 5, the **Bulk Action Results** window opens and displays a summary of your modifications. Click [OK].
    - If you selected the Perform preliminary validation and prompt for confirmation radio button in step 8 and a problem was found, the Bulk Segment Validation Results window opens.
      a. Click [View Badges]. An explanation of the problem is displayed.
      b. Click [OK].
      c. Click [Continue]. The **Bulk Action Results** window opens and displays a summary of your modifications.
      d. Click [OK].

Badge Form

Badge Form (View Mode)



Last name: Johnson

First name: Sandy

Middle name: A

Cardholder ID: 123456789

Badge type: Employee

Badge ID	Issue Code	Badge Type	Activate Date	Badge Status	Deactivate Date	Emboss
1	0	Employee	7/8/1996	Active	7/8/2011	0

Badge ID: 1

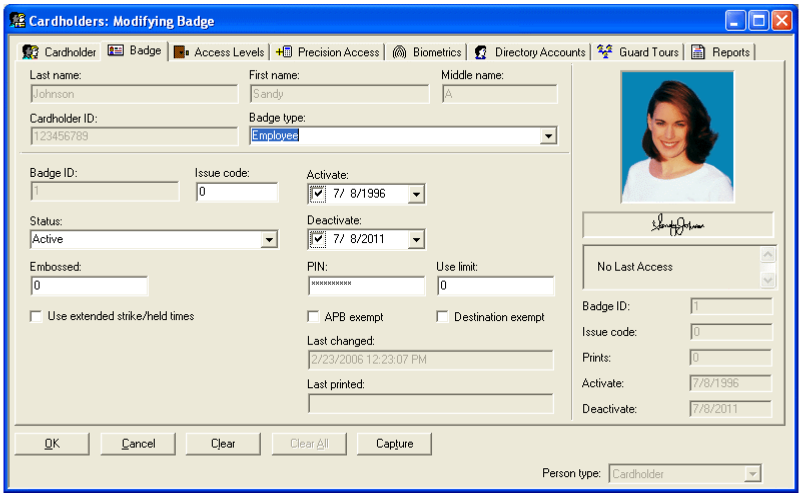
Issue code: 0

Prints: 0

Activate: 7/8/1996

Deactivate: 7/8/2011

Badge Form (Modify Mode)



Last name: Johnson

First name: Sandy

Middle name: A

Cardholder ID: 123456789

Badge type: Employee

Badge ID: 1

Issue code: 0

Activate: ☑ 7/ 8/1996

Status: Active

Deactivate: ☑ 7/ 8/2011

Embossed: 0

PIN: **********

Use limit: 0

□ Use extended strike/held times

□ APB exempt

□ Destination exempt

Last changed: 2/23/2006 12:23:07 PM

Last printed:

Badge ID: 1

Issue code: 0

Prints: 0

Activate: 7/8/1996

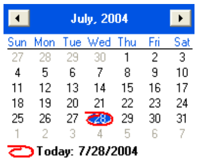
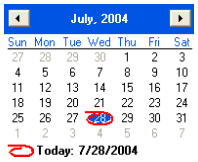
Deactivate: 7/8/2011

Person type: Cardholder

Cardholders Folder - Badge Form

Form Element	Comment
Badge listing window	Displayed in view mode. Lists all badges for the selected cardholder. If you right-click on a badge in this listing window, the following options are available: • One Free Pass - If selected, allows the selected badge to violate anti-passback rules one time. This is the same as selecting **One Free Pass** from the **Cardholder** menu. • APB Move Badge - If selected, displays the Area Move Badges window from where you can move a badge to a new area. This is the same as selecting **APB Move Badge** from the **Cardholder** menu. • Encode - If selected, displays the Encode Badge window from where you can encode the badge configurations selected for this badge onto a smart card. This is the same as clicking [Encode]. • Encoding History - Displays historical encoding information for the selected badge including card format, type, encoding count, and last time encoded. • Import Badge - Displays the Import Card window, in which you may select a reader to import cards from. • Import Badge ID - Displays the Encoder selection list window, in which you may select an encoder to read a badge ID from. In order for this option to be available for selection and function correctly: An encoder with the **Device type** “Digion24 (MIFARE)” must be configured in **Administration** > **Workstations** > Encoders/Scanners tab. The selected badge must be associated with a badge type that has “Import from card” selected in the **Generate badge ID** field in **Administration** > **Badge Types** > Badge ID Allocation tab > ID Allocation sub-tab. The system should have **Maximum badge number length** set to “10” in **Administration** > **System Options** > Hardware Settings tab.
Badge ID	Displayed in add or modify mode. Indicates the numeric identifier that is assigned to this badge. The maximum Badge ID length is determined in System Administration or ID CredentialCenter in the System Options folder > Hardware Settings form (non-segmented systems) or the Segments folder > Segments form > Hardware Settings sub-tab (segmented systems).
Issue code	Displayed in add or modify mode. Indicates the selected badge's issue code if your installation uses issue codes on its badges.

Cardholders Folder - Badge Form (Continued)

Form Element	Comment
Activate	Displayed in add or modify mode. Indicates the date when the selected badge becomes valid. The current date (at the time the badge record is created) is entered by default, but you can change this value by typing a numeric date into the field, or by selecting a date from the drop-down calendar.  ◄ July, 2004 ► Sun Mon Tue Wed Thu Fri Sat 27 28 29 30 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 Today: 7/28/2004 • To select a month, click on the ◄ and ► navigation buttons. • You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it. • Navigate to a year by clicking on the displayed year to access the year spin buttons 2003 ⇕. • Once you have selected a month and a year, click on the day that you want the selected badge to activate on.
Deactivate	Displayed in add or modify mode. Indicates the date when the selected badge becomes invalid. A default date is assigned based on the **Badge type**, but you can change this value by typing a numeric date into the field, or by selecting a date from the drop-down calendar.  ◄ July, 2004 ► Sun Mon Tue Wed Thu Fri Sat 27 28 29 30 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 1 2 3 4 5 6 7 Today: 7/28/2004 • To select a month, click on the ◄ and ► navigation buttons. • You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it. • Navigate to a year by clicking on the displayed year to access the year spin buttons 2003 ⇕. • Once you have selected a month and a year, click on the day that you want the selected badge to deactivate on.
Status	Displayed in add or modify mode. Indicates the badge status for the selected badge. Status drop-down list choices are defined on the Simple Lists form of the List Builder folder.

Cardholders Folder - Badge Form (Continued)

Form Element	Comment
PIN	Displayed in add or modify mode. Indicates the personal identification number for the selected badge. PIN numbers are used in conjunction with card readers that are operating in “Card and Pin,” or “Pin or Card,” mode. The maximum PIN length is determined by the **PIN type** field in the Access Panels folder. For increased security, PIN codes are not viewable by any user. However, if the system is configured to randomly generate a new PIN code when adding a badge, the user can see the PIN code when they first add the badge (but not later).
Use limit	Displayed in add or modify mode. Imposes a restriction on the number of times a cardholder can use his/her badge at readers marked with the “Enforce Use Limit” option. A use limit value of zero (0) indicates that a badge has no uses at readers that enforce a use limit. A use limit value of 255 or that is left empty indicates that the badge has unlimited uses. **Note:** Users who have upgraded to this current build should note that the Use Limit feature has changed. Having a use limit of “0” no longer means unlimited. It now means none. A use limit of “255” now means unlimited. Also, performing a download of your system will no longer reset the uses count. **Note:** When the use limit for a badge is modified the uses left are updated to reflect the new use limit assigned. For example, if you have 10 total uses and have already used 5 (so 5 are left), and you increase the Use limit to 15, the panel will be updated so the uses left will be 10. Conversely if you have a badge with 10 total uses and have already used 5 (so 5 are left), and you decrease the Use Limit count to 8, the panel will be updated so the uses left will be 3. **Note:** Making changes to the use limit feature while your system is offline with the host may cause the badges to become out of synch with the panel.
APB exempt	Displayed in add or modify mode. When this check box is selected, any anti-passback violation for the selected badge will granted access into the anti-passback area with no violation noted in the Alarm Monitoring application.
Destination exempt	Displayed in add or modify mode. Select this check box if you want the selected badge record to be exempt from destination assurance processing. When selected, the badge will not be included in the destination assurance processing and no alarms will be generated if the cardholder violates any of the destination assurance settings. Via the Reports folder, you can run a Destination Assurance Exempt Cardholders report to see a list of which cardholders will be exempt from processing. For more information, refer to the Destination Assurance Folder chapter in the System Administration User Guide.
Use extended strike/held times	Displayed in add or modify mode. When this check box is selected, extended held open and extended strike times will be used for the selected badge. **Note:** This option is supported by Bosch hardware only.
Override blocking	Select this to give the cardholder assigned to this badge the ability to unlock a door that has been blocked with a blocking card. Locks are blocked to deny entrance in unusual cases such as a police investigation. It is important to leave this field deselected unless you are certain the user of this badge template should be able to open a blocked lock. For more information, refer to “Configure Blocking Cards for ILS Integra Locks” and “Configure Special Purpose Cards for ILS Offline/Wireless Locks” in the System Administration User Guide.

Cardholders Folder - Badge Form (Continued)

Form Element	Comment
Embossed	Displayed in add or modify mode. If applicable, enter in this field any numbers or characters that are embossed on the card. Typically this applies to Proximity cards, which are embossed by the manufacturer prior to delivery.
Default floor	Indicates which floor number is called by default when the badge is presented to a reader associated with the DEC (elevator terminal). Configure the Default floor -128 to 127. **Note:** Ensure the **Default floor** and its **Default door** is included in the **Allowed Floors** configured for the elevator terminal. **Note:** This field is only available when elevator dispatching is configured.
Default door	Indicates which elevator door (front or rear) is opened at the **Default floor** when the badge is presented to a reader associated with the DEC (elevator terminal). **Note:** This field is only available for elevator terminals associated with a version “V2” DES or DER elevator dispatching device.
Last changed	Displayed in add or modify mode. Indicates the date when the selected badge record was last saved.
Last printed	Displayed in add or modify mode. Indicates the most recent date that the selected badge was printed.

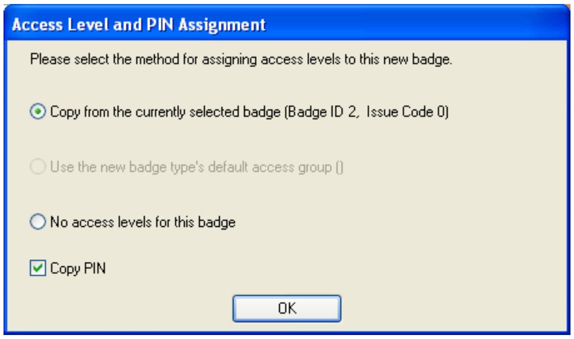
Badge Form Procedures

Add or Replace a Badge Record

1. In Alarm Monitoring, select **Badge Info** from the **View** menu. In all other applications, select **Cardholders** from the **Administration** menu.
2. Locate the existing cardholder/visitor record.
3. On the Badge tab, click [Add].
4. Select the badge type.
5. Enter the badge activation and deactivation dates.
6. Depending on how badge ID allocation is configured, you may need to manually enter a badge ID.
7. If the badge will be used for access control and access requires a card and/or personal identification number (PIN), ask the cardholder/visitor to enter a PIN.

Note: The length of PIN codes is configured in System Administration under the Access Panels folder > Options sub-tab and the Cardholder Options folder. If a PIN code is configured to be n-digits long and a cardholder enters a PIN code longer than n, the PIN code gets downloaded with the badge record, but gets truncated at n digits. For example, if a cardholder enters “123456” and the PIN type is 4-digits, then “1234” gets downloaded.

8. Enter any additional information and click [OK].
9. If this is the only active badge assigned to the cardholder/visitor, you are finished. Otherwise, continue with the next step.
10. If the cardholder/visitor record already has an active badge, the Change Badge Status dialog opens, prompting you to change the status of the “old” badge. To do this:
    a. Verify the current active (old) badge is selected.
    b. Select the new status from the **New Status** drop-down list. Choices include the default badge status values, and any badge status values that were added in the List Builder folder.
    c. Click [OK].
    d. The Access Level and Pin Assignment dialog opens, prompting you to assign an access level and PIN to the recently added (new) badge.



Access Level and PIN Assignment

Please select the method for assigning access levels to this new badge.

● Copy from the currently selected badge (Badge ID 2, Issue Code 0)

○ Use the new badge type's default access group ()

○ No access levels for this badge

☑ Copy PIN

Note: Select the No access levels for this badge radio button to manually assign access levels or to not assign access levels at all.

e. Click [OK].

Modify a Badge Record

1. Locate the badge record you want to change.
2. Click [Modify].
3. Make the changes you want to the record.

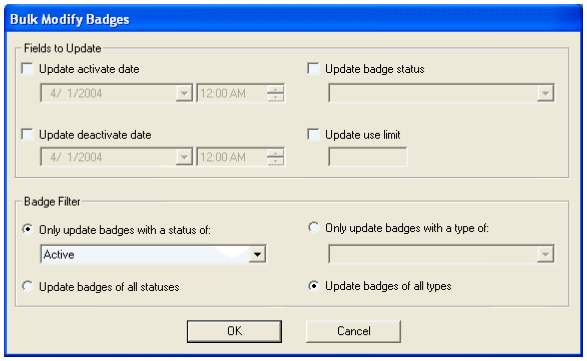
Note: If the PIN type is modified on the Access Panel and/or the General Cardholder Options form, you must log off/log on before you modify a cardholder's pin number.

4. Click [OK] to save the changes, or the [Cancel] button to revert to the previously saved values.

Modify Badges for a Selected Group of Cardholders

Note: This procedure cannot be performed in Visitor Management.

1. Locate the group of cardholders whose records you want to modify.
2. Select **Bulk** > **Modify Badges** from the **Cardholder** menu. The Bulk Modify Badges window opens.



Bulk Modify Badges

Fields to Update

☐ Update activate date 4/ 1/2004 12:00 AM

☐ Update badge status

☐ Update deactivate date 4/ 1/2004 12:00 AM

☐ Update use limit

Badge Filter

● Only update badges with a status of: Active

○ Only update badges with a type of:

○ Update badges of all statuses

● Update badges of all types

3. If you want to update the activation date, deactivation date, badge status, or use limit, do so in the Fields to Update section.

Note: The **Update use limit** field refers to the number of times a cardholder can use a badge at readers marked with the "enforce use limit" option. If you do update the use limit and leave the field empty it will be set to 255 (unlimited uses). In previous versions of ReadykeyPRO this would be set to 0, which now means 0 (or no) uses. Also note that a bulk use limit change updates a cardholder's previous use number. So, if a badge originally was set to 5 uses, and has already used 3, and then a bulk update changed the use limit to 4, then the badge would only have 1 use left.

4. If you want to filter which badges from the selected group get modified, do so in the Badge Filter section. You can filter by badge status and/or badge type.
5. If you do not want to filter badges, select the **Update badges of all statuses** and/or **Update badges of all types** radio buttons.
6. Click [OK]. A message displays asking if you want to continue with the modification.
7. Click [Yes]. The Bulk Action Results window opens and displays a summary of your modifications.
8. Click [OK].

Encoding Prerequisites

Several steps must occur in ReadykeyPRO to properly encode a magnetic, Wiegand, or smart card. Each step occurs in a different folder in the ReadykeyPRO application.

1. In the Workstations folder > Encoding form, configure an inline or standalone encoder/scanner.

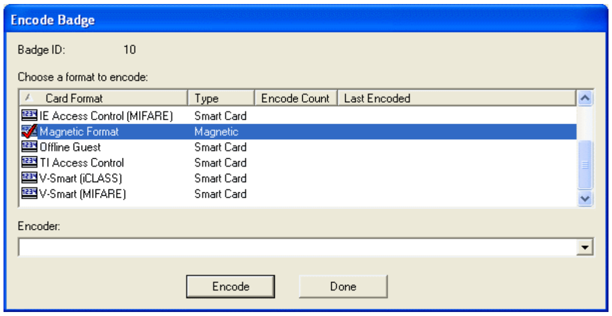
Note: You do not need to configure USB encoders/scanners (e.g. MIFARE Pegoda contactless smart card reader) in ReadykeyPRO applications. Simply install the drivers and attach the hardware to the workstation. This does not apply to the ScanShell 800-R/1000-A.

2. In the Card Formats folder, create a card format that will contain data to be encoded on a badge.
3. In the Badge Types folder > Encoding form, assign an encoding format to a badge type. In other words, assign a card format to be encoded on a badge of a specific type.
4. In the Cardholders folder, add a cardholder or visitor record to the database.
5. In Multimedia Capture, capture the cardholder/visitor’s photo, signature, and/or biometric data.
6. In the Cardholders folder, encode the badge.

Encode a Badge

This procedure assumes the magnetic encoder has been set up and configured in System Administration on the **Administration** > **Workstations** > Encoders/ Scanners form.

1. Display a cardholder/visitor in the Cardholders folder. You can do this by enrolling a cardholder or searching for one or several cardholders.
2. Click [Encode]. The Encode Badge window opens.



Badge ID: 10

Choose a format to encode:

Card Format	Type	Encode Count	Last Encoded
IE Access Control (MIFARE)	Smart Card		
Magnetic Format	Magnetic		
Offline Guest	Smart Card		
TI Access Control	Smart Card		
V-Smart (iCLASS)	Smart Card		
V-Smart (MIFARE)	Smart Card		

Encoder:

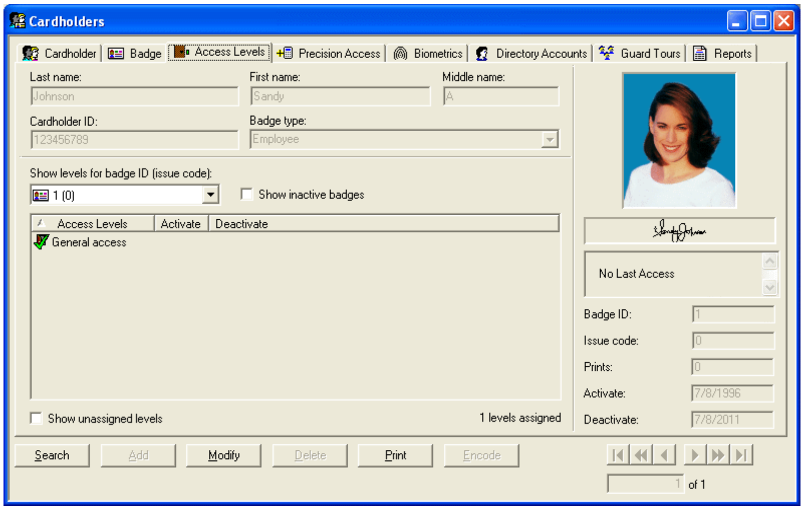
3. Select a format to encode and an **Encoder**, then click [Encode].
4. Follow the instructions that display on your monitor.

Delete a Badge Record

1. Locate the badge record you want to delete.
2. Click [Delete].
3. Click [OK].

Access Levels Form

Access Levels Form (View Mode)



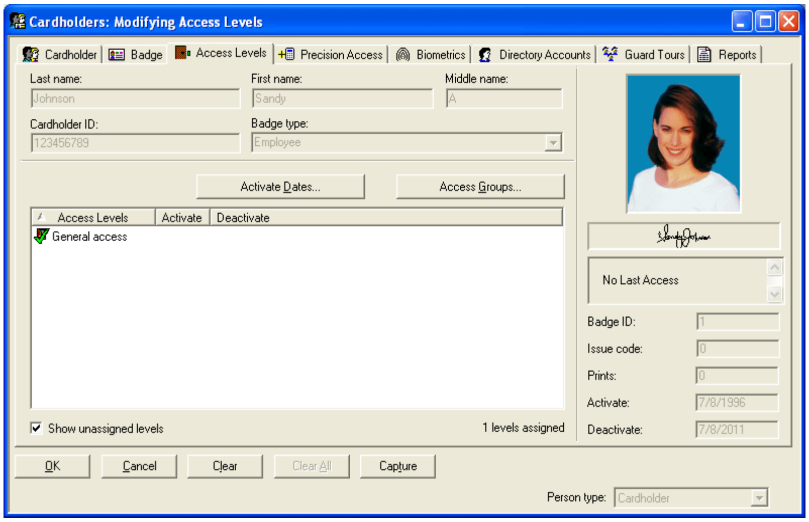
Last name: Johnson
First name: Sandy
Middle name: A
Cardholder ID: 123456789
Badge type: Employee
Show levels for badge ID (issue code): 1 (0)
☐ Show inactive badges

Access Levels	Activate	Deactivate
General access		

☐ Show unassigned levels
1 levels assigned

No Last Access
Badge ID: 1
Issue code: 0
Prints: 0
Activate: 7/8/1996
Deactivate: 7/8/2011
1 of 1

Access Levels Form (Modify Mode)



Last name: Johnson
First name: Sandy
Middle name: A
Cardholder ID: 123456789
Badge type: Employee

Access Levels	Activate	Deactivate
General access		

☑ Show unassigned levels
1 levels assigned

No Last Access
Badge ID: 1
Issue code: 0
Prints: 0
Activate: 7/8/1996
Deactivate: 7/8/2011
Person type: Cardholder

Cardholders Folder - Access Levels Form

Form Element	Comment
Show levels for badge ID (issue code)	Displayed in view mode. Lists the badge ID and issue code (in parentheses) for the current active badge. If the **Show inactive badges** check box is selected, the list includes both the active and the inactive badge(s) assigned to the selected cardholder. Select a badge ID (issue code) from the list and the corresponding access levels for that badge will be displayed in the **Access levels** display.

Cardholders Folder - Access Levels Form (Continued)

Form Element	Comment
Show inactive badges	Displayed in view mode. When selected, the **Show levels for badge ID (issue code)** drop-down list will list both the active and inactive badge(s) assigned to the selected cardholder.
Access levels display	Displayed in a view and modify mode. When the **Show unassigned levels** check box is selected, lists both access levels that **have been** and that **can be** assigned to the selected cardholder/badge record. If the **Show unassigned levels** check box is not selected, only access levels that **have been** assigned will be listed. If they exist, also displays the access level's activation and deactivation dates.
Show unassigned levels	Displayed in view and modify mode. When selected, the **Access levels** display lists both access levels that **have been** and that **can be** assigned to the selected cardholder/badge record.
Number of levels assigned	Displayed in view and modify mode. Displays the number of access levels that have been assigned to the selected cardholder/badge record. For example: 6 levels assigned.
Intrusion Authority	**Note:** The authority levels assigned act as access levels. Make note of this as the maximum number of access levels is usually 32. This button is displayed in modify mode. When clicked, displays the Intrusion Authority Levels window from where you can assign intrusion authority levels. These levels will allow the cardholder the ability to issue commands via the keypad. For more information, refer to the Command Keypad Templates Folder in the System Administration User Guide.
Activate Dates	This button is displayed in modify mode. When clicked, displays the Access Level Activation Dates window from where you can select the dates when the selected access level will become valid and invalid.
Access Groups	This button is displayed in modify mode. When clicked, displays the Select Access Levels in a Group window from where you can choose the access level group that you want to select access levels from.

Access Levels Form Procedures

Note: HID Edge supports a maximum of eight (8) access levels per badge per Edge device. If you attempt to assign an access level to an HID badge that is over the 8 access levels per badge limit per device, it will not be assigned, and an error message will be displayed listing the 8 access levels already assigned to the badge.

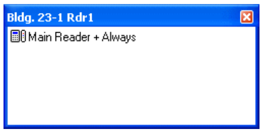
Assign Access Levels to a Badge

1. Select **Cardholders** from the **Administration** menu. The Cardholders folder opens.
2. Select the Access Levels tab.
3. Locate the cardholder record for which you want to assign access levels.
4. From the **Show levels for badge ID (issue code)** drop-down list, select the badge you want to assign access levels to.

Note: If the **Show inactive badges** check box is selected, the **Show levels for badge ID (issue code)** drop-down list will list both the active and inactive badge(s) assigned to the selected cardholder.

5. Click [Modify].
6. Select the **Show unassigned levels** check box. The **Access levels** display will list both access levels that **have been** and that **can be** assigned to the selected cardholder/badge record.

Note: To find out more about a particular access level, either double-click on an access level entry, or right-click on an access level entry and select **Level Definition**. A popup window opens, listing the reader/time zone combinations that define the access level. For example:

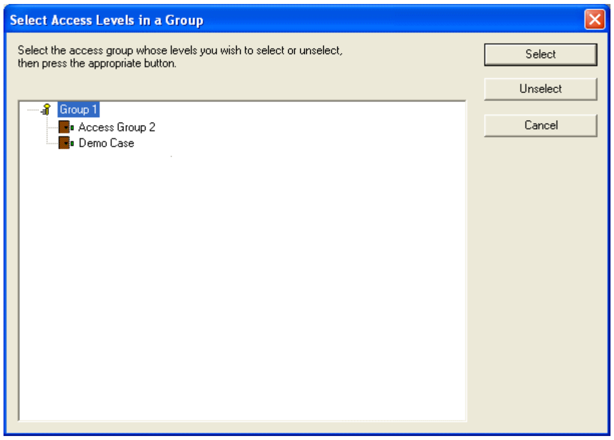


Bldg. 23-1 Rdr1

Main Reader + Always

7. Click on an access level in the **Access levels** display to select it. Optional: If you want to assign all the access levels that belong to an access group:

    a. Click [Access Groups]. The **Select Access Levels in a Group** window opens.



Select Access Levels in a Group

Select the access group whose levels you wish to select or unselect, then press the appropriate button.

- Group 1
  - Access Group 2
  - Demo Case

    b. The **Select Access Levels in a Group** window lists all currently defined access groups. You can expand an entry to display the list of access levels that make up a group. Select an access level or an access group. If you select an access group, you select all of the access levels it contains.

    c. Click [Select].

    d. Click [Yes].

8. Repeat step 7 for each access level you want to assign.

9. Click [OK].

Assign Intrusion Authority to the Cardholder

1. On the Access Levels form, click [Modify].

2. Click [Intrusion Authority]. The Intrusion Authority Levels window opens.

3. Select what access levels you would like to assign Level 1 and/or Level 2 authority.

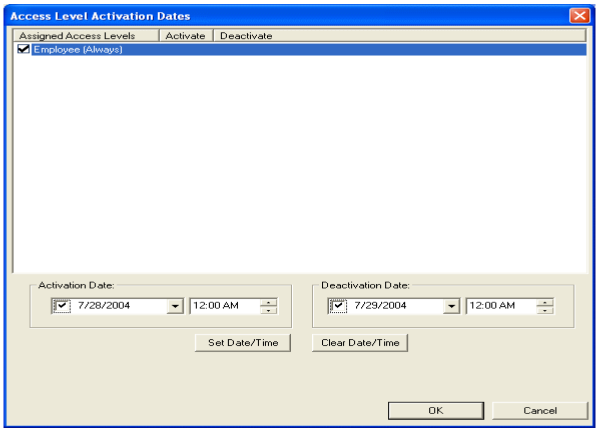
4. Click [OK]. On the access levels listing window you will see an intrusion authority column that shows you what intrusion authority level(s) that access level now shares.

Important: The authority levels assigned act as access levels but do not count toward the maximum number of access level assignment allowed per badge. When the

“Advanced Permission Control” intrusion command configuration option is selected, the maximum number of access level assignments allowed per badge is reduced to 30.

Assign Activation and Deactivation Dates to Access Levels

1. On the Access Levels form, click [Modify].
2. The access levels listing window displays all access levels that are currently configured for use with the selected cardholder's badge type. From the listing window, select one or more access levels.
3. Click [Activate Dates]. The Access Level Activation Dates window opens. The selected access levels that have been assigned to the selected cardholder/badge record will be listed in the Assigned Access Levels listing window.

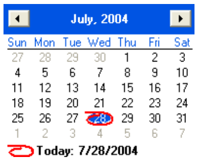


Assigned Access Levels	Activate	Deactivate
☑ Employee (Always)		

Activation Date: ☑ 7/28/2004 12:00 AM

Deactivation Date: ☑ 7/29/2004 12:00 AM

4. Click on an access level entry to select it.
5. In the Activation Date section:
   a. Type a numeric date into the field, or select a date from the drop-down calendar.



July, 2004

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Today: 7/28/2004

   - To select a month, click on the ◄ and ► navigation buttons.
   - You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.
   - Navigate to a year by clicking on the displayed year to access the year spin buttons 2003 ⬍.
   - Once you have selected a month and a year, click on the day that you want the selected badge to activate on.

   b. If your system is configured so that you can specify a specific activation time, enter a time in the field to the right of the date field. This time will be used in conjunction with the selected activation date.

Notes: To specify the activation time, the **Store expiration date** field on the Options sub-tab of the Access Panels form must be set to **Date only** or **Date and time**.

The activation time you enter should match the granularity setting on the Cardholder Options folder, General Cardholder Options form. Otherwise, the time you enter will be rounded down. For example if the granularity is set to 30 minutes, and you enter any time between 4:00 and 4:29 the time will automatically be rounded to 4:00. Any time entered between 4:31 and 4:59 will be rounded to 4:30.

6. In the Deactivation Date section, repeat step 5, choosing the date when you want the selected badge to become invalid.
7. Click [Set Date/Time].
8. Repeat steps 4-7 for each access level entry.
9. Click [OK].

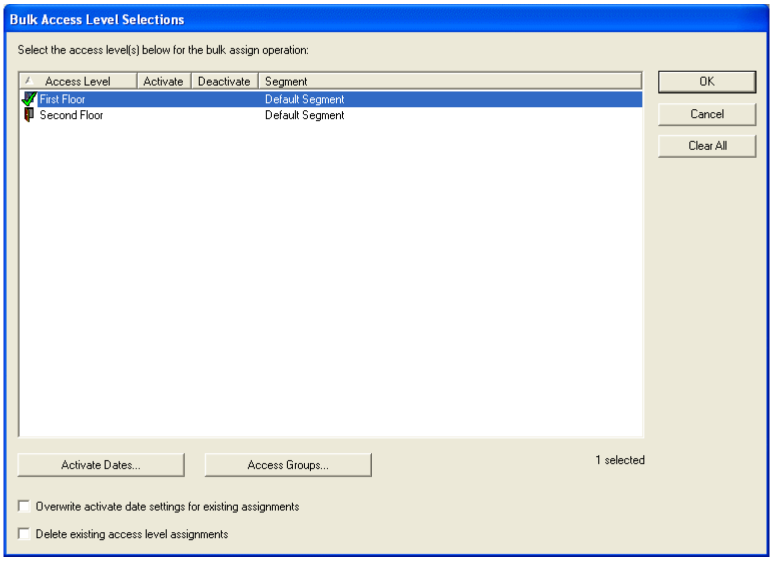
Assign Access Levels to a Selected Group of Cardholders

Important: The linkage server is required to be running for any bulk access level update. However, since the linkage server runs independently of System Administration it may take several minutes for the linkage server to finish processing any bulk updates even though System Administration indicates that the bulk update task is complete.

Note: HID Edge supports a maximum of eight (8) access levels per badge per HID controller. If you attempt to assign an access level that results in more than 8 access levels going to a badge for a single HID controller, the assignment will not be allowed, and an error message will display with a list of the 8 access levels already selected for this controller.

Note: This procedure cannot be performed in Visitor Management.

1. Locate the group of cardholders that you want to assign access levels.
2. Select **Bulk** > **Assign Access Levels** from the **Cardholder** menu. The Bulk Access Levels Selections window opens.



Select the access level(s) below for the bulk assign operation:

Access Level	Activate	Deactivate	Segment
✓ First Floor			Default Segment
Second Floor			Default Segment

1 selected

□ Overwrite activate date settings for existing assignments

□ Delete existing access level assignments

3. To modify access levels:
   a. Select (place a checkmark beside) the access level(s) you want to assign.
   b. If you want to assign an entire access group, click [Access Groups]. Highlight the access group and click [Select].

Note: You can expand access groups to display associated access levels. You can also double-click access levels to display associated readers

   c. Select the **Delete existing access level assignments** check box if you want to delete the existing access level assignments and apply the new access level assignments. If you do not select this check box, the cardholders will retain their existing access levels in addition to their new access level assignments.

4. To modify activation/deactivation dates:
   a. Click [Activate Dates].The Access Level Activation Dates dialog opens.

Note: Although you can assign multiple access levels to a record, you can only assign activation/deactivation dates to one access level at a time.

b. Select the first access level.

c. Set the activation and deactivation dates.

d. If there is more than one access level that you want to assign dates to, click [Set] and continue setting the activation/deactivation dates.

e. When you are finished, click [OK].

f. Select the **Overwrite activate date settings for existing assignments** check box to apply the new dates.

g. Click [OK] and acknowledge any messages that display.

Remove Access Levels From a Selected Group of Cardholders

Note: This procedure cannot be performed in Visitor Management.

1. Locate the group of cardholders that you want to remove access levels from.
2. Select **Bulk** > **Remove Access Levels** from the **Cardholder** menu. The **Bulk Access Levels Selections** window opens.
3. Click on the access level you want to remove to select it. You can select multiple entries.
   Optional: If you want to remove all the access levels that belong to an access group:
   a. Click [Access Groups]. The **Select Access Levels in a Group** window opens.
   b. The **Select Access Levels in a Group** window lists all currently defined access groups. You can expand an entry to display the list of access levels that make up a group. Select an access level or an access group. If you select an access group, you select all of the access levels it contains.
   c. Click [Select].
   d. Click [Yes].
4. Click [OK].

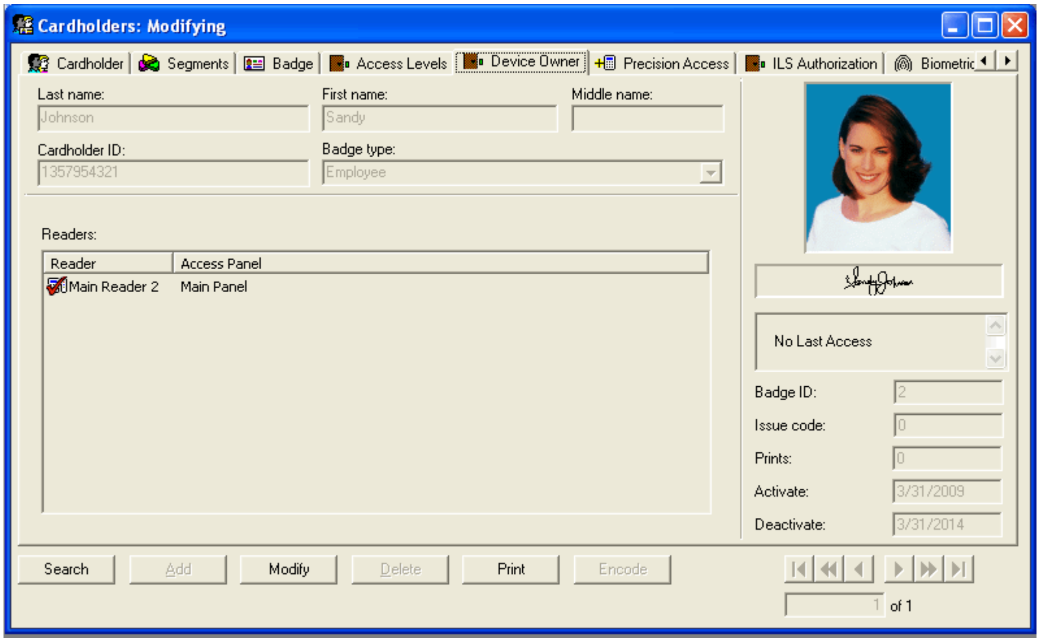
Note: **All** active badges will be affected by this change, even in multiple active badge environments.

Modify Access Levels Assignments

1. Locate the cardholder/badge record whose access level assignments you want to change.
2. Click [Modify].
3. Make the changes you want to the record.
    - Select the access level to assign it to a cardholder/badge record.
    - Deselect the access level to limit cardholder/badge access.
    - Click [Clear all] to deselect all the access level assignments.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

For more information, refer to NGP Procedures in the System Administration User Guide.

Device Owner Form



Last name: Johnson

First name: Sandy

Middle name:

Cardholder ID: 1357954321

Badge type: Employee

Readers:

Reader	Access Panel
☑ Main Reader 2	Main Panel

No Last Access

Badge ID: 2

Issue code: 0

Prints: 0

Activate: 3/31/2009

Deactivate: 3/31/2014

1

Cardholders Folder - Device Owner Form

Form Element	Comment
Readers listing window	Lists the reader device(s) for all of the access levels belonging to the displayed cardholder. Select the reader(s) that you want the cardholder to own.

Device Owner Form Procedures

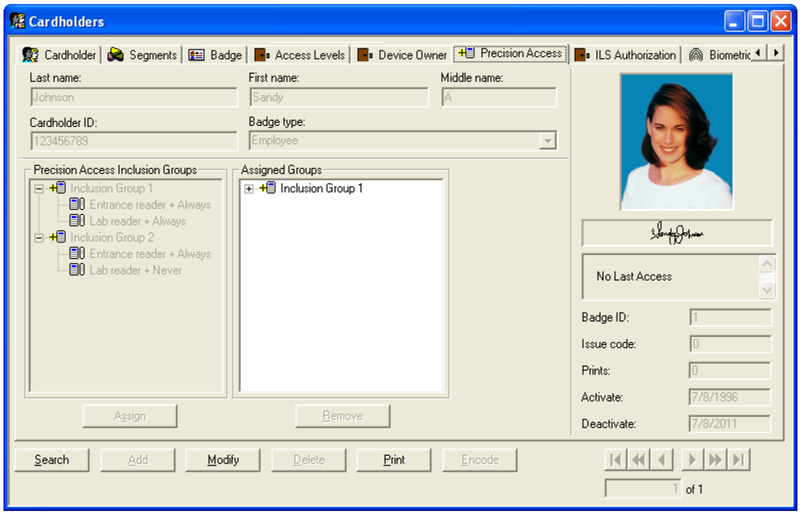
Assign a Cardholder to Own a Device

Important: To add or modify device owners you must have device owner permissions. For more information, refer to Cardholder Permission Groups Tree on page 374.

1. Select **Cardholders** from the **Administration** menu. The Cardholders folder opens.
2. Select the Device Owner tab.
3. Locate the cardholder record that you want to assign to be a device owner.
4. The Readers listing window is populated with the readers that the cardholder has access to. Select the reader(s) that you wish to make the cardholder owner of.
5. Click [OK].

Precision Access Form

Note: The Precision Access tab is only displayed if “Inclusion” is selected in the **Precision Access Mode** field on the General Cardholder Options form of the Cardholder Options folder in the System Administration software application.



Last name: Johnson
First name: Sandy
Middle name: A
Cardholder ID: 123456789
Badge type: Employee

Precision Access Inclusion Groups
- Inclusion Group 1
  - Entrance reader + Always
  - Lab reader + Always
- Inclusion Group 2
  - Entrance reader + Always
  - Lab reader + Never

Assigned Groups
- Inclusion Group 1

No Last Access

Badge ID: 1
Issue code: 0
Prints: 0
Activate: 7/8/1996
Deactivate: 7/8/2011

1 of 1

Cardholders Folder - Precision Access Form

Form Element	Comment
Precision Access Inclusion Groups	Lists all currently defined Inclusion groups (your system will have one or the other) and the readers and timezones/elevator control levels that belong to each. An +▦ icon precedes each inclusion group entry. Inclusion groups are defined on the Precision Access form of the Access Levels folder.
Assigned Groups	Lists the Inclusion Groups assigned to the selected cardholder/badge record.
Assign	Assigns to the selected cardholder/badge record the access levels selected in the Precision Access Inclusion Groups field.
Remove	Removes from the current cardholder/badge record the access levels selected in the Precision Access Inclusion Groups field.

Precision Access Form Procedures

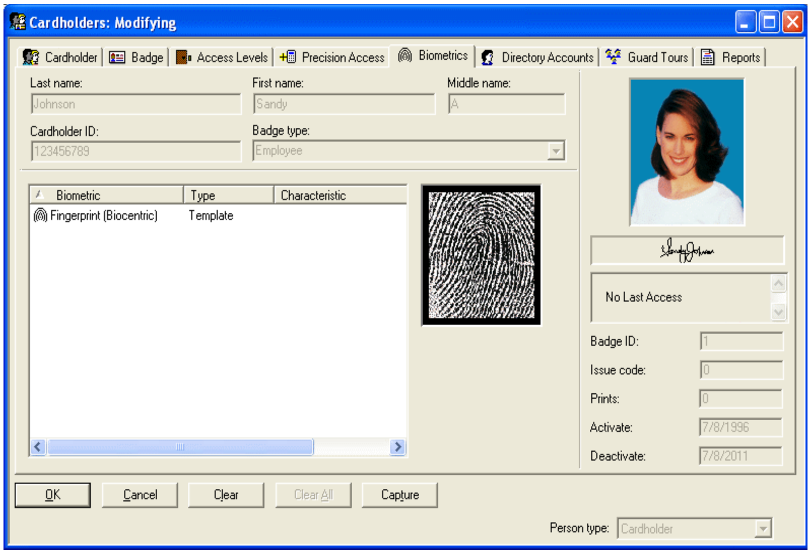
Assign Precision Access Groups to a Badge

1. Select **Cardholders** from the **Administration** menu.The Cardholders folder opens.
2. Select the Precision Access tab.
3. Locate the cardholder record that you want to assign precision access. Precision access can only be assigned to the selected cardholder's/visitor's active badge.
4. Click [Modify].
5. In the **Precision Access Inclusion Groups** window, select a precision access group.
    - The window contains all currently defined precision access groups. You can expand an entry to display the list of readers and timezones (if entries are Inclusion groups) that make up the group.
    - You can select only one group at a time.
    - By selecting a precision access group you select all of the reader-timezone combinations it contains. These combinations are defined on the Precision Access form of the Access Levels folder.
6. Click [Assign]. The group(s) you selected will be listed in the **Assigned Groups** window.
7. Repeat steps 5 and 6 for each additional group you want to assign to the badge. You can assign multiple Inclusion groups in addition to the 6 access levels that a cardholder can normally have.
8. Click [OK].

Remove Precision Access Groups From a Badge

1. Locate the record of the cardholder whose precision access assignment you want to remove.
2. In the **Assigned Groups** window, select the precision access group to be removed.
3. Click [Remove].
4. Repeat steps 2 and 3 for each precision access group you want to remove.
5. Click [OK].

Biometrics Form



Last name: Johnson
First name: Sandy
Middle name: A
Cardholder ID: 123456789
Badge type: Employee

Biometric	Type	Characteristic
Fingerprint (Biocentric)	Template	

No Last Access

Badge ID: 1
Issue code: 0
Prints: 0
Activate: 7/8/1996
Deactivate: 7/8/2011

Person type: Cardholder

Cardholders Folder - Biometrics Form

Form Element	Comment
Biometric listing window	In search mode, lists all biometric features and the type associated with each. In view mode, lists the selected cardholder's biometric information (if any exists). There are three biometric features, Fingerprint, Hand Geometry and Iris. A biometric fingerprint's type can be template or image.
Fingerprint image	Displayed in view mode. Displays a visual representation of the cardholder's fingerprint. For more information, refer to Appendix A: Multimedia Capture on page 187.
Search Type	Displayed in search mode. This field is used in conjunction with the listing window. Click on a biometric feature in the listing window and select a choice from the **Search Type** drop-down list to search for a record that **Has** or **Does Not Have** a fingerprint image, a fingerprint template, iris data, or a hand geometry template associated with the cardholder.

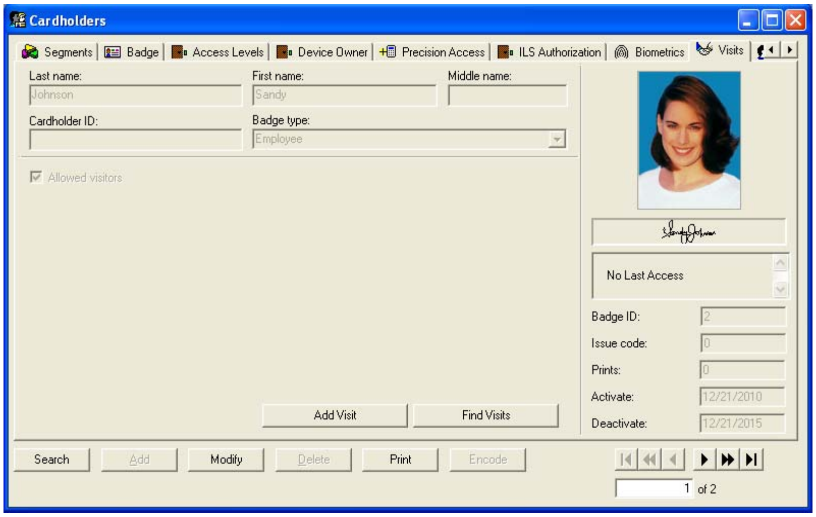
Biometrics Form Procedures

Search for a Cardholder’s Biometric Record

1. Select **Cardholders** from the **Administration** menu. The Cardholders folder opens.
2. Select the Biometrics tab.
3. Click [Search].
4. In the **Biometric** listing window, click on a biometric feature to select it.
5. Choose either “Has” or “Does Not Have” from the **Search Type** drop-down list to search for a record that has or does not have specific biometric data associated with the cardholder.
6. Click [OK].
   ReadykeyPRO retrieves and displays the first matching record. Use the ⏮, ⏪, ◀, ▶, ⏩ and ⏭ buttons to navigate through the database. A dimmed button means that the associated operation is not possible (e.g., moving to the next record while the last record is being displayed).

Visits Form

Visits Form (View Mode)



Last name: Johnson

First name: Sandy

Middle name:

Cardholder ID:

Badge type: Employee

☑ Allowed visitors

No Last Access

Badge ID: 2

Issue code: 0

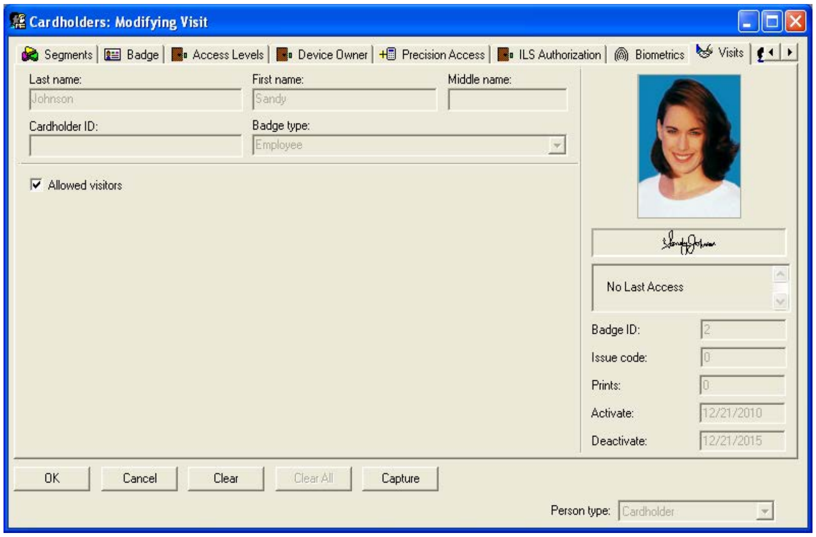
Prints: 0

Activate: 12/21/2010

Deactivate: 12/21/2015

1 of 2

Visits Form (Modify Mode)



Cardholders: Modifying Visit

Last name: Johnson

First name: Sandy

Middle name:

Cardholder ID:

Badge type: Employee

☑ Allowed visitors

No Last Access

Badge ID: 2

Issue code: 0

Prints: 0

Activate: 12/21/2010

Deactivate: 12/21/2015

Person type: Cardholder

Cardholders Folder - Visits Form

Form Element	Comment
Allowed visitors	When selected in modify mode, the selected cardholder is allowed to be assigned visitors. When not selected, the cardholder will not be available for visit assignment in the Visitor Management application.
Add Visit	In modify mode, click this button to display the Adding Visit window. From here you can add or modify visits, display visit records for a selected date range, and search for visit records based on the scheduled time in, scheduled time out, time in, time out, or date and time last changed.
Find Visits	This button quickly looks up visit records associated with the record whose name is specified in the **Last name**, **First name** and **Middle name** fields.
Type	Displayed in modify mode. Indicates the type of visit.
Purpose	Displayed in modify mode. Indicates the purpose of the visit.

Visits Form Procedures

Modify a Cardholder's Permission to Have Visitors

A cardholder must have permission to have visitors visit. This permission can only be granted (or taken away) in System Administration or ID

CredentialCenter, but not in Visitor Management. To change a cardholder's permission to have visitors:

1. Select **Cardholders** from the **Administration** menu.
2. Click the Cardholders tab.
3. Locate the record of the cardholder that you want to allow visitors.

Note: Cardholders who are visitors cannot be assigned visitors.

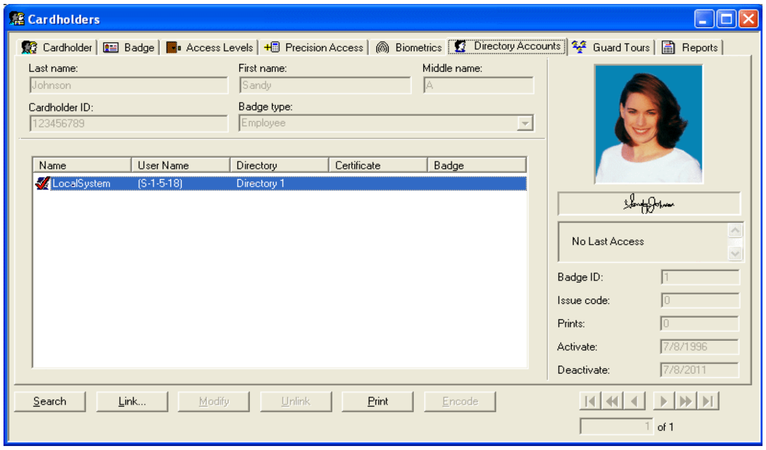
4. Click the Visits tab.
5. Click [Modify].
6. The **Allowed visitors** check box setting controls a cardholder's permission to have visitors. Select the setting you want for the selected cardholder. The two possible settings are:
   - When the **Allow visitors** check box is selected, the cardholder will be allowed to have visitors. Only cardholders with the Allow visitors check box will be returned when searching for a cardholder and attempting to add a new visit.
   - When the **Allow visitors** check box is not selected, no visits to the cardholder can be scheduled.

Note: Changing the **Allow visitors** check box setting for a cardholder will only change the cardholder's ability to have visitors after the setting has been changed; any previously scheduled visits will be allowed to occur.

7. Click [OK].

Directory Accounts Form

Note: The Directory Accounts form is not available in Visitor Management.



Last name: Johnson
First name: Sandy
Middle name: A
Cardholder ID: 123456789
Badge type: Employee

Name	User Name	Directory	Certificate	Badge
LocalSystem	{S-1-5-18}	Directory 1		

No Last Access

Badge ID: 1
Issue code: 0
Prints: 0
Activate: 7/8/1996
Deactivate: 7/8/2011

Cardholders Folder - Directory Accounts Form

Form Element	Comment
Directory accounts listing window	Lists the directory accounts that have been linked to the selected cardholder.
Link	When selected, displays the **Select Account** window from where you can link a directory account to the selected cardholder.
Unlink	When selected, unlinks the selected cardholder from the directory account that is selected in the Directory Accounts listing window.

Directory Accounts Form Procedures

Link a Cardholder to a Directory Account

Note: This procedure cannot be performed in Visitor Management.

1. Select **Cardholders** from the **Administration** menu. The Cardholders folder opens.
2. Select the Directory Accounts tab.
3. Locate the cardholder record for which you want to link a directory account.
4. Click [Link]. The Select Account window opens. In the Select Account window:
   a. In the **Directory** drop-down list, select the directory you wish to link to.
   b. In the **Field** drop-down list select whether to search for a name or user name.
   c. In the **Condition** drop-down list, select how the value will be related to the field. For example, a search where the **Field** selected is “Name”, the **Condition** selected is “contains” and the **Value** specified is “Lake” will display all accounts where the name contains the word “Lake”, such as Lisa Lake.
   d. In the **Value** field, type or select a word you think may be in the user name or name. If you leave this field empty, all accounts for the selected directory will be displayed when the search is executed.

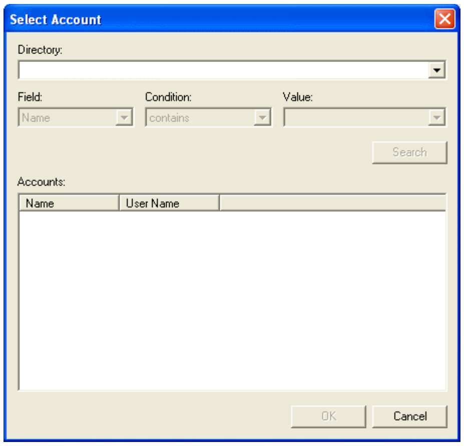
Note: To help you search, the **Value** field will contain different ways that the selected account may be expressed. For example, if the user account Lisa

Lake is selected, the permutations listed might be "L. Lake", "LISA", "Lisa", "Lisa L.", "Lisa Lake", "LL", "Lake" and "Lake, Lisa."

e. Click [Search].

f. The accounts associated with the selected **Directory** will be displayed in the Accounts listing window.

- If the account you wish to link to is displayed, select it. Your window should look similar to the following:



Field: Name

Condition: contains

Value:

- If the account you wish to link to is not displayed, return to step d and select another **Value** to search for.

g. Click [OK].

h. Repeat steps 3 and 4 for each directory account you wish to link to the selected user account.

5. Click the [OK] button on the Directory Accounts form.

Unlink a Directory Account

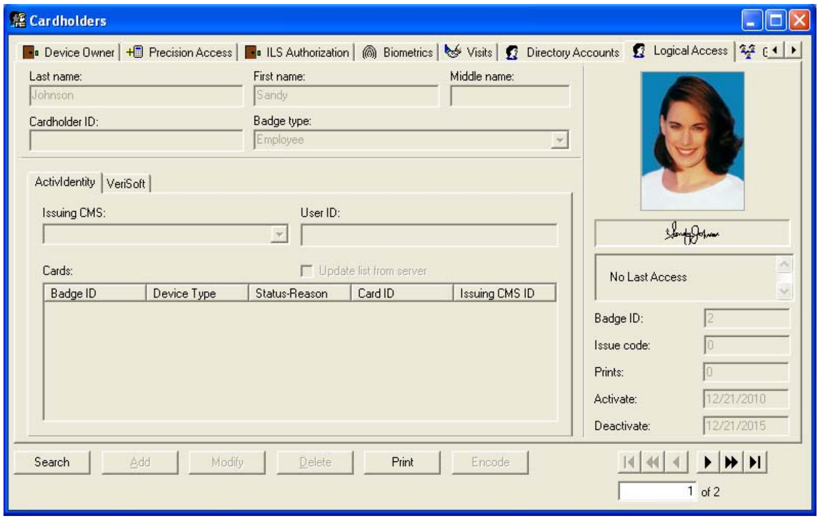
Note: This procedure cannot be performed in Visitor Management.

1. Locate the record of the cardholder you want to unlink a directory account from.
2. Click on an entry in the **Directory accounts** listing window to select it.
3. Click [Unlink].
4. Click [OK].

Logical Access Form

Before a badge can be issued to a user, the cardholder record for the user must have a logical user account linked to it on this form.

Displayed by: **Administration** > **Cardholders** > Logical Access form.



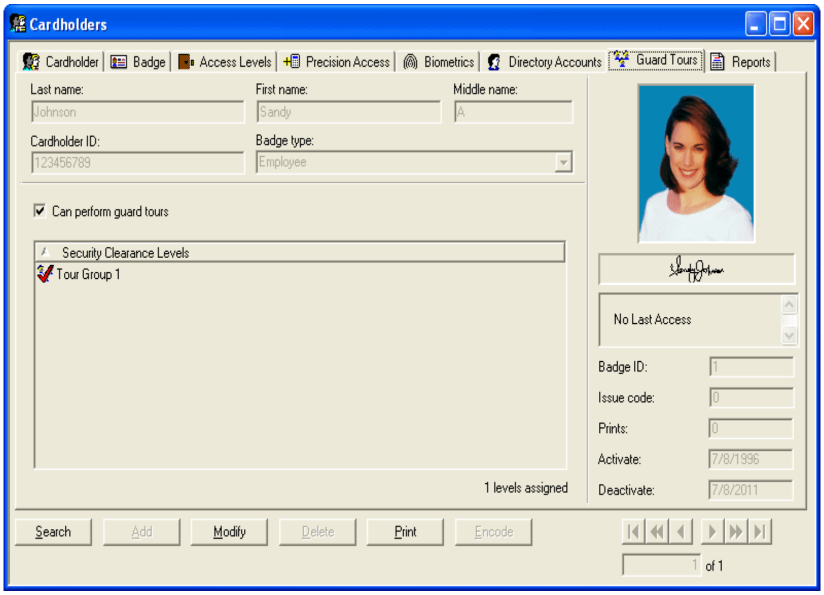
Last name: Johnson
First name: Sandy
Middle name:
Cardholder ID:
Badge type: Employee
No Last Access
Badge ID: 2
Issue code: 0
Prints: 0
Activate: 12/21/2010
Deactivate: 12/21/2015
1 of 2

Cardholders Folder - Logical Access Form

Form Element	Comment
Issuing CMS	The CMS that the user exists in. It will be the CMS that is connected to when issuing a badge to the cardholder.
User ID	The cardholder’s logical user account name.
Cards listing window	Lists all cards/badges that have been encoded or bound to the cardholder. Additional operations on the badge (such as resuming, suspending, terminating, or unlinking) can be performed by right-clicking on an entry in the list. • Resume • Suspend • Terminate • Unlink
Update from CMS	Allows badges that have been issued to the user outside of ReadykeyPRO to be displayed in the Cards listing window. Badges issued to users outside of ReadykeyPRO cannot be linked to a physical badge and thus do not support life cycle management.

Guard Tours Form

Note: The Guard Tours form is not available in Visitor Management.



Last name: Johnson

First name: Sandy

Middle name: A

Cardholder ID: 123456789

Badge type: Employee

☑ Can perform guard tours

Security Clearance Levels

Tour Group 1

1 levels assigned

No Last Access

Badge ID: 1

Issue code: 0

Prints: 0

Activate: 7/8/1996

Deactivate: 7/8/2011

1 of 1

Cardholders Folder - Guard Tours Form

Form Element	Comment
Can perform guard tours	Select this check box to if you want the selected cardholder to perform guard tours.
Security Clearance Levels listing window	Lists all security clearance levels that have been configured in the system. Security clearance levels are a means of limiting the number of tour guards to choose from when a tour is launched. Particular security clearance levels will be assigned only to guards who will need access to areas where a tour will take them. When a tour is launched, only guards with the appropriate security clearance level for that tour will be listed. Guard tours and security clearance levels are configured in the Guard Tour folder. **Note:** This field is enabled only if the **Can perform guard tours** check box is selected.
Number of levels assigned	Displays the number of security clearance levels that have been assigned to the selected cardholder. For example: 6 levels assigned.

Guard Tours Form Procedures

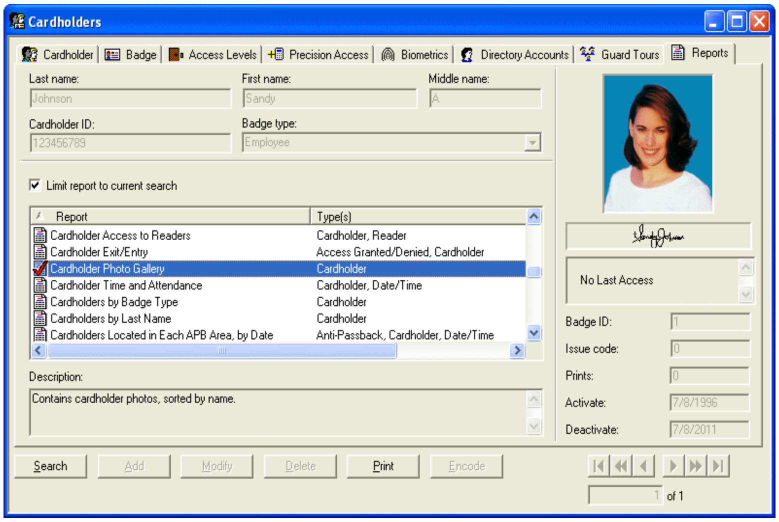
Assign Guard Tour Security Clearance Levels to a Cardholder

Note: This procedure cannot be performed in Visitor Management.

1. Select **Cardholders** from the **Administration** menu. The Cardholders folder opens.
2. Select the Guard Tours tab.
3. Locate the cardholder record for which you want to assign security clearance levels.
4. Click [Modify].
5. Select the **Can perform guard tours** check box.
6. In the **Security Clearance Levels** listing window, click on an entry to select it.
7. Click [OK].

Note: You can assign multiple security clearance levels to a cardholder.

Reports Form



Last name: Johnson

First name: Sandy

Middle name: A

Cardholder ID: 123456789

Badge type: Employee

☑ Limit report to current search

Report	Type(s)
Cardholder Access to Readers	Cardholder, Reader
Cardholder Exit/Entry	Access Granted/Denied, Cardholder
Cardholder Photo Gallery	Cardholder
Cardholder Time and Attendance	Cardholder, Date/Time
Cardholders by Badge Type	Cardholder
Cardholders by Last Name	Cardholder
Cardholders Located in Each APB Area, by Date	Anti-Passback, Cardholder, Date/Time

Description: Contains cardholder photos, sorted by name.

No Last Access

Badge ID: 1

Issue code: 0

Prints: 0

Activate: 7/8/1996

Deactivate: 7/8/2011

1 of 1

Cardholders Folder - Reports Form

Form Element	Comment
Limit report to current search	When selected, only cardholders in the current search will be included in the report.
Report listing window	Lists currently defined cardholder-related reports.
Description	A brief description of the report contents.

Reports Form Procedures

Run a Cardholder Report

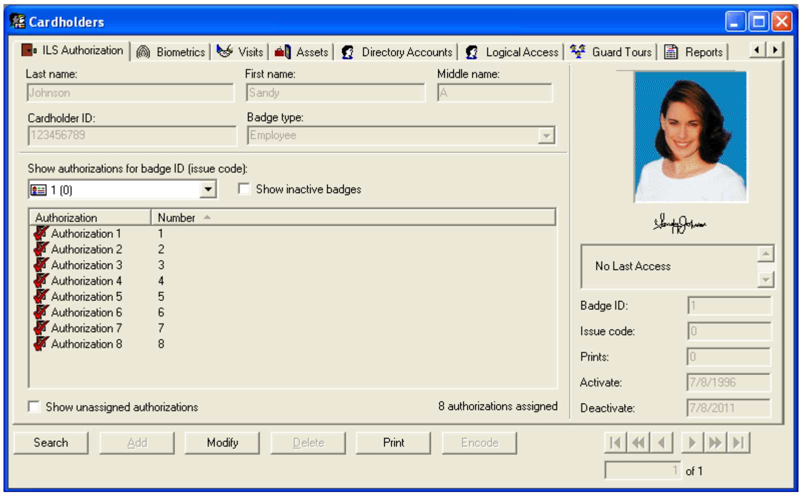
1. Select **Cardholders** from the **Administration** menu. The Cardholders folder opens.
2. Select the Reports tab.
3. Locate the cardholder record(s) for which you want to run a report. (If you want to run a report on all cardholder records, skip this step.)
4. In the **Reports** listing window, click on the name of the report you want to run.
5. Select the **Limit report to current search** check box if you want only cardholders in the current search to be included in the report. If you do not select this check box, all cardholder who meet the criteria specified in the **Description** field will be included in the report.
6. Click [Print]. The **Print Report Options** window opens. For more information, refer to Chapter 7: Print Report Options Window on page 181.

Note: Any report in the **Reports List** Window on the Event Reports form in the Reports folder that has “Cardholder” listed in the **Type(s)** column is available on the Reports form in the Cardholders folder. This means that a report can be generated on the Reports form in the Cardholders folder based on a cardholder search operation.

ILS Authorization Form

Note: To view these forms your system must have an ILS license.

ILS Authorization Form (View Mode)



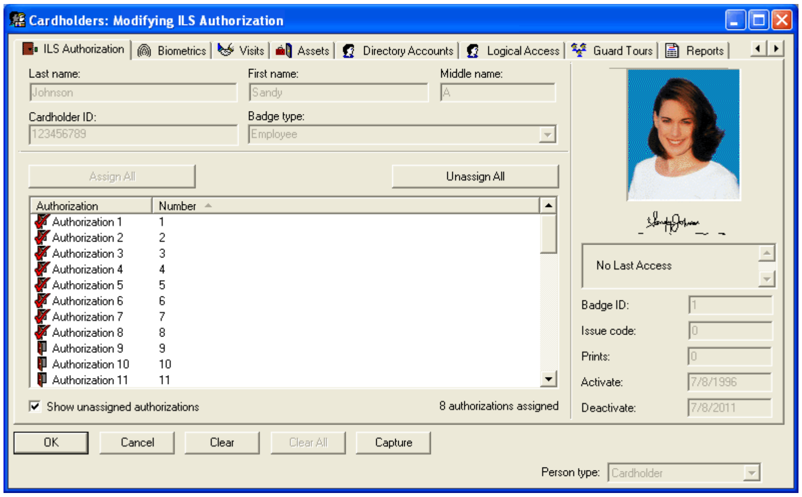
Last name: Johnson
First name: Sandy
Middle name: A
Cardholder ID: 123456789
Badge type: Employee
Show authorizations for badge ID (issue code): 1 (0)
□ Show inactive badges

Authorization	Number
Authorization 1	1
Authorization 2	2
Authorization 3	3
Authorization 4	4
Authorization 5	5
Authorization 6	6
Authorization 7	7
Authorization 8	8

□ Show unassigned authorizations
8 authorizations assigned

No Last Access
Badge ID: 1
Issue code: 0
Prints: 0
Activate: 7/8/1996
Deactivate: 7/8/2011

ILS Authorization Form (Modify Mode)



Last name: Johnson
First name: Sandy
Middle name: A
Cardholder ID: 123456789
Badge type: Employee

Authorization	Number
Authorization 1	1
Authorization 2	2
Authorization 3	3
Authorization 4	4
Authorization 5	5
Authorization 6	6
Authorization 7	7
Authorization 8	8
Authorization 9	9
Authorization 10	10
Authorization 11	11

☑ Show unassigned authorizations
8 authorizations assigned

No Last Access
Badge ID: 1
Issue code: 0
Prints: 0
Activate: 7/8/1996
Deactivate: 7/8/2011
Person type: Cardholder

Cardholders Folder - ILS Authorization Form

Form Element	Comment
Listing window	Lists the ILS authorizations that can be assigned to the cardholder.
Show authorizations for badge ID (issue code)	Displayed in view mode. Lists the badge ID and issue code (in parentheses) for the current active badge. If the **Show inactive badges** check box is selected, the list includes both the active and the inactive badge(s) assigned to the selected cardholder. Select a badge ID (issue code) from the list and the corresponding access levels for that badge will be displayed in the authorization listing window.
Show inactive badges	Displayed in view mode. When selected, the **Show levels for badge ID (issue code)** drop-down list will list both the active and inactive badge(s) assigned to the selected cardholder.

Cardholders Folder - ILS Authorization Form (Continued)

Form Element	Comment
Show unassigned levels	Displayed in view and modify mode. When selected, the authorization listing window lists both access levels that have been and that can be assigned to the selected cardholder/badge record.
Assign All	Displayed in modify mode. Click to assign all authorizations displayed in the authorization listing window.
Unassign All	Displayed in modify mode. Click to unassign all authorizations displayed in the authorization listing window.

ILS Authorization Form Procedures

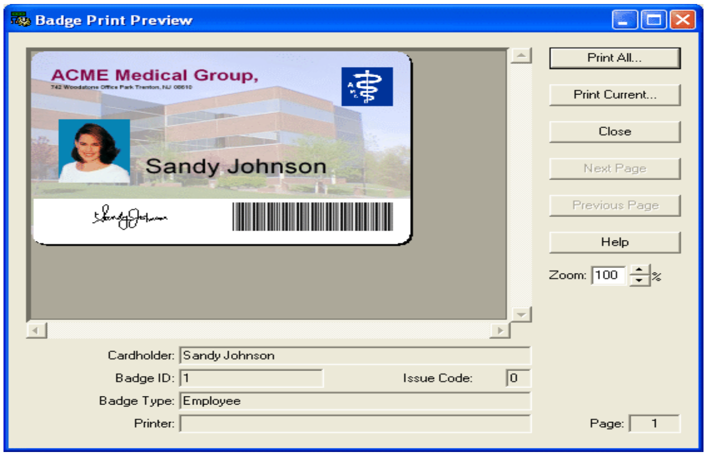
To read how to configure an ILS locking system, refer to the Integrated Locking Solutions appendix in the System Administration User Guide.

Chapter 13: Badge Print Preview Window

The Badge Print Preview window is used to:

- View (on-screen) a badge to be printed from the Cardholders folder.
- Print a badge.

This window is displayed by clicking [Print] in the Cardholders folder and then clicking [Print Preview], or by selecting **Print** from the **Application** menu. The **Application** menu is only available in System Administration and ID CredentialCenter.



Zoom: 100 %

Cardholder: Sandy Johnson

Badge ID: 1

Issue Code: 0

Badge Type: Employee

Printer:

Page: 1

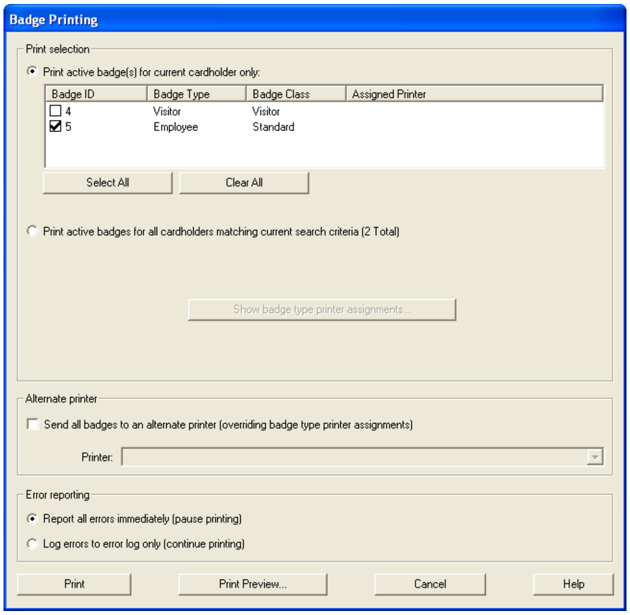
Badge Print Preview Window

Element	Comment
Preview window	Displays the currently selected badge layout with cardholder information.
Print All	Prints all the badges selected according to the Badge Printing window.
Print Current	Prints the badge that is currently displayed in the preview window.
Close	Click on this button to exit from the Badge Print Preview window.
Next Page	Allows you to view the next badge if multiple badges are being printed or to view the back layout of a two-sided badge.
Previous Page	Allows you to view the previous badge if multiple badges are being printed or to view the front layout of a two-sided badge.
Help	Displays online help for this topic.
Zoom	Enter a value to zoom in or zoom out on the badge in the preview window. • Entering a number greater than 100% will cause the preview to zoom in on the badge, displaying less area and more detail • Entering a number less than 100% will cause the preview to zoom out on the badge, display more area and less detail

Badge Print Preview Window (Continued)

Element	Comment
Badge information	Displays badge and cardholder information for the badge currently in the print preview window. Printer information displays also.
Page number	Displays the number of the page or badge that is currently in the preview window.

Badge Printing Form



● Print active badge(s) for current cardholder only:

Badge ID	Badge Type	Badge Class	Assigned Printer
□ 4	Visitor	Visitor	
☑ 5	Employee	Standard	

○ Print active badges for all cardholders matching current search criteria (2 Total)

□ Send all badges to an alternate printer (overriding badge type printer assignments)

● Report all errors immediately (pause printing)

○ Log errors to error log only (continue printing)

Badge Printing Form

Form Element	Comment
Print active badge(s) for current cardholder only	Select this to print the active badges currently shown on the Cardholders form. By default, the active badge currently selected on the Cardholder form is selected to print. If other active badges exist for the cardholder, these will be included and may be selected to print as well.
Select All	Click to select all badges of the current cardholder.
Clear All	Click to de-select all badges of the current cardholder.
Print active badges for all cardholders...	Select this option to print all active badges that match the search criteria currently in the Cardholders form.

Badge Printing Form

Form Element	Comment
Show badge type printer assignments	Click to show what printer is assigned to the current print selection.
Send all badges to an alternate printer	Select to open the Printer dialog box which allows you to select a printer other than the one assigned.
Printer	Select what printer should be used.
Report all errors immediately (pause printing)	Select to pause the printing when an error occurs. Selecting this causes errors to be reported immediately.
Log errors to error log only (continue printing)	Select this to continue printing when errors occur. Selecting this causes errors to be logged for further review.
Print	Click to print your current selection.
Print Preview	Click to preview what will be printed.
Cancel	Closes the Badge Printing form.

Badge Print Preview Window Procedures

Preview and Print a Badge

1. Select an active badge from within the Cardholders folder (Cardholders, Badge, Access Levels, Assets or Precision Access form).
   - Before printing, make sure that you are properly configured to print badges. Configurations are done using the Badge Types and Card Formats folders in System Administration or ID CredentialCenter.
   - Make sure the proper printer is chosen. This is configured by selecting **Badge Types** from the **Administration** menu in System Administration or ID CredentialCenter and setting the printer assignments on the Printing/Encoding folder.
2. Do one of the following:
   - Select **Print** from the **Application** menu.
   - Click [Print] on any form within the Cardholders folder (Cardholders, Badge, Access Levels, Assets or Precision Access form).
3. The Badge Printing window displays.
   - The Print selection section determines which badges are printed or previewed out of the cardholders listed in the current search results.
     – To print/preview specific badges for the current cardholder select **Print active badge(s) for current cardholder only**. The badge selected within the Cardholder form is selected by default. If multiple active badges are included in the list, select any of these to

print or preview as well. Only the active badges for the current cardholder display in the Print selection section.

  - To print all the active badges for the current cardholder select **Print active badges for all cardholders matching current search criteria**. If you click [Show badge type printer assignments] the following information displays within the Badge Printing window: Badge Type, Primary Segment and Assigned Printer.

Notes: Badges will not print if at least one badge does not have a printer assigned to it or at least one badge has been assigned to a printer that ReadykeyPRO no longer recognizes. You must establish a network connection to a remote printer (via control panel) in order ReadykeyPRO to recognize that printer.

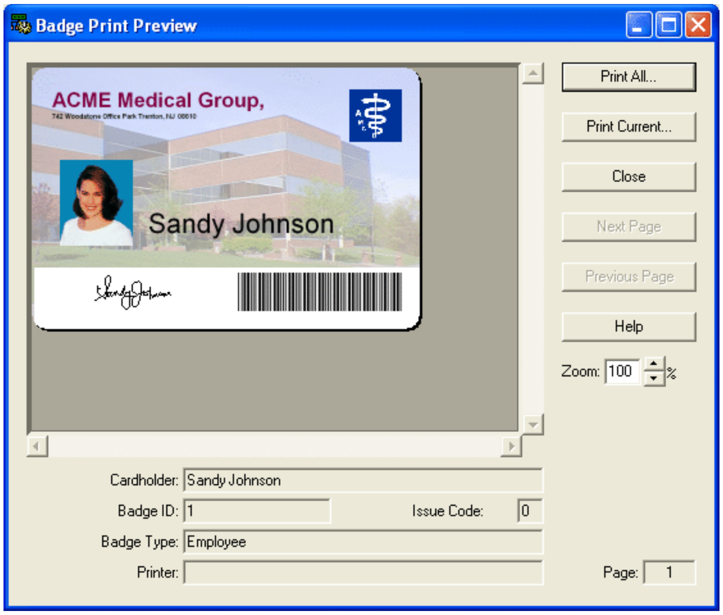
To be printable, a badge must be active, have a print count of zero if you do not have permission to print duplicates or a print count less than the maximum number of prints for its badge type if you have permission to print duplicates. Also, a badge must have a front and/or back layout assigned to its badge type.

- The **Alternate printer** section allows you to override badge type printer assignments and send all badges to an alternate printer. This section is only active when an alternate printer is configured and the user has permission to choose an alternate printer.
- The **Error Reporting** section allows you to configure how printing errors are handled. All badge printing is logged to the transaction log (print previews are not logged).
  - Click the **Report all errors immediately (pause printing)** radio button if you want to be prompted to either abort printing or skip to the next badge (or badge type) when an error occurs.
  - Click the **Log errors to error log only (continue printing)** radio button if you want errors logged and badge printing to continue on to the next badge (or if the error is associated with the badge type, the printing will move onto the next badge type).

4. It is recommended that you preview your badges first before printing them. If there is no need to preview the badge(s), you may print at this time by

clicking [Print]. Skip to step 9. If you wish to exit the window without printing, click [Cancel]. Otherwise continue on to the next step.

5. Click [Print Preview] to display the Badge Print Preview window.



Zoom: 100 %

Cardholder: Sandy Johnson

Badge ID: 1

Issue Code: 0

Badge Type: Employee

Printer:

Page: 1

The current badge displays along with cardholder data and printer information.

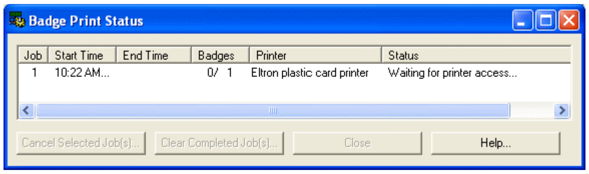
6. Use the [Next Page] and [Previous Page] buttons to view the next badge or other side of a two-sided badge.

7. You can zoom in or out on the badge by changing the percentage value in the **Zoom** box. A larger number displays the badge close-up, in more detail. A smaller number will display more of the badge, in less detail.

8. To print the badge(s), do one of the following:
   - Click [Print Current]. Doing so will print the badge that is currently in the preview window.
   - Click [Print All] to print all of the badges that have been selected.
   - To exit from the window without printing, click [Close].

Note: If a user attempts to print a badge that has already been printed the maximum number of times then an error displays and the badge does not print. As with other printing errors the user can continue on to the next badge if a batch print is being performed.

9. If you decided to print badges a status window displays to indicate the status of the print operation.



Job	Start Time	End Time	Badges	Printer	Status
1	10:22 AM...		0/ 1	Eltron plastic card printer	Waiting for printer access...

A *single* print job entry represents all the badges selected in the **Print selection** section.

Chapter 4: Visits Folder

The Visits folder contains the Status search form, the Visit form, the Details form, the E-mail form and the Reports form with which you can:

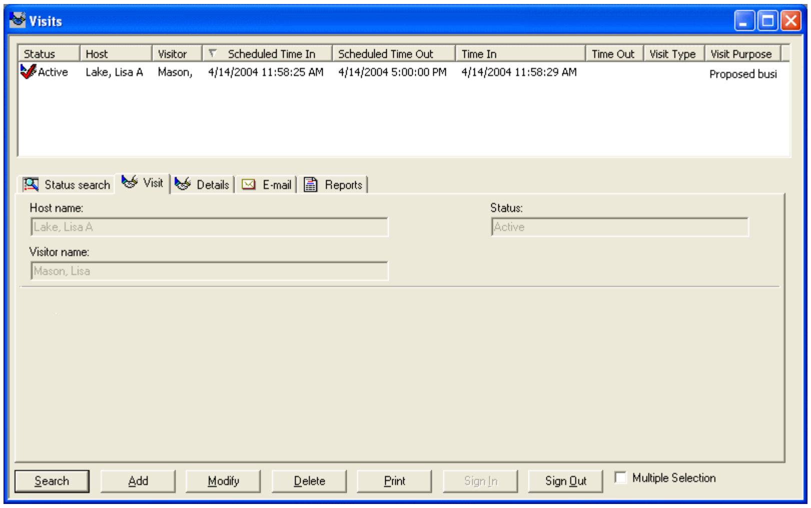
- Display visit records for a selected date range
- Search for visit records based on the scheduled time in, scheduled time out, time in, time out or date and time it was last changed
- Display visit records that are scheduled in the future, scheduled and are late, active, active and overstayed and finished
- Filter and display visit records for a selected cardholder, visitor or both
- Display the cardholder or visitor record associated with a visit
- Refresh the Visits listing window
- Send e-mail notifications regarding visits
- Add or modify visits
- Delete a visit or multiple visits
- Print a disposable badge or multiple disposable badges
- Sign out and sign in a visit or multiple visits
- Generate a report for either a defined search criteria or for all visits

Toolbar Shortcut

This folder is displayed by selecting **Visits** from the **Administration** menu or by selecting the Visits toolbar button.

The forms in the Visits folder are divided into two sections: the form elements that are common to every form in the Visits folder (shown in the screen shot that follows) and the form elements that are unique to each form. For descriptions of the common form elements refer to the Visits Folder Field Table table on page 128. For descriptions of the unique form elements refer to the Status Search Form Field Table table on page 148, the Visit Form Field Table table on page 145, the Details Form Field Table table on page 150, and the E-mail Form Field Table

table on page 151, and the Reports Form Field Table table on page 154.



Status	Host	Visitor	Scheduled Time In	Scheduled Time Out	Time In	Time Out	Visit Type	Visit Purpose
Active	Lake, Lisa A	Mason,	4/14/2004 11:58:25 AM	4/14/2004 5:00:00 PM	4/14/2004 11:58:29 AM			Proposed busi

Host name: Lake, Lisa A

Status: Active

Visitor name: Mason, Lisa

Notes: This documentation refers to visit data fields that are shipped as the default by Bosch. If you have used the FormsDesigner application to customize your visit data, the elements on your Visits folder forms will be different.

Forms and fields that pertain to segmentation are only available if segmentation is enabled on your system.

Visit Right-Click Menu

If you right-click on a visit in the listing window, a menu will be displayed. The menu contains the following options:

Right-click menu option	Description
Select All	Enabled only when the **Multiple Selection** check box is selected. If selected, all visits in the listing window will be selected.
Clear All	If selected, all visits selected in the listing window will be deselected.
Add	Selecting this option does the same thing as clicking the [Add] button - it allows you to add another visit based on the currently selected visit.
Modify	Selecting this option does the same thing as clicking the [Modify] button - it allows you to change the visit that is currently selected.
Delete	Selecting this option does the same thing as clicking the [Delete] button - it allows you to delete the visit that is currently selected. The visit will be deleted without prompting for confirmation.
Sign In	This option is only available for a visit that is not active/not signed in. If the **Multiple Selection** check box is selected, multiple visits can be selected and signed in at once. Selecting this option does the same thing as clicking the [Sign In] button. If selected, the Sign In Visit(s) window is displayed. In this window, select whether to print disposable badges for the visitor that is being signed in.

Right-click menu option	Description
Sign Out	This option is only available for a visit that is active/signed in. If the **Multiple Selection** check box is selected, multiple visits can be selected and signed out at once. Selecting this option does the same thing as clicking the [Sign Out] button. To use this feature, you must first configure a badge status to use when doing an automatic sign out. This is done on the General Cardholder Options form of the Cardholder Options folder. For more information, refer to Configure System-wide Visit Options on page 46. When selected, the actual **Time out** for the visit is updated to the current date/time. If the visitor has an active badge, the deactivate date is updated and the badge status is set to the status setup that was selected on the General Cardholder Options form.
Find Cardholder	Opens the Cardholders folder and displays the cardholder record that is associated with the currently selected visit.
Find Visitor	Opens the Cardholders folder and displays the visitor record that is associated with the currently selected visit.
Refresh	Click this button to refresh the visits listed in the Visits listing window. When someone else makes changes in the database, you may need to click this button to see the changes. (Cardholder information is not automatically updated, but visit information is.)

Visits Folder Field Table

Visits Folder

Form Element	Comment
Common form elements	
Visits listing window	Displays the status, host, visitor, scheduled time in, scheduled time out, time in, time out, visit type and visit purpose for visit records.
Host name	Specifies the host for whom you want to display scheduled visits.
Visitor name	Specifies the visitor for whom you want to display scheduled visits.
Status	Displays the status of the visit. Choices include: • **Scheduled** - A visit that has a scheduled time in and scheduled time out that are both in the future • **Late** - A visit where the current date and time is after the scheduled time in • **Overstayed** - A visit where the current date and time is after the scheduled time out • **Active** - A visit that has been signed in and the scheduled time out has not yet been reached • **Finished** - A visit occurred in the past and has been signed out
Search	Allows you to search based on any field on any form in the Visits folder. The search results will be displayed in the Visits listing window.
Add	Allows you to add a visit record.
Modify	Allows you to modify a selected visit record. Multiple selection cannot be used when modifying visit records. If the **Multiple Selection** check box is selected and multiple visit records are selected, the [Modify] button will be grayed out.
Delete	Allows you to delete a selected visit record. If the **Multiple Selection** check box is selected, multiple visit records can be deleted at once. The visit(s) will be deleted without prompting for confirmation.
Print	Allows you to print a disposable badge. Disposable badge types are configured in the Badge Types folder. For a badge type to be used to print disposable badges, it must have “Visitor” selected for the **Class** and the **Disposable** check box must be selected (on the Badge Type sub-tab). If segmentation is enabled, the correct segment must be selected on the Segment Membership sub-tab.
Sign In	If selected, the Sign In Visit(s) window is displayed. In this window, select whether to print disposable badges for the visitor(s) that are being signed in. If the **Multiple Selection** check box is selected, multiple visit records can be signed in at once.
Sign Out	To use this feature, you must first configure a badge status to use when doing an automatic sign out. This is done on the General Cardholder Options form of the Cardholder Options folder. For more information, refer to Configure System-wide Visit Options on page 46. When selected, the actual **Time Out** for the visit is updated to the current date/time. If the visitor has an active badge, the deactivate date is updated and the badge status is set to the status setup that was selected on the General Cardholder Options form.

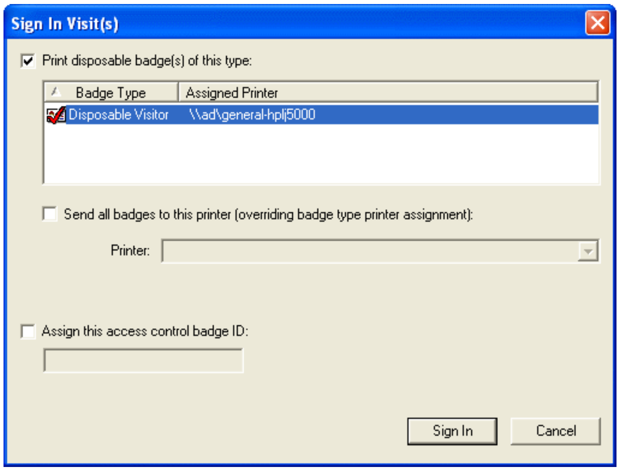
Visits Folder (Continued)

Form Element	Comment
Multiple Selection	If selected, more than one entry in the listing window can be selected simultaneously. The changes made on this form will apply to all selected visits. This feature is primarily used for printing badges, signing in visits and signing out visits.

Sign In Visit(s) Window

This window is displays when:

- A visit is added in the Visits folder and the **Sign In Now** check box is selected on the Visit form.
- A visit record is selected in the Visit listing window in the Visits folder and the [Sign In] button is clicked.
- Automatic sign in is enabled. For more information about this feature, refer to the Automatic Sign In section of the Visitor Management User Guide.



Sign In Visit(s)

☑ Print disposable badge(s) of this type:

Badge Type	Assigned Printer
☑ Disposable Visitor	\\ad\general-hplj5000

□ Send all badges to this printer (overriding badge type printer assignment):

Printer:

□ Assign this access control badge ID:

Visits Folder - Sign In Visit(s) Window Field Table

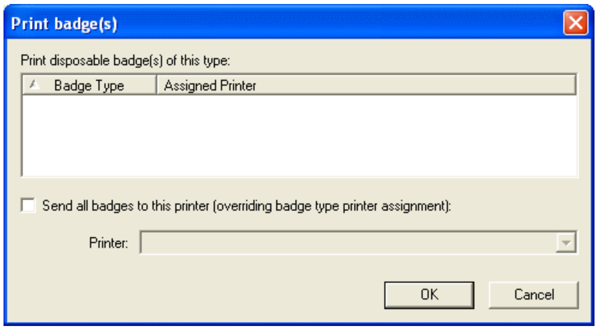
Form Element	Comment
Print disposable badge(s) of this type	• For this field to be enabled, the **Allow disposable badge printing** check box on the Visits form in the Cardholder Options folder in System Administration or ID CredentialCenter must be selected. • Displays a list of disposable badge types that can be selected for the visit. • Only those badge types that are disposable are listed. • If you do not want to print a disposable badge for the visitor, deselect this check box.

Visits Folder - Sign In Visit(s) Window Field Table (Continued)

Form Element	Comment
Send all badges to this printer (overriding badge type printer assignment)	• Select this check box to select an alternate printer • For these fields to be enabled, the user must have be rights to access to the **Choose alternate printer** option via the Users Folder, Cardholder Permission Groups Form. • Selecting this check box overrides the printer assignments in the Printing/Encoding form of the Badge Types folder.
Assign this access control badge ID	• For this field to be enabled, the **Allow access control badge assignment** check box on the Visits form in the Cardholder Options folder in System Administration or ID CredentialCenter must be selected. • The badge must already exist in the system • The existing badge's class must be "Visitor" • If the visitor already has an active access control badge (from a manual assignment or another visit), this field will automatically be populated with that ID. • If you do not want to assign an access control badge ID for the visitor, deselect this check box.
Sign In	Signs in the visit using the options selected on the form.
Cancel	Closes the Sign In Visit(s) window without signing in the visit.

Print Badge(s) Window

This window displays when the [Print] button is clicked on any form in the Visits folder.


Print badge(s)
Print disposable badge(s) of this type:
Badge Type
Assigned Printer
□ Send all badges to this printer (overriding badge type printer assignment):
Printer:
OK
Cancel

Visits Folder - Print Badge(s) Window Field Table

Form Element	Comment
Print disposable badge(s) of this type	• For this field to be enabled, the **Allow disposable badge printing** check box on the Visits form in the Cardholder Options folder in System Administration or ID CredentialCenter must be selected. • Displays a list of disposable badge types that can be selected for the visit. You must select a badge type and only one badge type can be selected. • Only those badge types that are disposable are listed.

Visits Folder - Print Badge(s) Window Field Table

Form Element	Comment
Send all badges to this printer (overriding badge type printer assignment)	• Select this check box to select an alternate printer. Chose the printer from the drop-down list. • For these fields to be enabled, the user must have access rights to the **Choose alternate printer** option via the Users Folder, Cardholder Permission Groups Form • Selecting this check box overrides the printer assignments in the Printing/Encoding form of the Badge Types folder.
OK	Prints the disposable badge
Cancel	Closes the Print Badge(s) window without printing the visit.

Visits Folder Procedures

The following procedures pertain to every form in the Visits folder unless otherwise noted.

Visit Search Capabilities

In search mode, you can search on any combination of fields in the Visits folder, including the Status search, Visit and Details forms. On the E-mail and Reports forms, you can only search for the host name or visitor name.

Comparison Operators

Comparison operators are symbols that represent specific actions. You can refine your search by prefixing search fields with a comparison operator. Refer to the following table to identify the comparison operators you can use with different fields.

Comparison operator	Description	Text field	Numeric field	Drop-down list
=	Equal to	Yes	Yes	Yes
!= or <>	Not equal to	Yes	Yes	Yes
>	Greater than	Yes	Yes	NA
<	Less than	Yes	Yes	NA
>=	Greater than or equal to	Yes	Yes	NA
<=	Less than or equal to	Yes	Yes	NA
%	Contains	Yes	NA	NA

Notes: "Equal to" is the default comparison operator for numeric and drop-down list fields.

If you type an equal to sign "=" in a field and nothing else, ReadykeyPRO will search for records that have an empty value for that field. For example, typing an "=" in the Department field will find every record that does not have an assigned department.

Search Fields Using "Begins With"

For text and drop-down list fields you can search records whose values begin with specific characters by entering those characters in the field. For example, when searching by last name, a filter of "L" will find "Lake", "Lewis", etc. A filter of "Lake" will find "Lake", "Lakeland", etc.

Note: The default comparison operator for text fields is "begins with".

Search Multiple Fields

When you search multiple fields, the search criteria for each field is combined. For example, typing "A" in **Last name** field and "B" in **First name** field will find all people whose last name begins with "A" and whose first name beings with "B".

One *exception* is searching access levels, which uses an "or" comparison for multiple selections. For example, selecting both "Access Level A" and "Access Level B" will find all cardholders with either "Access Level A" or "Access Level B" assigned.

Note: If you want to search for a range of Badge IDs, take advantage of the two Badge ID fields on the Badge form. One field is located in the middle-left section of the form and the other field is located in the right section of the form. Note, the form must be in modify mode to see both fields. Type ">= 100" in one field and "<= 200" in the other to find all badges with IDs between 100 and 200 (inclusive).

Search for All Visits to a Selected Cardholder

This procedure will search for every person who visited a selected cardholder.

1. Select **Visits** from the **Administration** menu. The Visits folder opens.
2. On the Visit tab, click [Search].
3. Do one of the following:
   - Enter the full or partial last name of the cardholder in the **Host name** drop-down list.
   - Use the Select Host Wizard by leaving the **Host name** drop-down list blank and clicking the [...] button to the right it. When the wizard opens, enter any information that you know about the cardholder and click [Next]. The wizard will display all records that match the criteria you entered. Select the correct cardholder and click [Finish].
4. Click [OK]. ReadykeyPRO displays all the visits made to the selected cardholder. If you entered a partial cardholder name, ReadykeyPRO displays all the visits made to the cardholders that meet the search criteria.

Search for All Visits by a Selected Visitor

1. Select **Visits** from the **Administration** menu. The Visits folder opens.
2. On the Visit tab, click [Search].
3. Do one of the following:
   - Enter the full or partial last name of the visitor in the **Visitor name** drop-down list.
   - Use the Select Host Wizard by leaving the **Visitor name** drop-down list blank and clicking the [...] button to the right it. When the wizard opens, enter any information that you know about the visitor and click [Next]. The wizard will display all records that match the criteria you entered. Select the correct visitor and click [Finish].
4. Click [OK]. ReadykeyPRO displays all the cardholders the selected visitor has met with. If you entered a partial visitor name, ReadykeyPRO displays all the cardholders visited by the visitors that meet the search criteria.

Search for Scheduled, Active or Finished Visits

1. Select **Visits** from the **Administration** menu. The Visits folder opens.
2. On the Status search tab, click [Search].
3. In the Search for visits section, select that status you wish to search for.
   - To search for scheduled visits, select the **Scheduled, future** check box.
     – If you wish to search for visits that are scheduled to begin in a specified amount of time, select the **Starting within** check box and specify the number of minutes, hours, or days.

    - By default, scheduled visits that are late getting started are included in the search. If you do not want to search for scheduled visits that are late, deselect the **Scheduled, late** check box.
  - To search for active visits, select the **Active** check box.
    - If you wish to search for visits that are scheduled to end within a specified amount of time, select the **Ending within** check box and specify the number of minutes, hours, or days.
    - By default, active visits that are late signing out (overstayed) are included in the search. If you do not want to search for overstayed visits, deselect the **Active, overstayed** check box.
  - To search for finished visits, select the **Finished** check box.

4. The refresh rate is how often (in minutes) the database is queried for changes.
   - Select the **Use system default rate** check box to use the system default rate. Notice the **Refresh rate** field automatically populates with the default value.
   - Deselect the **Use system default rate** check box to use a different rate. Enter the new rate in the **Refresh rate** field. This setting is stored on a per user basis.
5. Click [OK]. The visit records that meet the search criteria display in the Visits listing window.

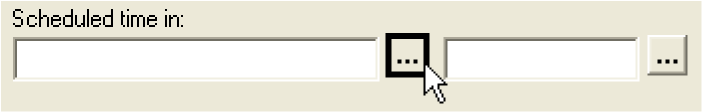
Search for All Visits for a Specific Date or Time

Depending on the fields you populate, this procedure will search for:

- Visits scheduled to start on a specific date or time.
- Visits scheduled to end on a specific date or time.
- Visits that start on a specific date or time.

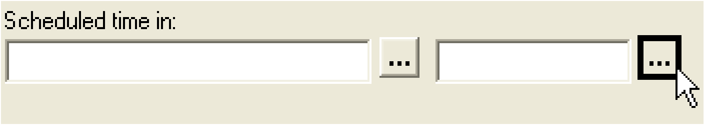
- Visits that end on a specific date or time.

1. Select **Visits** from the **Administration** menu. The Visits folder opens.
2. On the Visit tab, click [Search].
3. To search for a specific date:
   a. Click the [...] button to the right of one of the four date fields (Scheduled time in, Scheduled time out, Time in, or Time out).

   b. The Select Date(s) window opens. Complete one of the following:
      - Select a time range and the number of days to search. If you select “Today”, you do not need to enter the number of days to search.
      - Select a time range and a date.
      - Select a start date and the number of days to search.
      - Select a start date and end date.

   c. Click [OK]. The code for the search criteria that you specified displays in the Visit form.
4. To search for a specific time:
   a. Click the [...] button to the right of one of the four time fields.

   b. The Select Time Range window opens. Select the start time range and enter a time.
   c. Select the end time range and enter a time.

Notes: If you select “None” for a time range, you cannot enter a specific time.

You can change the time by using the spin buttons or typing new values. The hour, minute, and time of day are adjusted individually.

   d. Click [OK].

5. Click [OK] on the Visit form. The visit records that meet the search criteria display in the listing window.
6. Repeat steps 3-5 to search for scheduled time in, scheduled time out, time in, or time out.

Retrieve the Most Recent Visit Search Results

1. Display the Cardholders folder or Visits folder by completing one of the following:
   - To display the Cardholders folder in Alarm Monitoring, select **Badge Info** from the **View** menu. For all other applications, select **Cardholders** from the **Administration** menu.
   - To display the Visits folder in Alarm Monitoring, select **Visits** from the **View** menu. For all other applications, select **Visits** from the **Administration** menu.
2. Click [Search].
3. Click [Last Search]. The criteria you selected from the most recent search operation will be inserted into the appropriate fields.
4. You can optionally modify your search criteria.
5. Click [OK].
6. ReadykeyPRO retrieves and displays the first matching record. Use the navigational buttons to look at additional matching records.

Find a Cardholder or Visitor Associated with a Visit

1. Select **Visits** from the **Administration** menu. The Visits folder opens.
2. Locate the visit record that you wish to find the visitor or cardholder for.
3. Right-click on the visit record.
   - If you wish to view the cardholder record, select **Find Cardholder**.
   - If you wish to view the visitor record, select **Find Visitor**.
4. The record of the corresponding cardholder or visitor will be displayed in the Cardholder or Visitor window.

Add a Visit Record

To add a visit, information about the visit needs to be entered on the Visit, Details and E-mail forms in the Visits folder; it does not matter which form you start with. When the Visits folder opens, the Visit form displays by default, so this procedure begins on that form.

1. Select **Visits** from the **Administration** menu. The Visits folder opens.
2. On the Visit form:
   a. A new visit record can either be based on an existing visit record or it can be an entirely new record.
      - To create a record based on an existing visit record, select a visit record in the Visits listing window, then click [Add]. The fields prepopulate with the information from the selected visit. You can select new values for any field.
      - To create a record that is not based on an existing visit record, make sure that no visit record is selected in the Visits listing window, then click [Add]. The fields will be blank to begin with.

Note: Steps b and c can be done in either order.

b. Click the [...] button to the right of the **Host name** drop-down list. The Select Host Wizard: Search form opens. For more information, refer to Select Host Wizard: Search Form on page 156.

1) Specify your search criteria by typing full or partial entries in the enabled fields.

Note: Leave all fields blank to display all cardholders.

2) If a visitor is specified and you wish to search for only cardholders who have been visited by that visitor, select the **Previous hosts for current visitor only** check box.

3) Click [Next].

4) The Select Host Wizard: Select form opens. In the Cardholder listing window, select the cardholder you wish to add a visitor for. For more information, refer to Select Host Wizard: Select Form on page 158.

5) Click [Finish]. The cardholder's name appears in the **Host name** field on the Visit form.

c. Click the [...] button to the right of the **Visitor name** field. The Select Visitor Wizard: Search form displays.

1) Specify your search criteria by typing full or partial entries in the enabled fields.

Note: Leave all fields blank to display all visitors.

2) If a cardholder is specified and you wish to only search for visitors who have visited that cardholder, select the **Previous visitors for current host only** check box.

3) Click [Next].

4) The Select Visitor Wizard: Select or Add form displays. If the Visitor is listed below, select the visitor and click [Finish]. The visitor's name appears in the **Visitor name** field on the Visit form. If the Visitor is not listed below, select the **Create new visitor** radio button and click [Next]. The Select Visitor Wizard: Add form displays. Enter the new visitor's information and click [Finish].

Note: For a detailed description of the Select Visitor Wizard: Select or Add form refer to Select Visitor Wizard: Select or Add Form on page 161.

d. In the **Scheduled time in** fields, specify the date and time the visit will begin. You can either type the values or select them.

Note: If the **Sign In Now** check box is selected, these fields will be grayed out.

e. In the **Scheduled time out** fields, specify the date and time the visit will end. You can either type the values or select them.

f. Select the **Sign In Now** check box if the visit is starting immediately. If you select this option, the **Scheduled time in** fields will become grayed out and the date and time when you click the [OK] button will be assigned as the visit's **Time in**.

3. Click the Details tab. For a detailed description of the Details form refer to Details Form on page 150. On the Details form:

   a. In the **Type** drop-down list, select the type of visit.

Note: Types of visits must first be configured in the List Builder, which is displayed in System Administration or ID CredentialCenter by selecting the **Administration** menu, then selecting **List Builder**. For more information refer to the List Builder Folder chapter in the System Administration User Guide.

   b. In the **Purpose** field, type the reason for the visitor's visit.

4. You may wish to send e-mail notifications to all parties that require information about a scheduled visit. For a detailed description of the E-mail form refer to E-mail Form on page 151. To set up e-mail notifications, click the E-mail tab. On the E-mail form:

Note: For an e-mail to be sent, the **Allow e-mail notification** check box on the Visits form in the Cardholder Options folder must be selected.

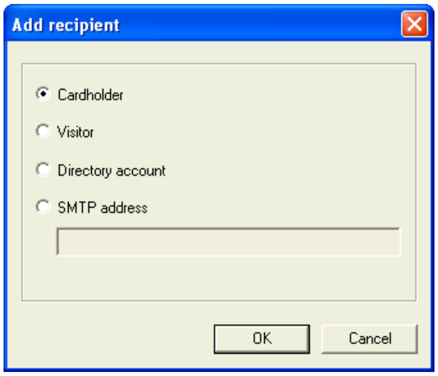
   a. In the Include section, verify the **Default Recipients** check box is selected as long as you wish to send e-mail messages to the default recipients. The default recipients are configured in the following locations:

- On segmented systems, select **Administration** > **Segments**, click the Segments tab, then click the Visits sub-tab. On the Visits sub-tab, you can view or modify the default recipients.
- On nonsegmented systems, select **Administration** > **System Options**, then click the Visits tab. On the Visits tab, you can view or modify the default recipients.

b. Select the **Cardholder for this visit** check box if you wish to have an e-mail sent to the cardholder for this visit.

c. Select the **Visitor for this visit** check box if you wish to have an e-mail sent to the visitor for this visit.

d. Click [Add] if you wish to add another recipient. The Add recipient window displays. You may add a cardholder, visitor, directory account or SMTP address.



Add recipient

● Cardholder

○ Visitor

○ Directory account

○ SMTP address

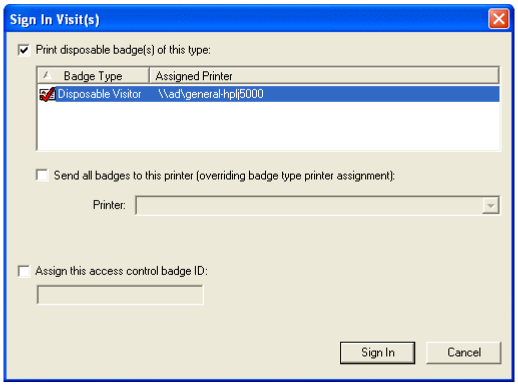
- If you select the **Cardholder** radio button and click [OK], the Select Host Wizard: Search form displays. For a detailed description of the Select Host Wizard: Search form refer to Select Host Wizard: Search Form on page 156.
- If you select the **Visitor** radio button and click [OK], the Select Visitor Wizard: Search form displays. For a detailed description of the Select Visitor Wizard: Search form refer to Select Visitor Wizard: Search Form on page 160.
- If you select the **Directory account** radio button and click [OK], the Select Account window displays.
- If you select the **SMTP address** radio button, type the SMTP address, then click [OK]. An example of an SMTP address is “joesmith@company.com”.

5. Click [OK].

6. If the **Sign in now** check box was selected, proceed to step 7. If the **Sign in now** check box was not selected, the visit will be added. The value for the **Time In** column for the visit will remain blank and the visit can be signed in later when it actually occurs.

7. If none of the **Allow disposable badge printing**, **Allow access control badge assignment** and **Allow e-mail notification** check boxes are checked

on the Visits form in the Cardholder Options folder, the visit will be signed in. If any of those options are selected, the Sign In Visit(s) window displays.



☑ Print disposable badge(s) of this type:

Badge Type	Assigned Printer
Disposable Visitor	\\ad\general-hplj5000

☐ Send all badges to this printer (overriding badge type printer assignment):

Printer:

☐ Assign this access control badge ID:

8. The **Print disposable badge(s) of this type** check box and listing window are enabled if the **Allow disposable badge printing** check box is selected on the Visits form in the Cardholder Options folder.
   - If enabled, you can print a disposable badge for the user by selecting the **Print disposable badge(s) of this type** check box, then selecting a disposable badge type to be assigned and printed.

Note: Disposable badge types are configured in the Badge Types folder. For a badge type to be used to print disposable badges, it must have “Visitor” selected for the **Class** and the **Disposable** check box must be selected (on the Badge Type sub-tab). If segmentation is enabled, the correct segment must be selected on the Segment Membership sub-tab.

   - If the check box is deselected, the system will not print a disposable badge.

9. To override the badge type printer assignment select the **Send all badges to this printer (overriding badge type printer assignment)** check box and select the printer from the drop-down list. This check box and drop-down list

are enabled if the **Print disposable badge(s) of this type** check box is selected and the user has the correct permissions.

10. The **Assign this access control badge ID** check box and field are enabled if the **Allow access control badge assignment** check box is selected on the Visits form in the Cardholder Options folder.
    - If enabled, you can select the **Assign this access control badge ID** check box and then type the number of an existing badge that has the class “Visitor” in the field or leave the field blank.
    - If the visitor already has an active access control badge (from manual assignment or another visit), this field will automatically be filled in with that ID.
    - If the check box is deselected, the system will not attempt to assign an access control badge ID.
11. Click [Sign In]. The visit will be added, the **Time In** field will be updated to the current date and time and any access control badge assigned will become active.

Modify a Visit Record

1. Select **Visits** from the **Administration** menu. The Visits folder opens.
2. Locate the visit record you want to change and select it in the Visits listing window.

Note: Multiple selection cannot be used when modifying visits.

3. Click [Modify].
4. Make the changes you want to the record. Changes can be made on any tab in the Visits folder.
5. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Visit Record

1. Select **Visits** from the **Administration** menu. The Visits folder opens.
2. In the Visits listing window select the visit record you want to delete.

Note: To select multiple visit records select the **Multiple Selection** check box.

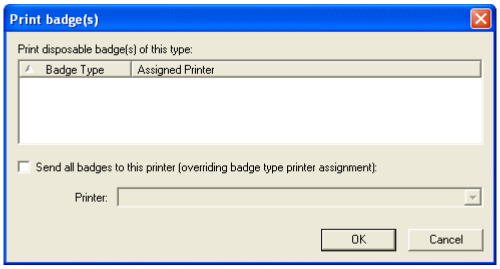
3. Click [Delete].
4. Click [OK]. The visit(s) will be deleted without confirmation.

Print a Visitor Badge

1. Select **Visits** from the **Administration** menu. The Visits folder opens.
2. In the Visits listing window select the visit record you want to print.

Note: To select multiple visit records select the **Multiple Selection** check box.

3. On any form in the Visits folder, click [Print].
4. The Print badge(s) window displays. In the **Print disposable badge(s) of this type** listing window select the type of badge to print.


Print badge(s)
Print disposable badge(s) of this type:
Badge Type
Assigned Printer
□ Send all badges to this printer (overriding badge type printer assignment):
Printer:
OK
Cancel

Note: Disposable badge types are configured in the Badge Types folder and must have “Visitor” selected for the **Class** and the **Disposable** check box selected (on the Badge Type sub-tab). If segmentation is enabled, the correct segment must be selected on the Segment Membership sub-tab.

5. To select an alternate printer select the **Send all badges to this printer (overriding badge type printer assignment)** check box and choose a printer from the drop-down list. This check box and drop-down list are enabled if the user has the correct permissions.
6. Click [OK].

Sign in a Previously Scheduled Visit and Print a Badge

Each visit has a time that it is scheduled to begin. When the visitor arrives and the visit actually begins, the visit should be “signed in”. When a visit is signed in, the actual **Time In** of the visitor is updated to the current date and time and any access control badge that the visitor is issued is activated. A visit can be signed in immediately after it is added or it can be signed in later.

1. Open the Sign In Visit(s) dialog by completing one of the following:
    a. Add a visit. For more information, refer to Add a Visit Record on page 136.
    b. Search for an existing visit and click [Sign In]. For more information, refer to Search for Scheduled, Active or Finished Visits on page 133.
2. Depending on how the badge types are configured, different fields are active on the Sign In Visit(s) form.
    - To print a disposable visitor's badge using the default printer assignment, complete steps a and d (below).
    - To print a disposable visitor's badge by overriding the default printer assignment, complete steps a, b, and d.
    - To print a non-disposable visitor's badge by using the default printer assignment, complete steps c and d.
    - To print a non-disposable visitor's badge by overriding the default printer assignment, complete steps a through d.
        a. Select the Print disposable badge(s) of this type check box and select a badge type.
        b. Select the Send all badges to this printer (overriding badge type printer assignment) check box and select the printer from the drop-down list.
        c. Select the Assign this access control badge ID check box and enter the badge ID. Note, the badge ID must exist in the database as an active visitor badge ID. If the visitor already has an active access control badge, this field will automatically be filled in with that ID.
        d. Click [Sign In].

Note: Disposable badge types are configured in the Badge Types folder. For a badge type to be used to print disposable badges, it must have "Visitor" selected for the **Class** and the **Disposable** check box must be selected (on the Badge Type sub-tab). If segmentation is enabled, the correct segment must be selected on the Segment Membership sub-tab.

Sign Out a Visit

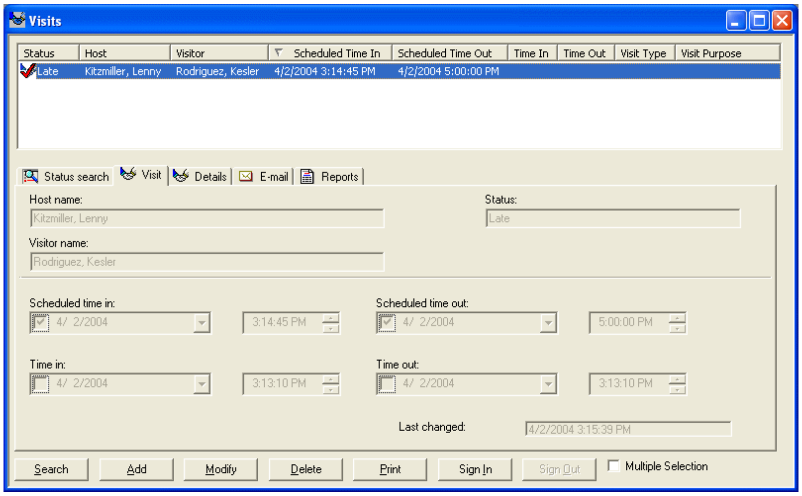
Each visit has a time that it is scheduled to end. When the visitor leaves and the visit actually ends, the visit should be "signed out." When a visit is signed out, the actual **Time Out** of the visitor is updated to the current date and time and any access control badge that the visitor is issued is deactivated.

To use the Sign Out feature, you must first configure a badge status to use when doing an automatic sign out. This is done on the Visits form in the Cardholder

Options folder. For more information, refer to Configure System-wide Visit Options on page 46.

1. Select **Visits** from the **Administration** menu. The Visits folder opens.
2. Locate the active visit record that needs to be signed out.
3. In the Visits listing window, select the active visit that you want to sign out by clicking on it.
4. Click [Sign Out].
5. The message “Are you sure you wish to sign out the selected visit(s)? This will also deactivate any badges the visitors have.” will be displayed. Click [Yes] to complete the sign out. The **Time out** will be updated to the current date/time. If the visitor has an active badge, the deactivate date will be updated and the badge status will be set to the status setup that was selected on the Cardholder Options form. The signed out visit will appear in the Visits listing window.

Visit Form



Status	Host	Visitor	Scheduled Time In	Scheduled Time Out	Time In	Time Out	Visit Type	Visit Purpose
✓ Late	Kitzmiller, Lenny	Rodriguez, Kesler	4/2/2004 3:14:45 PM	4/2/2004 5:00:00 PM				

Host name: Kitzmiller, Lenny

Status: Late

Visitor name: Rodriguez, Kesler

Scheduled time in: ☑ 4/ 2/2004 3:14:45 PM

Scheduled time out: ☑ 4/ 2/2004 5:00:00 PM

Time in: □ 4/ 2/2004 3:13:10 PM

Time out: □ 4/ 2/2004 3:13:10 PM

Last changed: 4/2/2004 3:15:39 PM

Visit Form Overview

The Visit form is displayed by default when the Visits folder opens. It is used to:

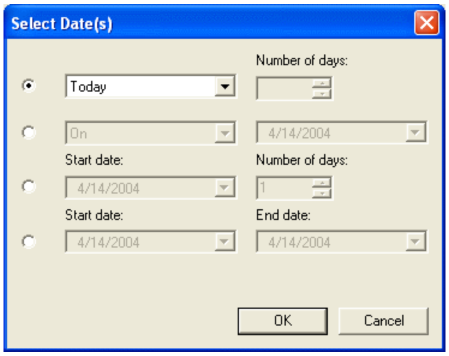
- Add or modify visits
- Display visit records for a selected date range
- Search for visit records based on the scheduled time in, scheduled time out, time in, time out or date and time last changed

Visit Form Field Table

Form Element	Comment
Scheduled time in	Select the date and time that the visit is expected to start.
Time in	When a visit is signed in, the visit's **Time in** gets updated to the current date and time.
Scheduled time out	Select the date and time that the visit is expected to end.
Time out	When a visit is signed out, the visit's **Time out** gets updated to the current date and time.
Last changed	Indicates the date and time on which this visit record was last modified and saved. This date and time are only updated when visit information is changed, not when badge information is changed. The last changed date is saved individually for each badge record as well.

Select Date(s) Window

This window is only displayed when the Visit form in the Visits folder is in Search mode. In Search mode, click the [...] button to the right of the first **Scheduled time in**, **Time in**, **Scheduled time out** or **Time out** field.



Visit Form - Select Date(s) Window Field Table

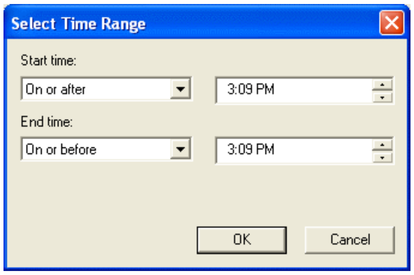
Form Element	Comment
Day	Used when searching for a scheduled time in, time in, scheduled time out or time out. Selects visits that occurred today, on a previous number of days or on a specified number of days in the future.
Specific Date	Used when searching for the date portion of a scheduled time in, time in, scheduled time out or time out. Selects visits that occurred on a specified date. Choices include on, on or after, after, on or before or before a specified date.
Number of Days After a Date	Used when searching for the date portion of a scheduled time in, time in, scheduled time out or time out. Selects visits between a specified start date and a specified number of days after the start date.

Visit Form - Select Date(s) Window Field Table (Continued)

Form Element	Comment
Between Two Dates	Used when searching for the date portion of a scheduled time in, time in, scheduled time out or time out. Selects all visits that occurred between the specified Start date and the End date.
OK	Enters the code for the selected search criteria in the respective field on the Visit form in the Visits folder.
Cancel	Closes the Select Date(s) window without selecting a date search criteria.

Select Time Range Window

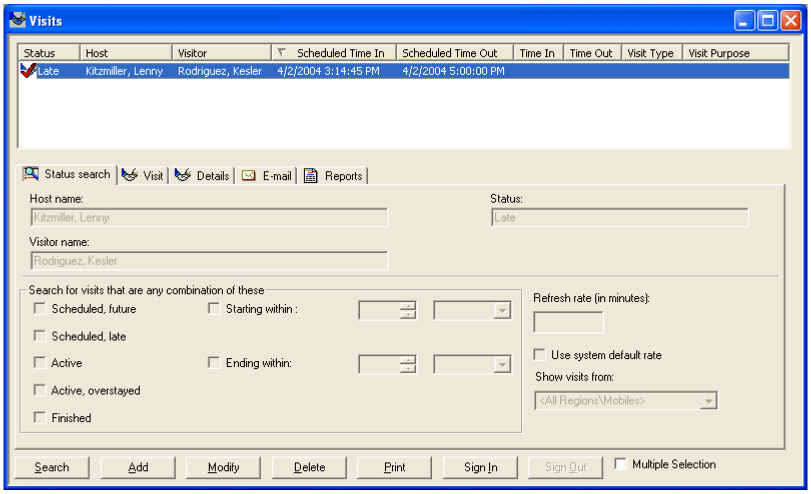
This window is only displayed when the Visit form in the Visits folder is in Search mode. In Search mode, click the [...] button to the right of the second **Scheduled time in**, **Time in**, **Scheduled time out** or **Time out** field.



Visit Form - Select Time Range Window Field Table

Form Element	Comment
Start time	Used when searching for the time portion of a scheduled time in, time in, scheduled time out or time out. Allows you to search for visits that start on or after or after a specified time. If “None” is selected, no time restraints are put on the visit records that are returned. (Visits that started at any time on the specified date will be returned.)
End time	Used when searching for the time portion of a scheduled time in, time in, scheduled time out or time out. Allows you to search for visits that end on or before or before a specified time. If “None” is selected, no time restraints are put on the visit records that are returned. (Visits that ended at any time on the specified date will be returned.)
OK	Enters the code for the selected search criteria in the respective field on the Visit form in the Visits folder.
Cancel	Closes the Select Time Range window without selecting a time search criteria.

Status Search Form



Status	Host	Visitor	Scheduled Time In	Scheduled Time Out	Time In	Time Out	Visit Type	Visit Purpose
Late	Kitzmiller, Lenny	Rodriguez, Kesler	4/2/2004 3:14:45 PM	4/2/2004 5:00:00 PM				

Host name: Kitzmiller, Lenny

Status: Late

Visitor name: Rodriguez, Kesler

Search for visits that are any combination of these

□ Scheduled, future
□ Starting within :
□ Scheduled, late
□ Active
□ Ending within:
□ Active, overstayed
□ Finished

Refresh rate (in minutes):

□ Use system default rate

Show visits from: <All Regions\Mobiles>

□ Multiple Selection

Status Search Form Overview

The Status Search form is only enabled when the [Search] button is clicked. It is used to:

- Search for Visits that meet a specified criteria (scheduled in the future, scheduled but late, active, finished, etc.)
- Set the refresh rate

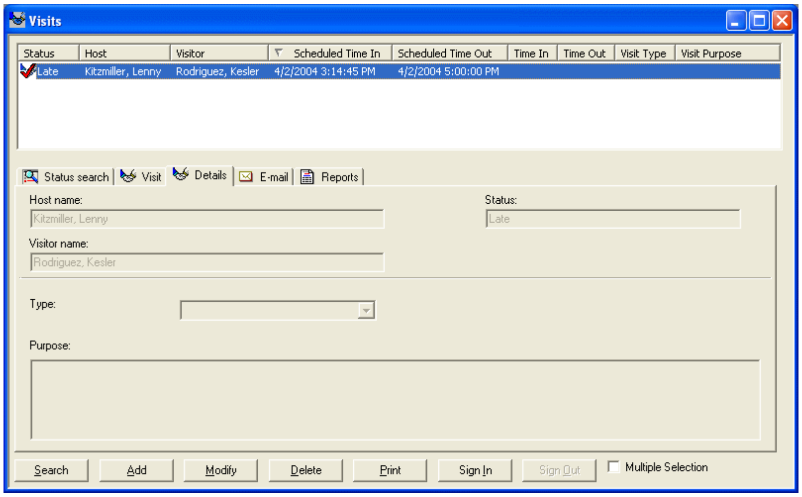
Status Search Form Field Table

Form Element	Comment
Scheduled, future	If selected, the search will find visits that are scheduled in the future, i.e., have a scheduled time in that is in the future and have not been signed in yet
Starting within	Enabled for selection only when the **Scheduled, future** check box is selected. If selected, specify the number of hours, days or minutes that the visit is scheduled to begin in. For example, you can search for all visits that are scheduled to begin within the next two days.
Scheduled, late	If selected, the search will find visits that are late, i.e., have a scheduled time in that is in the past and have not been signed in yet
Active	If selected, the search will find all visits that are currently signed in and have not been signed out yet
Ending within	Enabled for selection only when the **Active** check box is selected. If selected, specify the number of hours, days or minutes that the visit is scheduled to end in. For example, you can search for all visits that are scheduled to end within the next two days.
Active, overstayed	If selected, the search will find all visits that are currently signed in where the current date and time is after the scheduled time out. For example, a visitor that was supposed to leave at 3 p.m., but is still visiting at 5 p.m.
Finished	If selected, the search will locate visits that occurred in the past.

Status Search Form Field Table (Continued)

Form Element	Comment
Refresh rate (in minutes)	The refresh rate is how often the database is queried to see if it has changed. The refresh rate is stored on a per user basis and only applies when searching based on a status (i.e., the “Scheduled, future”, “Scheduled, late”, “Active”, “Active, overstayed” or “Finished” status) on the Status search form in the Visits folder. The default value is set in the **Refresh rate (in minutes)** field on the Visits form in the Cardholder Options form. A custom refresh rate can be specified as long as the **Use system default rate** check box is not selected.
Use system default rate	If selected, the system default rate will be used when refreshing. The system default rate is set in the **Refresh rate (in minutes)** field on the Visits form in the Cardholder Options folder. If not selected, a custom refresh rate can be specified in the **Refresh rate (in minutes)** field.
Show visits from	For Enterprise systems only: From this drop-down, select a server node (Regional or Master) or a mobile station from which to display visits. Alternatively, select "<All Regions\Mobiles>" to display visits from all server nodes and mobile stations. When a visit is added, in order for it to be displayed at another server node or mobile station, replication must be performed at the computer where the visit was added.

Details Form



Visits

Status	Host	Visitor	Scheduled Time In	Scheduled Time Out	Time In	Time Out	Visit Type	Visit Purpose
Late	Kitzmiller, Lenny	Rodriguez, Kesler	4/2/2004 3:14:45 PM	4/2/2004 5:00:00 PM				

Host name: Kitzmiller, Lenny

Status: Late

Visitor name: Rodriguez, Kesler

Type:

Purpose:

□ Multiple Selection

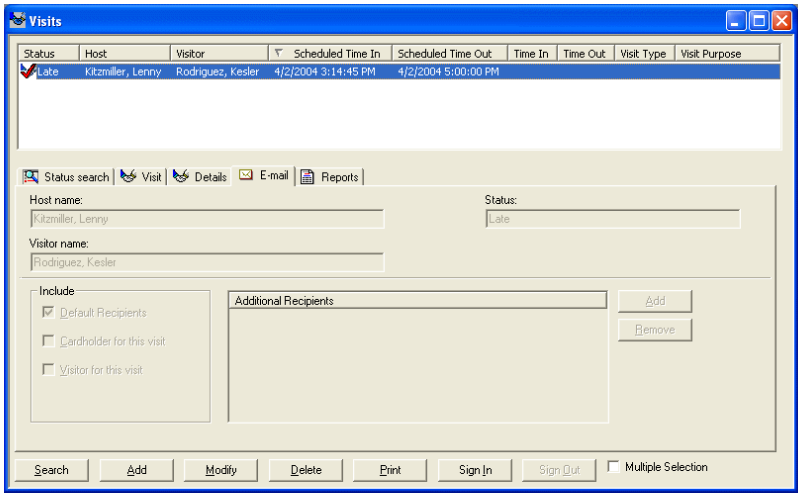
Details Form Overview

The Details form is a user-defined form that has been created for you. This form can be modified or even deleted using FormsDesigner. By default, the form contains the type and purpose of the visit.

Details Form Field Table

Form Element	Comment
Type	Select the type of visit. **Note:** Types of visits must first be configured in the List Builder, which is displayed by selecting the **Administration** menu, then selecting **List Builder**. For more information refer to the List Builder Folder chapter in the System Administration User Guide.
Purpose	Type the reason why the visitor is visiting the cardholder.

E-mail Form



Status	Host	Visitor	Scheduled Time In	Scheduled Time Out	Time In	Time Out	Visit Type	Visit Purpose
Late	Kitzmiller, Lenny	Rodriguez, Kesler	4/2/2004 3:14:45 PM	4/2/2004 5:00:00 PM				

Host name: Kitzmiller, Lenny

Status: Late

Visitor name: Rodriguez, Kesler

Include

☑ Default Recipients

□ Cardholder for this visit

□ Visitor for this visit

Additional Recipients

□ Multiple Selection

E-mail Form Overview

The E-mail form is used to specify e-mail addresses and pager numbers that are automatically notified of visits. You can:

- Add a recipient
- Remove a recipient
- Specify whether to e-mail the default recipients, the cardholder being visited and/or the visitor

E-mail Form Field Table

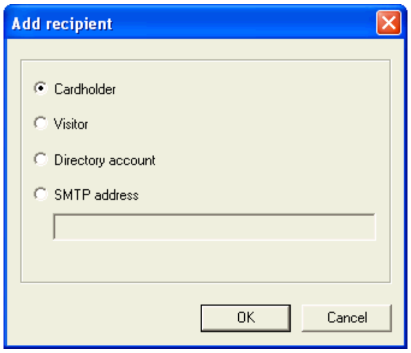
Form Element	Comment
Default Recipients	Select this check box if you wish to send e-mail messages to the default recipients. • On segmented systems, select **Administration** > **Segments**, click the Segments tab, then click the Visits sub-tab. On the Visits sub-tab, you can add or remove recipients. These recipients will be collectively considered the “Default Recipients” on the E-mail form in the Visits folder. • On non segmented systems, select **Administration** > **System Options**, then click the Visits tab. On the Visits tab, you can view or modify the default recipients. Whether this check box is selected by default when a new visit is added is determined by the **Include default recipients by default** check box on the Visits form in the Cardholder Options folder.
Cardholder for this visit	Select this check box if you wish to have an e-mail sent to the cardholder for this visit. Whether this check box is selected by default when a new visit is added is determined by the **Include host’s e-mail by default** check box on the Visits form in the Cardholder Options folder.
Visitor for this visit	Select this check box if you wish to have an e-mail sent to the visitor for this visit. Whether this check box is selected by default when a new visit is added is determined by the **Include visitor’s e-mail by default** check box on the Visits form in the Cardholder Options folder.

E-mail Form Field Table (Continued)

Form Element	Comment
Additional Recipients listing window	Displays the e-mail addresses that will receive e-mail notification of visits. **Note:** The addresses for the default recipients are not displayed in this listing window.
Add	Click this button if you wish to add another recipient. The Add recipient window is displayed. You may add a cardholder, visitor, directory account or SMTP address. • If you select the **Cardholder** radio button and click [OK], the Select Host Wizard: Search form is displayed. • If you select the **Visitor** radio button and click [OK], the Select Visitor Wizard: Search form is displayed. • If you select the **Directory account** radio button and click [OK], the Select Account window is displayed. • If you select the **SMTP address radio button**, type the SMTP address, then click [OK]. An example of an SMTP address is “joesmith@company.com”.
Remove	Removes the selected recipient from the list of recipients that will receive notification of visits.

Add Recipient Window

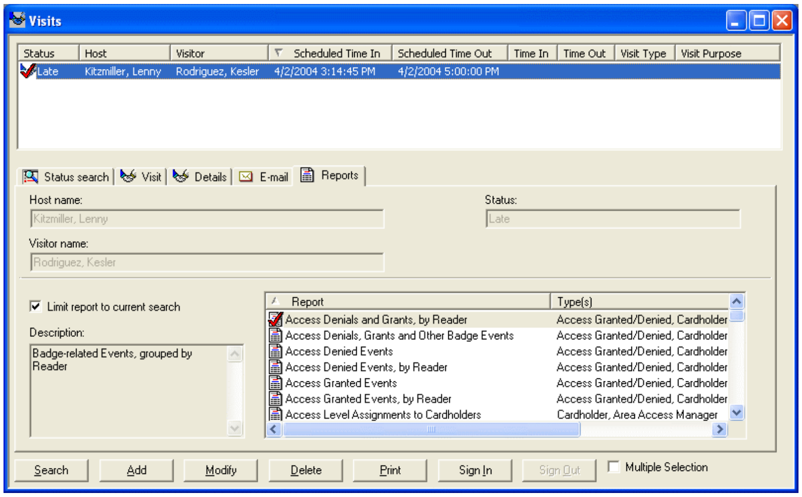
This window is displayed when the E-mail form in the Visits folder is in Add or Modify mode and the [Add] button to the right of the Additional Recipients listing window is clicked.



E-mail Form - Add Recipient Window Field Table

Form Element	Comment
Cardholder	The Select Host Wizard: Search form is displayed, which allows you to add a cardholder as an e-mail recipient. For more information, refer to Select Host Wizard: Search Form on page 156.
Visitor	The Select Visitor Wizard: Search form is displayed, which allows you to add a visitor as an e-mail recipient.
Directory account	The Select Account window is displayed, which allows you to add a directory account as an e-mail recipient.
SMTP address	Type the SMTP address, then click [OK]. An example of an SMTP address is "joesmith@company.com".
OK	• If you selected the **Cardholder** radio button, the Select Host Wizard: Search form is displayed. For more information, refer to Select Host Wizard: Search Form on page 156. • If you selected the **Visitor** radio button, the Select Visitor Wizard: Search form is displayed. For more information, refer to Select Visitor Wizard: Search Form on page 160. • If you selected the **Directory account** radio button, the Select Account window is displayed. • If you selected the **SMTP address** radio button and typed an SMTP address, the address will be added to the Additional Recipients listing window.
Cancel	Closes the Add recipient window without adding a recipient.

Reports Form



Status	Host	Visitor	Scheduled Time In	Scheduled Time Out	Time In	Time Out	Visit Type	Visit Purpose
Late	Kitzmiller, Lenny	Rodriguez, Kesler	4/2/2004 3:14:45 PM	4/2/2004 5:00:00 PM				

Host name: Kitzmiller, Lenny

Status: Late

Visitor name: Rodriguez, Kesler

☑ Limit report to current search

Description: Badge-related Events, grouped by Reader

Report	Type(s)
Access Denials and Grants, by Reader	Access Granted/Denied, Cardholder
Access Denials, Grants and Other Badge Events	Access Granted/Denied, Cardholder
Access Denied Events	Access Granted/Denied, Cardholder
Access Denied Events, by Reader	Access Granted/Denied, Cardholder
Access Granted Events	Access Granted/Denied, Cardholder
Access Granted Events, by Reader	Access Granted/Denied, Cardholder
Access Level Assignments to Cardholders	Cardholder, Area Access Manager

□ Multiple Selection

Reports Form Overview

The Reports form shows only visit-related reports. On the Reports form you can:

- Search for a cardholder
- Search for a visitor
- Generate a report

Reports Form Field Table

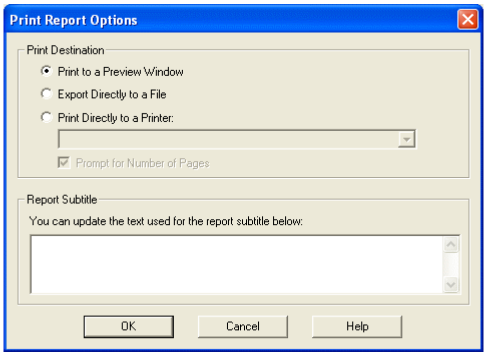
Form Element	Comment
Limit report to current search	If selected, the report will only include those records that match the rest of the search criteria specified on any form in the Visits folder. If not selected, the report will include all records for the selected report type.
Description	A brief description of the report contents.
Report listing window	Lists currently defined reports of the type(s) selected in the Report listing window.

Reports Form Procedures

Run a Visit Report from the Visits Folder

A visit report can be generated for either a defined search criteria or for all visits.

1. If you wish to generate a visit report that searches through all visit records not just those that match a search criteria, proceed to step 2. To generate a visit report based on a search criteria:
   a. Select **Visits** from the **Administration** menu. The Visits folder opens.
   b. In the Visits folder, click [Search].
   c. Run the search that you wish to print a report for. For more information on searching refer to the following:
      - Visit Search Capabilities on page 131
      - Search for All Visits to a Selected Cardholder on page 133
      - Search for All Visits by a Selected Visitor on page 133
      - Search for Scheduled, Active or Finished Visits on page 133
      - Search for All Visits for a Specific Date or Time on page 134
      - Retrieve the Most Recent Visit Search Results on page 136
   d. Click the Reports tab.
   e. Select the **Limit report to current search** check box.
   f. Proceed to step 3.
2. To generate a visit report that searches through all visits:
   a. Select **Visits** from the **Administration** menu. The Visits folder opens.
   b. In the Reports listing window, select the type of report you wish to print.
   c. Proceed to step 3.
3. Click [Print]. The Print Report Options window opens.



Print Report Options

Print Destination

● Print to a Preview Window

○ Export Directly to a File

○ Print Directly to a Printer:

☑ Prompt for Number of Pages

Report Subtitle

You can update the text used for the report subtitle below:

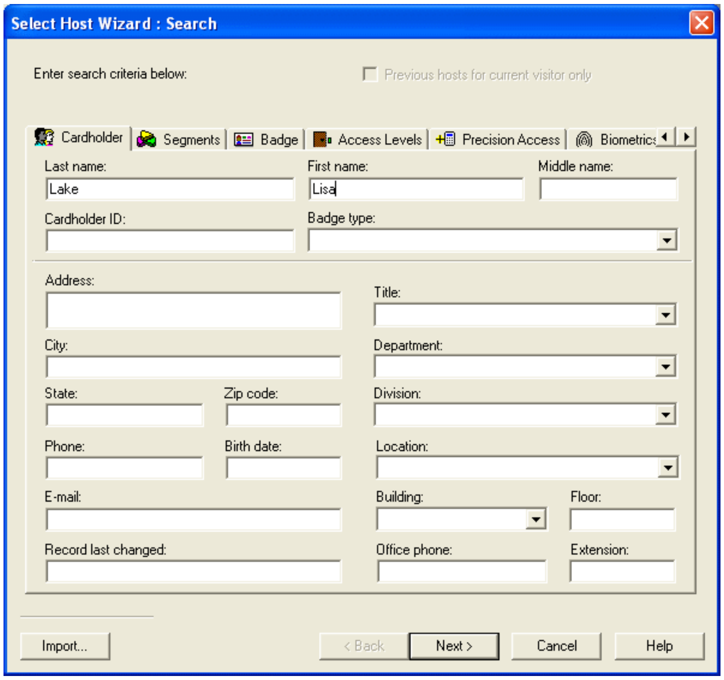
4. In the Print Destination section, select whether to print to a preview window, export directly to a file or print directly to a printer.
5. If you selected **Print Directly to a Printer** in the Print Destination section, select a printer in the drop-down list and choose whether to **Prompt for Number of Pages**.

6. In the Report Subtitle section, type the report subtitle. If the **Limit report to current search** check box is selected, the search criteria will be listed in the Report Subtitle section by default. The subtitle will be displayed below the report title on the report.
7. Click [OK]. The options selected in the Print Destination section will determine where the report is sent.

Select Host Wizard: Search Form

Note: If the FormsDesigner application has been used to customize your cardholder data, the elements on your Select Host Wizard: Search form will be different. The default fields are pictured below.

This form is displayed when the [Search] button in the Visits folder is clicked and then the [...] button to the right of the **Host name** field is clicked.



Last name: Lake

First name: Lisa

Select Host Wizard: Search Form Overview

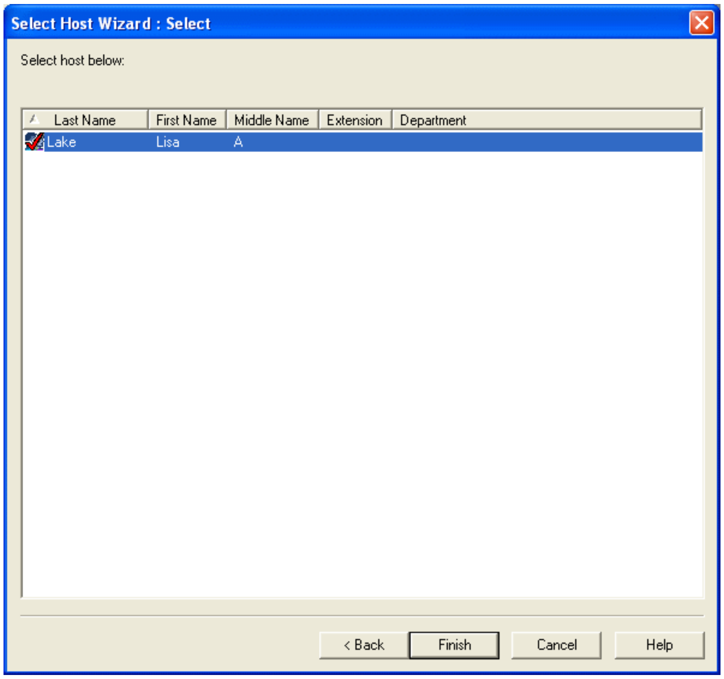
This form is used to enter search criteria that will allow you to locate a specific cardholder.

Visits Folder - Select Host Wizard: Search Form

Form Element	Comment
Previous hosts for current visitor only	This check box is only enabled when a visitor has been selected and a cardholder is being searched for. If selected, only those cardholders who have previously been visited by the selected visitor will be displayed on the Select Visitor: Select or Add form.
Last name	Indicates cardholder's last name.
First name	Indicates cardholder's first name.
Middle name	Indicates cardholder's middle name.
Cardholder ID	Indicates a cardholder's ID, which is most commonly their Social Security Number. The cardholder ID must be a numeric value.
Badge type	Selects which of the cardholder's badges (if he or she has more than one) is to be the active one.
User-defined fields	All fields below the line on this form are user-defined fields. The default fields are pictured, but your form may be different if the FormsDesigner application has been used to customize your cardholder data.
Back	This button is not used.
Next	The wizard will proceed to the Select Host Wizard: Select form.
Cancel	Closes the window without locating a cardholder and returns you to the Visit form in the Visits folder.
Help	Displays online help for this topic
Import	Displays the Select Import Source window, which allows you to select a device to import cardholder data from, such as a business card scanner

Select Host Wizard: Select Form

This form is displayed when the [Next] button on the Select Host Wizard: Search form is clicked.



Last Name	First Name	Middle Name	Extension	Department
Lake	Lisa	A		

Select Host Wizard: Select Form Overview

This form is used to select a cardholder record from those that matched the specified search criteria. The columns displayed are configured on the Cardholder Search Results form in the Cardholder Options folder. For more information refer to the Segments Folder chapter in the System Administration User Guide.

Visits Folder - Select Host Wizard: Select Form

Form Element	Comment
Cardholder listing window	A list of cardholder records that match the search criteria specified on the Select Host Wizard: Search form are displayed. **Note:** The fields that are displayed in columns are set on the Cardholder Search Results Lists form in the Cardholder Options folder.
Back	Returns to the Select Host Wizard: Search form.
Finish	Completes the wizard. The selected cardholder’s name will be displayed in the **Host name** field.
Cancel	Closes the window without selecting a cardholder and returns you to the Visit form in the Visits folder.

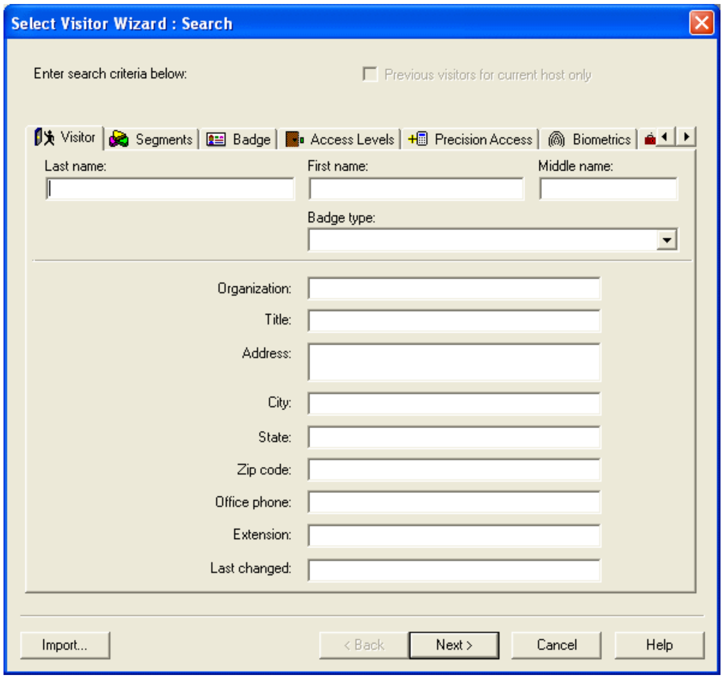
Visits Folder - Select Host Wizard: Select Form (Continued)

Form Element	Comment
Help	Displays online help for this topic

Select Visitor Wizard: Search Form

Note: If the FormsDesigner application has been used to customize your visitor data, the elements on your Select Visitor Wizard: Search form will be different. The default fields are pictured below.

This form is displayed when the [...] button to the right of the **Visitor name** drop-down list on the Visit form is clicked.



Select Visitor Wizard: Search Form Overview

This form is used to locate visitor records that match the specified search criteria.

Visits Folder - Select Visitor Wizard: Search Form

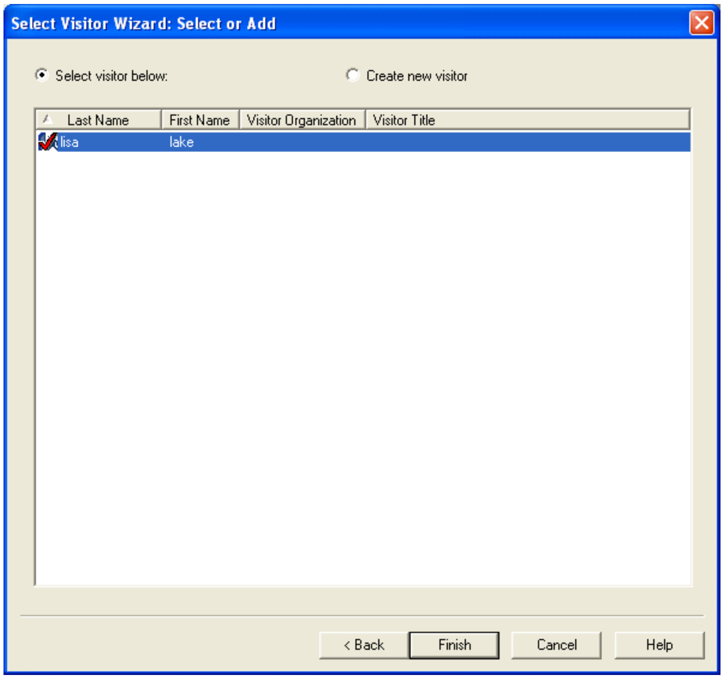
Form Element	Comment
Previous visitors for current host only	This check box is only enabled when a cardholder has been selected and a visitor is being searched for. If selected, only those visitors who have previously visited the selected cardholder will be displayed on the Select Visitor: Select or Add form.
Last name	Indicates visitor’s last name.
First name	Indicates visitor’s first name.
Middle name	Indicates visitor’s middle name.

Visits Folder - Select Visitor Wizard: Search Form (Continued)

Form Element	Comment
Badge type	Indicates the visitor’s badge type. Badge types are configured in the Badge Types folder. For more information refer to the Badge Types Folder chapter in the System Administration User Guide.
User-defined fields	All fields below the horizontal line on this form are user-defined fields. The default fields are pictured, but your form may be different if the FormsDesigner application has been used to customize your visitor data.
Back	This button is not used.
Next	The wizard will proceed to the Select Visitor Wizard: Select or Add form.
Cancel	Closes the window without locating a visitor and returns you to the Visit form in the Visits folder.
Import	Displays the Select Import Source window, which allows you to select a device to import visitor data from, such as a business card scanner
Help	Displays online help for this topic

Select Visitor Wizard: Select or Add Form

This form is displayed when the [Next] button on the Select Visitor Wizard: Search form is clicked.



Select Visitor Wizard: Select or Add

● Select visitor below: ○ Create new visitor

Last Name	First Name	Visitor Organization	Visitor Title
lisa	lake		

Select Visitor Wizard: Select or Add Form Overview

This form is displayed when adding a visit. From this form, you can:

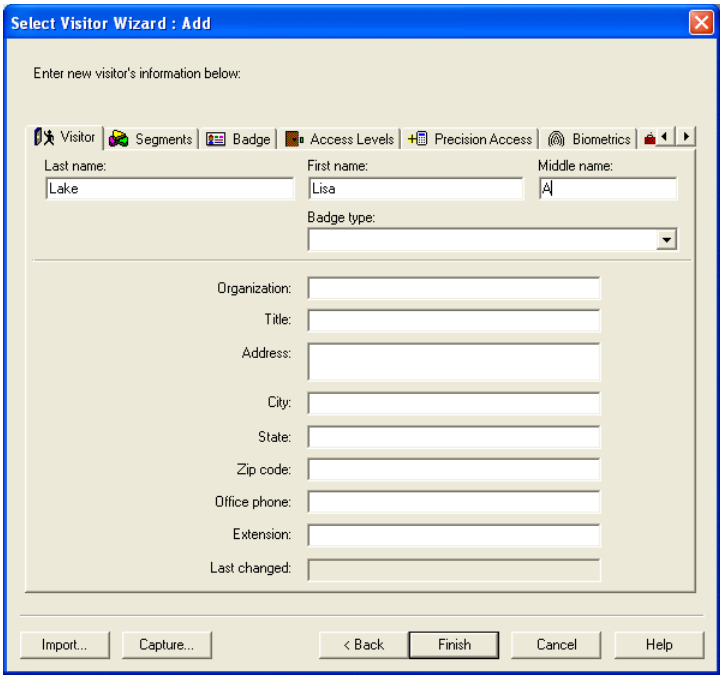
- Search for visitor records that match the specified search criteria.
- Add a new visitor record.

Visits Folder - Select Visitor Wizard: Select or Add Form

Form Element	Comment
Select visitor below	Select this option if the visitor you need to add a visit for is listed below in the Visitor listing window. If you select this option, also select a visitor in the Visitor listing window below.
Create new visitor	Select this option if the visitor you need to add a visit for is not listed in the Visitor listing window. If you select this option, the [Finish] button will be replaced with a [Next] button. When the [Next] button is clicked, the Select Visitor Wizard: Add form will be displayed, on which you can add a new visitor.
Visitor listing window	A list of visitor records that match the search criteria specified on the Select Visitor Wizard: Search form are displayed. **Note:** The fields that are displayed in columns are set on the Visitor Search Results Lists form in the Cardholder Options folder.
Back	Returns to the Select Visitor Wizard: Search form.
Finish	This button is displayed only if **Select visitor below** is selected. Click this button to complete the wizard. The selected visitor’s name will be displayed in the **Visitor name** field. If **Create new visitor** is selected, the [Finish] button is replaced by a [Next] button.
Cancel	Closes the window without selecting a visitor and returns you to the Visit form in the Visits folder.
Help	Displays online help for this topic

Select Visitor Wizard: Add Form

This form is displayed when **Create new visitor** is selected and the [Next] button is clicked on the Select Visitor Wizard: Select or Add form.



Select Visitor Wizard : Add

Enter new visitor's information below:

Last name: Lake

First name: Lisa

Middle name: A

Badge type:

Organization:

Title:

Address:

City:

State:

Zip code:

Office phone:

Extension:

Last changed:

Select Visitor Wizard: Add Form Overview

This form allows you to:

- Add a new visitor record
- Capture photographic information such as a photo, signature or biometric data for a visitor
- Import visitor data from a business card scanner or other similar device

Visits Folder - Select Visitor Wizard: Add Form

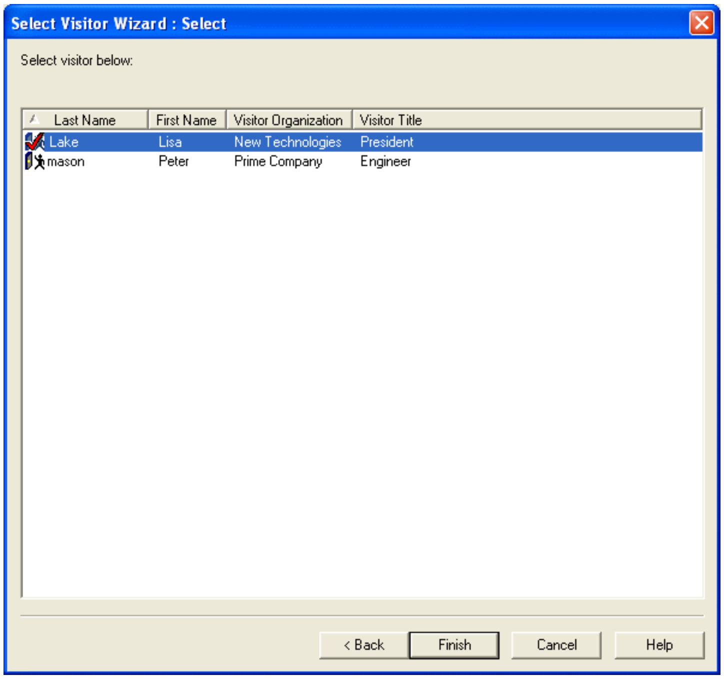
Form Element	Comment
Last name	Indicates visitor’s last name.
First name	Indicates visitor’s first name.
Middle name	Indicates visitor’s middle name.
Badge type	Select the visitor’s badge type. Badge types are configured in the Badge Types folder. For more information refer to the Badge Types Folder chapter in the System Administration User Guide.

Visits Folder - Select Visitor Wizard: Add Form (Continued)

Form Element	Comment
User-defined fields	All fields below the Name fields on this form are user-defined fields. The default fields are pictured, but your form may be different if the FormsDesigner application has been used to customize your visitor data.
Import	Displays the Select Import Source window, which allows you to select a device to import visitor data from, such as a business card scanner
Capture	Displays Multimedia Capture, where you can capture photographic information such as a photo, signature or biometric data for a visitor
Back	Returns to the Select Visitor Wizard: Select or Add form.
Finish	Completes the wizard. The visitor record will be added to the database and the name of the visitor who was just added will be displayed in the **Visitor name** field.
Cancel	Closes the window without adding a visitor and returns you to the Visit form in the Visits folder.
Help	Displays online help for this topic

Select Visitor Wizard: Select Form

This form is displayed when the [...] button to the right of the Visitor name field on the Visit form in the Visits folder is clicked.



Select visitor below:

Last Name	First Name	Visitor Organization	Visitor Title
Lake	Lisa	New Technologies	President
mason	Peter	Prime Company	Engineer

Select Visitor Wizard: Select Form Overview

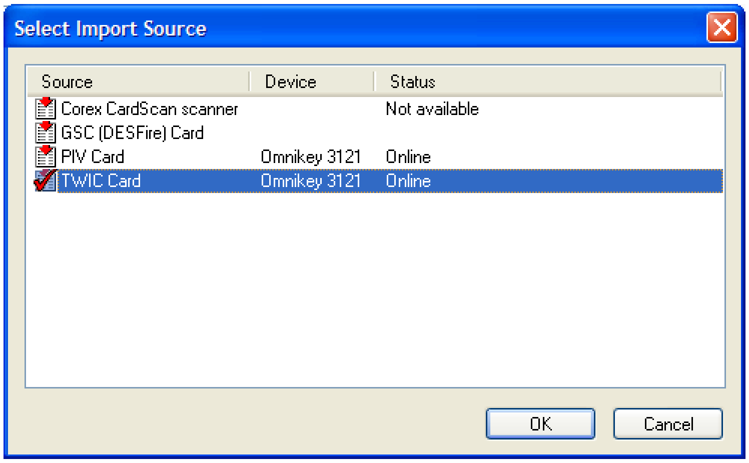
This form is displayed when searching; it is used to select a visitor record from those that matched the specified search criteria.

Visits Folder - Select Visitor Wizard: Select Form

Form Element	Comment
Last Name	Indicates visitor’s last name.
First Name	Indicates visitor’s first name.
Middle Initial	Indicates visitor’s middle initial.
User-defined fields	All fields below the Name fields on this form are user-defined fields. The default fields are pictured, but your form may be different if the FormsDesigner application has been used to customize your visitor data.
Back	Returns to the previous form.
Finish	Completes the wizard. The selected visitor’s name will be displayed in the **Visitor name** field.
Cancel	Closes the window without selecting a visitor and returns you to the Visit form in the Visits folder.
Help	Displays online help for this topic

Select Import Source Window

This window is displayed by clicking the [Import] button on any window in the Select Host Wizard or Select Visitor Wizard.



Source	Device	Status
Corex CardScan scanner		Not available
GSC (DESFire) Card		
PIV Card	Omnikey 3121	Online
✓ TWIC Card	Omnikey 3121	Online

Select Import Source Window Field Table

Form Element	Comment
Source listing window	Displays a list of available sources, such as a business card scanner, to import cardholder or visitor data from.
OK	If a valid source is selected, you will be able to import cardholder or visitor data using it.
Cancel	Closes the Select Import Source window without selecting a source to import cardholder or visitor data from.

Chapter 15: Assets Folder

The Assets folder contains forms with which you can:

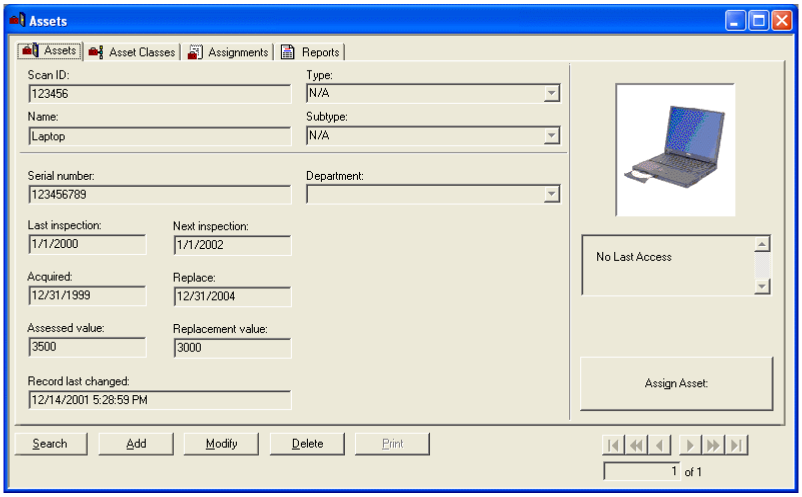
- Add, change or remove asset records.
- Assign assets to cardholders.
- Track assets that are assigned to cardholders.
- Preview and print asset reports.

The Assets folder contains four forms: the Assets form, the Asset Classes form, the Assignments form and the Reports form.

Toolbar Shortcut

This folder is displayed by selecting the **Asset Info** from the **View** menu.

Assets Form



Scan ID: 123456

Type: N/A

Name: Laptop

Subtype: N/A

Serial number: 123456789

Department:

Last inspection: 1/1/2000

Next inspection: 1/1/2002

Acquired: 12/31/1999

Replace: 12/31/2004

Assessed value: 3500

Replacement value: 3000

Record last changed: 12/14/2001 5:28:59 PM

No Last Access

1 of 1

Assets Folder - Assets Form

Form Element	Comment
Scan ID	Enter the Scan ID of the asset.
Name	Enter a descriptive name for the asset. This is a “friendly” name assigned to each asset to make it easy to identify. Each name must be unique and contain no more than 32 characters.
Type	Select the type of asset being configured. Available choices depend on what asset types were added in the Asset Types and Subtypes Management window. The window is displayed by selecting **Asset Types and Subtypes** from the **Asset** menu.
Subtype	Select the subtype of the asset being configured. Available choices depend on what asset subtypes were added in the Asset Types and Subtypes Management window. The window is displayed by selecting **Asset Types and Subtypes** from the **Asset** menu.
Serial Number	Enter the serial number of the asset you are adding.
Department	Select the department of the asset being configured. Available choices depend on what departments were added in the List Builder folder.
Last Inspection	Enter the date when the asset was last inspected.
Next Inspection	Enter the date when the asset will be inspected next.
Acquired	Enter the date when the asset was acquired.
Replace	Enter the date when the asset will be replaced.
Assessed Value	Enter the assessed value of the asset.
Replacement Value	Enter the replacement value of the asset.
Record Last Changed	Indicates the date of when the selected asset record was last changed.
Photo	Displays a photo capture of the asset if one was added in Multimedia Capture.

Assets Folder - Assets Form (Continued)

Form Element	Comment
Last Access	Displays the date and time of the asset's last access.
Assign Asset/ Assign To	When adding or modifying an asset, select the [Assign Asset] button to launch the Cardholders folder. On the Cardholder form you can search for or add a cardholder to assign to the asset being configured. Once you have located the cardholder on the Cardholder form, their name will appear on the [Assign To] push button. Click on this button to assign the asset to the cardholder. If the Cardholders folder is already open and a cardholder record is displayed, then the [Assign To] button will automatically display the name of that cardholder record.
Search	Click on this button to search for an asset based on a value entered in one or more of the fields.
Last Search	Click on this button the display the findings of the previous search.
⏮	Moves to the first matching record.
⏪	Moves 10 matching records back.
◀	Moves to the previous matching record.
▶	Moves to the next matching record.
⏩	Moves 10 matching records forward.
⏭	Moves to the last matching record.
Record count	Displayed in view mode and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.
Add	Used to add an asset record.
Capture	Launches Multimedia Capture where you can add a photo of the asset.
Modify	Used to change an asset record.
Delete	Used to delete an asset record.

Assets Form Procedures

Add an Asset

Note: This procedure does not apply to view/edit only workstations.

1. Select **Asset Info** from the **View** menu. The Assets folder opens.
2. Click [Add].
3. In the **Scan ID** field, enter an ID number for the asset.
4. In the **Name** field, enter a descriptive name for the asset. This is a “friendly” name assigned to each asset to make it easy to identify. Each name must be unique and contain no more than 32 characters.
5. If you want to identify the asset by type, select one from the **Type** drop-down list. If you want to identify the asset by subtype, select one from the **Subtype** drop-down list. If you don’t want to identify the asset by type and/or subtype, choose N/A from the **Type** and **Subtype** drop-down lists.
6. Type in a **Serial Number** and then choose the **Department** of the asset from the drop-down list.
7. Enter the date of the asset’s **Last Inspection** and the date of the asset’s **Next Inspection**.
8. Enter the date of when the asset was acquired in the **Acquired** field.
9. Enter the date of when the asset will be replaced in the **Replace** field.
10. In the **Assessed Value** field type the amount, in dollars, of the asset’s value. In the **Replacement Value** field type the amount, in dollars, it will cost to replace the asset.
11. Click [Capture] to launch Multimedia Capture from where you can capture a photo of the asset to be displayed on the Assets form. For more information refer to the Multimedia Capture appendix in the System Administration User Guide.
12. You can switch to the Asset Classes form if you want to configure groups and classes now. For more information, refer to Asset Classes Form Procedures on page 252.
13. Click [OK].

Modify an Asset

Note: This procedure does not apply to view only workstations.

1. Locate the asset record that you want to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save your changes, or [Cancel] to revert to the previously saved values.

Delete an Asset

Note: This procedure does not apply to view/edit only workstations.

1. Locate the asset record that you want to delete.
2. Click [Delete].
3. Click [OK].

Assign a Cardholder to an Asset

Note: This procedure does not apply to view only workstations.

1. Locate the asset record that you want to assign.
2. If the Cardholders folder was already open and a cardholder record displayed, proceed to 3. If not, click [Assign Asset] to launch the Cardholders folder.
3. In the Cardholders folder, retrieve the record of the cardholder you want to assign to the asset. On the Assets form of the Assets folder, the name of the cardholder will appear in the [Assign To] push button.
4. Click [Assign To] to assign the asset.

Search for an Asset Record

1. Select **Asset Info** from the **View** menu. The Assets folder opens.
2. Click [Search].
3. Specify your search criteria by typing full partial entries in the enabled fields.
4. Click [OK].
   ReadykeyPRO retrieves and displays the first matching record. Use the ⏮, ⏪, ◀, ▶, ⏩ and ⏭ buttons to navigate through the database. A dimmed button means that the associated operation is not possible (e.g., moving to the next record while the last record is being displayed).

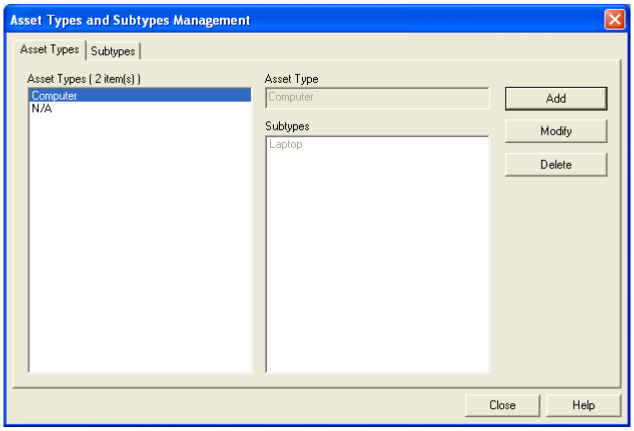
Retrieve the Most Recent Search Results

1. Click [Search].
2. Click [Last Search]. The criteria you selected from the most recent search operation will be inserted into the appropriate fields.
3. If you want, modify your search criteria.
4. Click [OK].
   ReadykeyPRO retrieves and displays the first matching record. Use the ⏮, ⏪, ◀, ▶, ⏩ and ⏭ buttons to navigate through the database. A dimmed button means that the associated operation is not possible (e.g., moving to the next record while the last record is being displayed).

Add an Asset Type/Subtype

Note: This procedure does not apply to view only workstations.

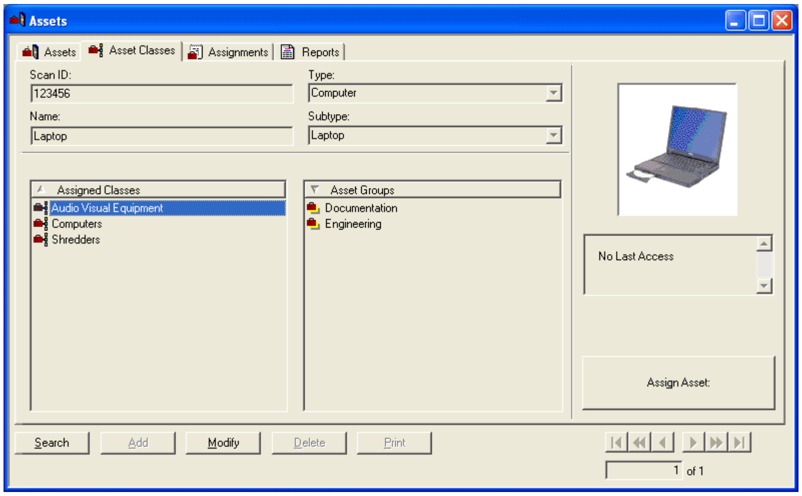
1. Select **Asset Info** from the **View** menu. The Assets folder opens.
2. Select **Asset Types and Subtypes** from the **Asset** menu. The Asset Types and Subtypes Management window opens.



3. Select and asset type in the Asset Types listing window. If you want to modify a subtype, select the Subtype tab first.
4. Click [Modify] and make your desired changes.
5. Click [OK].
6. Click [Close] to return to the Assets form.

Asset Classes Form

Asset Classes Form (View Mode)



Scan ID: 123456

Type: Computer

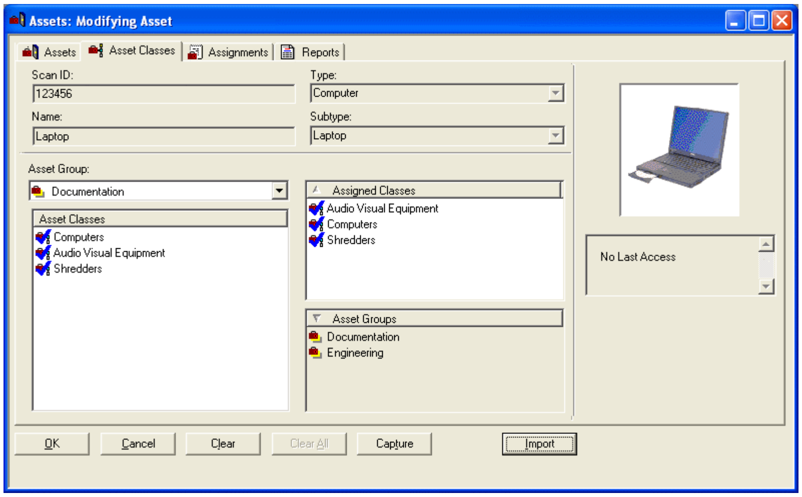
Name: Laptop

Subtype: Laptop

Assigned Classes	Asset Groups
Audio Visual Equipment	Documentation
Computers	Engineering
Shredders	

No Last Access

Asset Classes Form (Modify Mode)



Scan ID: 123456

Type: Computer

Name: Laptop

Subtype: Laptop

Asset Group: Documentation

Asset Classes
- Computers
- Audio Visual Equipment
- Shredders

Assigned Classes
- Audio Visual Equipment
- Computers
- Shredders

Asset Groups
- Documentation
- Engineering

No Last Access

Asset Classes Form Field Table

Assets Folder - Asset Classes Form

Form Element	Comment
Scan ID	Indicates the Scan ID of the asset.
Name	Indicates the name of the asset.
Type	Indicates the type of asset being configured.
Subtype	Indicates the subtype of the asset being configured.
Assigned Classes	(View and modify mode) Displays the classes that are currently assigned to a group in the Asset Groups listing window.
Asset Groups	(View mode) Displays the asset groups that correspond with the classes in the Assigned Classes listing window.
Asset Group	(Modify mode) Select the asset group(s) to which the asset will belong.
Asset Classes	Select the asset classes that will be assigned to the asset. Groups can contain as many as 32 classes, but each asset can only belong to as many as 15 classes.
Photo	Displays a photo capture of the asset if one was added in Multimedia Capture.
Last Access	Displays the date and time of the asset's last access.
Assign Asset/ Assign To	When adding or modifying an asset, select the [Assign Asset] button to launch the Cardholders folder. On the Cardholders form you can search for or add a cardholder to assign to the asset being configured. Once you have located the cardholder on the Cardholders form, their name will appear on the [Assign To] push button. Click on this button to assign the asset to the cardholder. If the Cardholders folder is already open and a cardholder record is displayed, then the [Assign To] button will automatically display the name of that cardholder record.
Search	Click on this button to search for an asset based on a value entered in one or more of the fields.
Last Search	Click on this button the display the findings of the previous search.
⏮	Moves to the first matching record.
⏪	Moves 10 matching records back.
◀	Moves to the previous matching record.
▶	Moves to the next matching record.
⏩	Moves 10 matching records forward.
⏭	Moves to the last matching record.

Assets Folder - Asset Classes Form (Continued)

Form Element	Comment
Record count	Displayed in view mode and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.
Add	This button is not used.
Modify	Used to change an asset classes record.
Delete	This button is not used.
Print	This button is not used.

Asset Classes Form Procedures

Assign Classes to an Asset

Note: This procedure does not apply to view only workstations.

1. Locate the record of the asset that you want to assign classes to.
2. Click [Modify].
3. Select an **Asset Group** from the drop-down list.
4. In the **Asset Classes** listing window, select the classes you want to assign. You can select as many as 15 classes for each asset.
5. Click [OK].

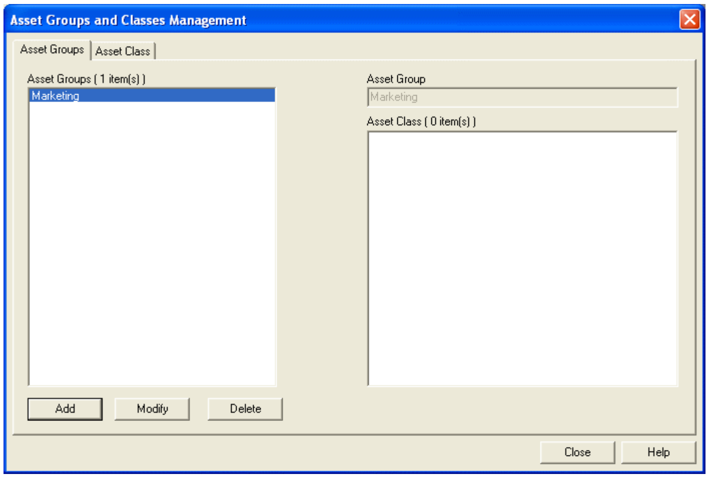
Modify an Asset Classes Assignment

Note: This procedure does not apply to view only workstations.

1. Locate the record of the asset that you want to change.
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save your changes, or [Cancel] to revert to the previously saved values.

Add Asset Groups and Classes

1. Select **Asset Info** from the **View** menu. The Assets folder opens.
2. Select **Asset Groups and Classes** from the **Asset** menu. The Asset Groups and Classes Management window opens.



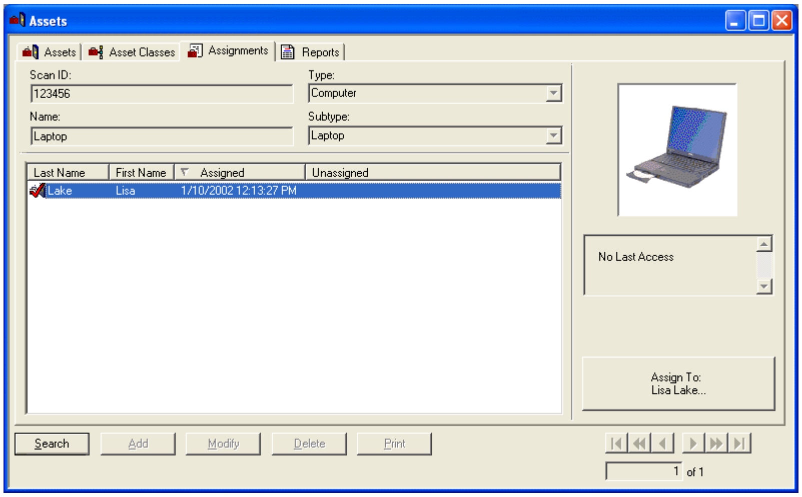
Asset Groups (1 item(s))
Marketing

Asset Group: Marketing

Asset Class (0 item(s))

3. To add an asset group:
   a. Click the Asset Groups tab.
   b. Click [Add].
   c. In the **Asset Group** field, enter the name of the group you are adding.
   d. Click [OK].
4. To add an asset class:
   a. Click the Asset Class tab.
   b. Click [Add].
   c. In the **Asset Class** field, enter the name of the class you are adding. You can add as many classes as you want but you can only assign as many as 32 classes to a group.
   d. Click [OK].
5. To assign a class to a group:
   a. Click the Asset Class tab.
   b. Select an asset class.
   c. Click [Modify].
   d. Select the name of an asset group.
   e. Click the <-- push button to remove the asset group. Click the --> push button add the asset group.
   f. Click [OK].

Assignments Form



Scan ID: 123456

Type: Computer

Name: Laptop

Subtype: Laptop

Last Name	First Name	Assigned	Unassigned
Lake	Lisa	1/10/2002 12:13:27 PM	

No Last Access

Assign To:
Lisa Lake...

1 of 1

Assets Folder - Assignments Form

Form Element	Comment
Scan ID	Displays the assets scan ID. If you click [Search], you can enter the scan ID you want to search.
Name	Displays the name of the asset. If you click [Search], you can enter the name of the asset you want to search.
Type	Displays the type of asset. If you click [Search], you can enter the type of asset you want to search.
Subtype	Displays the subtype of the asset. If you click [Search], you can enter the subtype of the asset you want to search.
Listing window	Displays a list of cardholders who are currently or have been assigned to the selected asset. You can choose the number of entries you want listed by selecting **Show Assignments X Days Past** from the **Asset** menu.
Last Name	When you select the [Search] button, enter the last name of a cardholder to locate the assets that have been assigned to them.
First Name	When you select the [Search] button, enter the first name of a cardholder to locate the assets that have been assigned to them.
Assigned	When you select the [Search] button, enter the date the asset was assigned if you want to locate the cardholder who was assigned to the asset on that date.
Unassigned	When you select the [Search] button, enter the date the asset was unassigned if you want to locate the cardholder who was unassigned to the asset on that date.
Photo	Displays a photo of the asset if one was captured in Multimedia Capture.
Last Access	Displays the date and time of the assets last access.

Assets Folder - Assignments Form (Continued)

Form Element	Comment
Assign Asset/ Assign To	Displays the name of the asset currently displayed in the Cardholders folder. If no name is displayed, when selected the Cardholders folder is launched from where you can search for and select the cardholder you wish to assign to the asset.
Search	Used to locate a cardholder or asset assignment record.
Last Search	Click on this button the display the findings of the previous search.
⏮	Moves to the first matching record.
⏪	Moves 10 matching records back.
◀	Moves to the previous matching record.
▶	Moves to the next matching record.
⏩	Moves 10 matching records forward.
⏭	Moves to the last matching record.
Record count	Displayed in view mode and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.

Assignments Form Procedures

Assign a Cardholder to an Asset

Note: This procedure does not apply to view only workstations.

1. Locate the record of that asset that you want to assign.
2. If the Cardholders folder was already open and a cardholder record displayed, proceed to 3. If not, click [Assign Asset] to launch the Cardholders folder.
3. On the Cardholders folder, retrieve the record of the cardholder you want to assign to the asset. On the Assignments form of the Assets folder, the name of the cardholder will appear in the [Assign To] push button.
4. Click [Assign To] to assign the selected asset to the selected cardholder. The name of the cardholder will appear in the listing window.

Unassign an Asset

Note: This procedure does not apply to view only workstations.

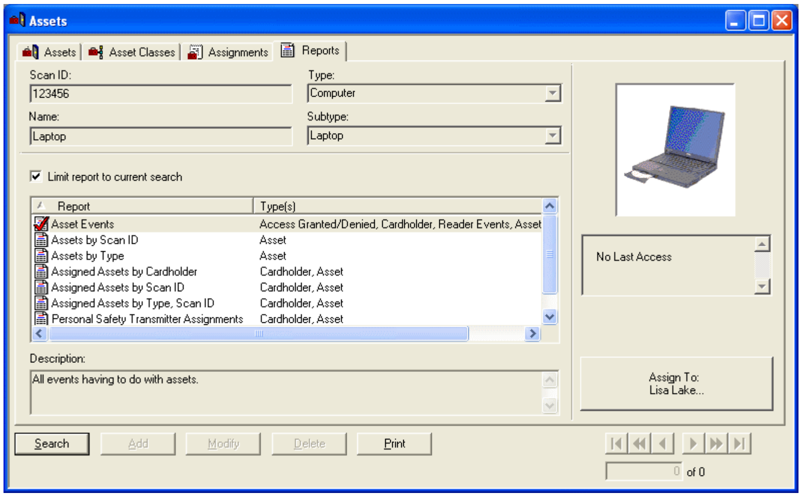
1. Locate the record of the asset that you want to unassign.
2. In the listing window, select the name of the cardholder who is currently assigned to the asset. The entry of the cardholder who is assigned will not list an **Unassigned** Date.
3. Right-click on the cardholder entry you selected and choose **Unassign Asset** from the menu. The **Unassigned** field will be updated to the current date.

Search for a Cardholder Assigned to an Asset

1. Locate the asset record that you want to look up a cardholder for.
2. In the listing window, select the name of the cardholder you want to look up.
3. Right-click on the cardholder entry you selected and choose **Find Cardholder** from the menu. The Cardholders folder will display the record of the cardholder you selected.

Reports Form

Note: The Reports form is not available in view/edit only workstations or in the Alarm Monitoring application.



Scan ID: 123456

Type: Computer

Name: Laptop

Subtype: Laptop

☑ Limit report to current search

Report	Type(s)
Asset Events	Access Granted/Denied, Cardholder, Reader Events, Asset
Assets by Scan ID	Asset
Assets by Type	Asset
Assigned Assets by Cardholder	Cardholder, Asset
Assigned Assets by Scan ID	Cardholder, Asset
Assigned Assets by Type, Scan ID	Cardholder, Asset
Personal Safety Transmitter Assignments	Cardholder, Asset

Description: All events having to do with assets.

No Last Access

Assign To:
Lisa Lake...

0 of 0

Assets Folder - Reports Form

Form Element	Comment
Scan ID	Displays the scan ID of the selected asset.
Name	Displays the name of the selected asset.
Type	Displays the type of the selected asset.
Subtype	Displays the subtype of the selected asset.
Listing window	Displays a list of the types of reports that can be previewed and/or printed. An 🗎 icon precedes each entry.
Limit report to current search	Select this check box if you want to limit this report to the search that you just completed.
Description	Displays a description of the report type you selected from the listing window.
Filename	Displays the file name of the report type.
Photo	Displays the captured photo of the currently selected asset.
Last Access	Displays the date and time of the asset's last access.
Assign Asset/ Assign To	Displays the name of the cardholder currently displayed in the Cardholders folder. If no name is displayed, when selected the Cardholders folder is launched from where you can search for and select the cardholder you wish to assign to the selected asset.

Assets Folder - Reports Form (Continued)

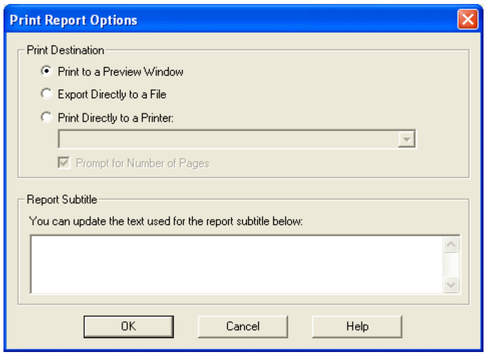
Form Element	Comment
Print	This button launches the Report Print Options window from where you can preview, print or export a report.
⏮	Moves to the first matching record.
⏪	Moves 10 matching records back.
◀	Moves to the previous matching record.
▶	Moves to the next matching record.
⏩	Moves 10 matching records forward.
⏭	Moves to the last matching record.
Record count	Displayed in view mode and indicates the number of the record out of the total number of records found by the most recent search operation. For example: 6 of 10. You can type in a number and hit the <Enter> key to jump to that record number.
Close	Closes the Assets folder.

Reports Form Procedures

Run an Asset Report

Note: This procedure does not apply to Alarm Monitoring.

1. In the listing window, select the type of report you want to run.
2. Select the **Limit report to current search** check box if you want to limit this report to the search that you just completed.
3. Click [Print]. The Print Report Options window will be displayed.



Print Report Options

Print Destination

● Print to a Preview Window

○ Export Directly to a File

○ Print Directly to a Printer:

☑ Prompt for Number of Pages

Report Subtitle

You can update the text used for the report subtitle below:

4. Choose a Print Destination and if you want, update the text used for the report subtitle.
5. Click [OK].
   - If you chose the **Print Directly to a Printer** radio button, select a printer from the drop-down list. If you select the **Prompt for Number of Pages** check box, the Print window will be displayed where you can select print range, number of copies and whether or not to collate your report.
   - If you chose the **Export Directly to a File** radio button, the Export window will be displayed. Choose the report Format and Destination from the drop-down lists. Depending on what you chose, enter the destination and format information in the corresponding window, then click [OK].
   - If you chose the **Print to a Preview Window** radio button, an asset report print preview window will be displayed from where you can view the selected report on the screen. For more information refer to the Report Print Preview Window chapter in the System Administration User Guide.

Chapter 5: Reports Folder

The Reports folder contains forms with which you can:

- View on the screen reports created using report layout templates in the database and current data
- Report on data that meets specified criteria (such as dates, times, readers, alarm panels, cardholders and badge IDs)
- Print a report, save it to a file or export the data

The folder contains eight forms: the Report Configuration form, the Reader Reports form, the Alarm Panel Reports form, the Anti-Passback Reports form, the Date/Time Reports form, the Event Reports form, the Receiver Account Zone Reports form, and the Alarm Acknowledgment Reports form.

Toolbar Shortcut

This folder is displayed by selecting **Reports** from the **Administration** menu or by selecting the Reports toolbar button.

Reports are installed when Database Setup is run. All reports are installed on the database server under the ReportTemplates subdirectory in the ReadykeyPRO installation path. By default, this location is **C:\Program Files\ReadykeyPRO\ReportTemplates**.

Note: Refer to the release notes for the versions of Seagate Crystal Reports that are supported. The release notes are located on the root of the ReadykeyPRO installation disc.

For more information, refer to Appendix B: Reports on page 267.

Overview of Visitor Management-Related Reports

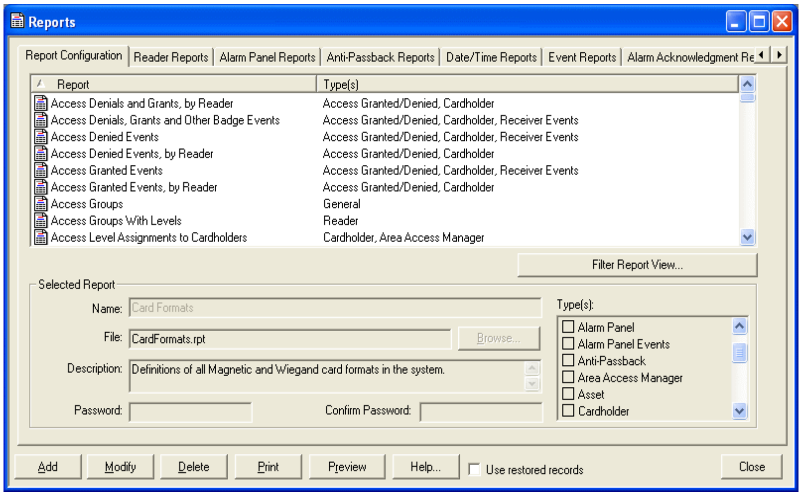
Reports features are available in System Administration, ID CredentialCenter, Digital Video and the standalone Visitor Management application. Reports for visit and visitor-related features function the same as reports for other ReadykeyPRO features and are available on the Report Configuration form. The types of reports, that include information about visits and visitors, that can be run are:

- Active Visits by Cardholder Name - lists all visits that are currently active (not signed out), grouped by cardholder name.
- Active Visits by Visitor Name - lists all visits that are currently active (not signed out), grouped by visitor name.
- Visitors - lists all visitors in the system. Note: This report might not run properly if you have deleted default visitor fields using FormsDesigner.
- Visit History - history of all visits in the system

Each of these reports can be configured so that a password must be supplied before the report can be generated. If a report has been password-protected, '*' characters will appear in the **Password** field on the Report Configuration form when the report is selected. If a report has not been password-protected, the **Password** field will be empty.

Permissions to view the Reports folder are set in System Administration or ID CredentialCenter. If a user does not have permissions for reports, then the **Reports** menu option will appear grayed out. Report permissions are reached by selecting **Users** from the **Administration** menu in System Administration, then clicking on the System Permission Groups tab. On the Software Options sub-tab of the System Permission Groups form, there are Add, Modify and Delete permissions for Reports.

Report Configuration Form



Report	Type(s)
Access Denials and Grants, by Reader	Access Granted/Denied, Cardholder
Access Denials, Grants and Other Badge Events	Access Granted/Denied, Cardholder, Receiver Events
Access Denied Events	Access Granted/Denied, Cardholder, Receiver Events
Access Denied Events, by Reader	Access Granted/Denied, Cardholder
Access Granted Events	Access Granted/Denied, Cardholder, Receiver Events
Access Granted Events, by Reader	Access Granted/Denied, Cardholder
Access Groups	General
Access Groups With Levels	Reader
Access Level Assignments to Cardholders	Cardholder, Area Access Manager

Selected Report

Name: Card Formats

File: CardFormats.rpt

Description: Definitions of all Magnetic and Wiegand card formats in the system.

Password:

Confirm Password:

Type(s):

- □ Alarm Panel
- □ Alarm Panel Events
- □ Anti-Passback
- □ Area Access Manager
- □ Asset
- □ Cardholder

Reports Folder - Report Configuration Form

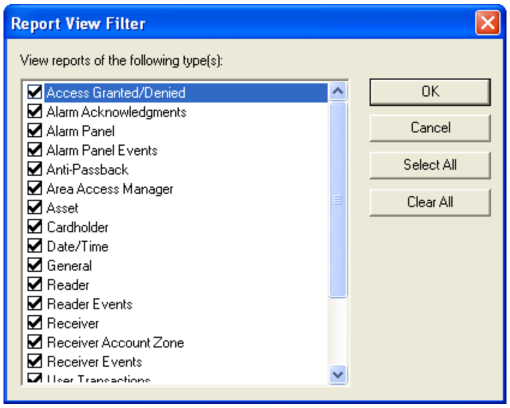
Form Element	Comment
Listing window	Lists currently defined reports of the type(s) selected in the Report View Filter window. Note that some reports are categorized under more than one type.
Filter Report View	Click this button to display the Report View Filter window from where you can choose the types of reports you wish to view.
Name	The name of the report.
File	The location and name of the file that contains the report.
Browse	Used to search through drives and directories to choose a report filename to insert into the **File** field.
Description	A brief description of the report contents.

Reports Folder - Report Configuration Form (Continued)

Form Element	Comment
Password	This field is optional. If you type a password here, a user attempting to print this report will be asked to first enter the correct password. A password can be from 1 to 32 characters in length. As you type, the password will appear in the field as a series of *s.
Confirm Password	If you typed something in the **Password** field, you must type exactly the same thing here. As with the **Password** field, your entry here will appear as a series of *s.
Type(s)	Lists the types of reports that you can configure. The system reports that are included with the installation are each assigned an appropriate Type. You can modify report types on the system reports but selecting invalid types could result in unwanted behavior. **Note:** To restore types back to their defaults, run Database Setup. **Note:** To make the report appear in Area Access Manager the Area Access Manager check box must be selected in the Types field.
Add	Used to configure a report.
Modify	Used to change a report configuration.
Delete	Used to remove a report.
Print	Opens the Print Report Options window.
Preview	Displays the selected report in the Report Print Preview window.
Help	Displays relevant on-screen help for this form.
Use restored records	If this check box is selected, data for an event or user transaction report is obtained from restored events/transactions in the database, rather than from the current “live” events/ transactions. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder.
Mode	In view mode, indicates the number of reports selected in the listing window and the total number of reports contained in all selected categories. For example: “1 of 42 selected.” In modify mode, indicates the current operation, such as “Modify Mode.”
Close	Closes the Reports folder.

Report View Filter Window

This window is displayed by clicking the [Filter Report View] button on the Report Configuration form.



View reports of the following type(s):

☑ Access Granted/Denied
☑ Alarm Acknowledgments
☑ Alarm Panel
☑ Alarm Panel Events
☑ Anti-Passback
☑ Area Access Manager
☑ Asset
☑ Cardholder
☑ Date/Time
☑ General
☑ Reader
☑ Reader Events
☑ Receiver
☑ Receiver Account Zone
☑ Receiver Events
☑ User Transactions

Reports Folder - Report View Filter Window

Form Element	Comment
Access Granted/ Denied	If this check box is selected, Access Granted and Access Denied reports will be included in the listing window. Reports of this type appear on the Reader Reports form for filtering.
Alarm Acknowledgments	If this check box is selected, Alarm Acknowledgment reports will be included in the listing window.
Alarm Panel	If this check box is selected, Alarm Panel reports will be included in the listing window. Reports of this type appear on the Alarm Panel Reports form for filtering.
Alarm Panel Events	If this check box is selected, Alarm Panel Events reports will be included in the listing window. Reports of this type appear on the Alarm Panel Reports form for filtering.
Anti-Passback	If this check box is selected, Anti-Passback reports will be included in the listing window. Reports of this type appear on the Anti-Passback Reports form for filtering.
Asset	If this check box is selected, Asset reports will be included in the listing window. Reports of this type appear on the Asset Reports form for filtering.
Cardholder	If this check box is selected, Cardholder reports will be included in the listing window. Reports of this type appear on the Reports form of the Cardholder folder for filtering.

Reports Folder - Report View Filter Window (Continued)

Form Element	Comment
Date/Time	If this check box is selected, Date/Time reports will be included in the listing window. Reports of this type appear on the Date/Time Report form for filtering.
General	If this check box is selected, general reports will be included in the listing window.
Reader	If this check box is selected, Reader reports will be included in the listing window. Reports of this type appear on the Reader Reports form for filtering.
Reader Events	If this check box is selected, Reader Events reports will be included in the listing window. Reports of this type appear on the Reader Reports form for filtering.
Receiver	If this check box is selected, the names of Receiver reports will be displayed in the listing window. Reports of this type appear on the Receiver Account Zone Reports form for filtering.
Receiver account Zone	If this check box is selected, the names of Account Zone reports will be displayed in the listing window. Reports of this type appear on the Receiver Account Zone Reports form for filtering.
Receiver Events	If this check box is selected, the names of Receiver Events reports will be displayed in the listing window. Reports of this type appear on the Receiver Account Zone Reports form for filtering.
User Transactions	If this check box is selected, User Transactions reports will be included in the listing window. Restored events/transactions are those restored using the [Restore Archive] button on the Restoring form of the Archives folder.
Video Events	If this check box is selected, Video events reports will be included in the listing window.
Visitor	If this check box is selected, Visitor reports will be included in the listing window.
OK	Click this button to save your changes and return to the Report Configuration form.
Cancel	Click this button to return to the Report Configuration form without saving your changes.
Select All	Click this button to select all check boxes in the window.
Clear All	Click this button to deselect all check boxes in the window.

Report Configuration Form Procedures

Add a Report

1. Select **Reports** from the **Administration** menu. The Reports folder opens.
2. Click [Add].
3. In the **Name** field, type a unique, descriptive name for the report.
4. Click [Browse]. The Open window opens.
5. Select the drive, then the directory, then the file name for an existing report layout.
6. Click [OK] to insert the selection into the **File** field on the Report Configuration form.

Note: You cannot use the Report Configuration form to design a report layout. Only existing layouts can be used to create reports. A valid report layout must have been designed using Crystal Reports for Windows™ and must have the file extension “rpt.”

7. In the **Description** field, type a description of this report's contents.
8. If you want to restrict previewing and printing of this report, type a password in the **Password** field.
9. Type the password again in the **Confirm Password** field.
10. In the **Type(s)** listing window, select the check boxes beside the most appropriate category for this report.

Note: You do not have to select a check box. Many of the reports currently in the system are uncategorized.

11. Click [OK] to add the report. The name of the report will be inserted alphabetically into the listing window.

Modify a Report

1. From the listing window, select the name of the report that you want to be changed. If the report is not listed, make sure that the appropriate check box is selected in the Report View Filter window (displayed by selecting the [Filter Report View] button).
2. Click [Modify].
3. Make the changes you want to the fields.
4. Click [OK] to save the changes, or [Cancel] to revert to the previously saved values.

Delete a Report

1. From the listing window, select the name of the report that you want to delete. If the report is not listed, make sure that the appropriate check box is selected in the Report View Filter window (displayed by selecting the [Filter Report View] button).
2. Click [Delete].
3. Click [OK].

Filter The Report View

1. On the Report Configuration form, click [Filter Report View]. The Report View Filter window opens.
2. Select the check boxes that correspond with the types of reports that you want to view. Click [Select All] to select all of the choices in the listing window. Click [Clear All] to deselect all of the choices in the listing window.
3. Click [OK]. The types of reports that correspond to the check boxes that you selected will be displayed in the listing window on the Report Configuration form.

Preview and Print a Report

For more information, refer to Preview and Print a Report on page 178.

Additional Reports Forms

The Reader Reports, Alarm Panel Reports, Anti-Passback Reports, Date/Time Reports, Event Reports, Receiver Account Zone Reports, and Alarm Acknowledgment Reports forms are displayed in standalone Visitor Management, but those reports must be run from System Administration or ID CredentialCenter. For more information refer to the Reports Folder chapter in the System Administration User Guide.

Chapter 7: Print Report Options Window

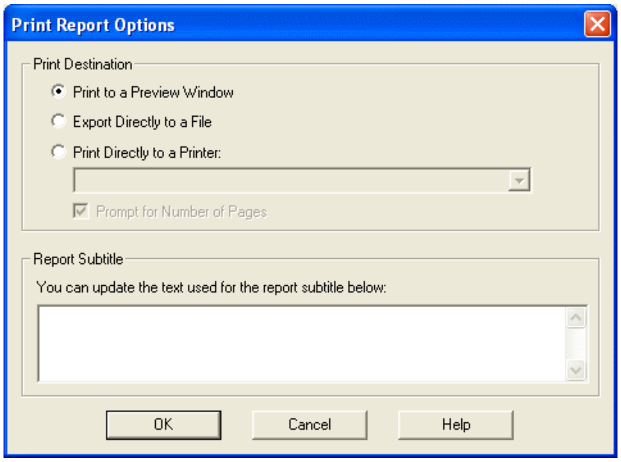
From the Print Report Options window, you can:

- Choose a destination for the report. Choices include:
  - Preview Window (the default)
  - Direct Export to a File
  - Directly to a Printer
- Update the subtitle used for the report

Toolbar Shortcut

This window is displayed by clicking the [Print] button or the Print toolbar button while a report is displayed.

Print Report Options Window



● Print to a Preview Window

○ Export Directly to a File

○ Print Directly to a Printer:

☑ Prompt for Number of Pages

You can update the text used for the report subtitle below:

Print Report Options Window Field Table

Print Report Options Window

Form Element	Comment
Print Destination	Includes the **Print to a Preview Window, Export Directly to a File** and **Print Directly to a Printer** radio buttons. Also includes the **Printer** drop-down list and the **Prompt for Number of Pages** check box.
Print to a Preview Window	If selected, the Report Print Preview window will be displayed when the [OK] button is clicked. In the Report Print Preview window, you can view the selected report on the screen. For more information, refer to Chapter 6: Report Print Preview Window on page 175.
Export Directly to a File	If selected, the Export window will be displayed when the [OK] button is clicked. Choose the report Format and Destination from the drop-down lists. Depending on what you choose, enter the destination and format information in the corresponding window, then click [OK].
Print Directly to a Printer	If selected, also select a printer from the Printer drop-down list. If you select the **Prompt for Number of Pages** check box, the Print window will be displayed where you can select the print range, number of copies and whether or not to collate your report.
Printer drop-down list	Select a printer in this field for the report to be printed on. This field is enabled for selection only when the **Print Directly to a Printer** radio button is selected. All printers currently configured for use are listed.
Prompt for Number of Pages	This field is enabled for selection only when the **Print Directly to a Printer** radio button is selected. If selected, the Print window will be displayed where you can select the print range, number of copies and whether or not to collate your report.
Report Subtitle	Includes the **Report Subtitle** textbox.
Report Subtitle textbox	Type the text here that will be displayed as the subtitle on the report.
OK	Prints the report using the options you selected.
Cancel	Closes the Print Report Options window without printing the report.
Help	Displays online help for this form.

Print a Report

1. Select a report from within the Reports folder. Reports are also available in the Cardholders folder (Reports form) and the Assets folder (Reports form). You can use this procedure to print those reports as well.

Notes: The report form is available from within the Reports folder, Cardholders folder and Assets folder for System Administration and ID CredentialCenter.

The report form is only available from the Cardholders folder in Alarm Monitoring. (**View** menu > **Badge Info** > Reports form/tab).

The availability of the Reports folder is subject to licensing restrictions.

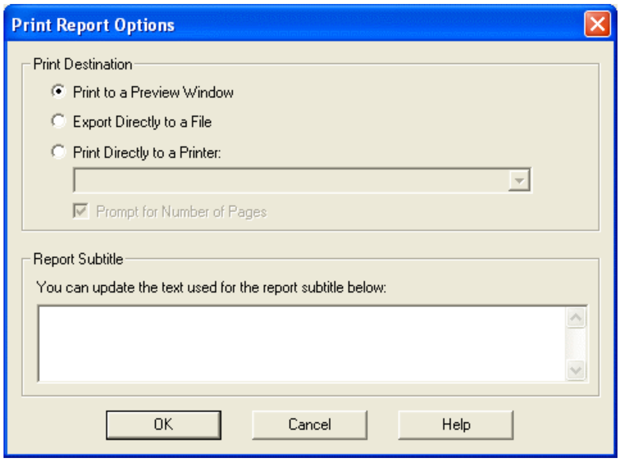
2. Select additional criteria if you want the report to include only a specific range of data.
3. Click one of the following:

Toolbar Shortcut

Print

- The Print button on the Main toolbar
- [Print] button on the form

4. The Print Report Options window opens.



Print Report Options

Print Destination

● Print to a Preview Window

○ Export Directly to a File

○ Print Directly to a Printer:

☑ Prompt for Number of Pages

Report Subtitle

You can update the text used for the report subtitle below:

OK Cancel Help

5. In the **Print Destination** section, select whether to print to a preview window, export directly to a file or print directly to a printer.
6. If you selected **Print Directly to a Printer** in the Print Destination section, select a printer in the drop-down list and choose whether to **Prompt for Number of Pages**.

Note: If the Linkage Server is running under a local system account it may not have permission to access a network printer (depending on its configuration). If this is the case you must select a local or default network printer. Contact your System Administrator to determine what account the Linkage Server is running under and the printers it can access.

7. In the Report Subtitle section, type the report subtitle. The subtitle will be displayed below the report title on the report.
8. Click [OK]. The options selected in the Print Destination section will determine where the report is sent.

Chapter 6: Report Print Preview Window

Toolbar Shortcut

If you click [Preview] or [Print Preview] while a report form is displayed, the report is automatically printed to the Report Print Preview window.

Previewing a report is done in a window. This allows you to preview multiple reports at the same time. It also means that while the report is processing, you can do other work. From the Report Print Preview window, you can:

- View an on-screen report created in the Reports folder.
- View an on-screen report created in the Cardholders folder (Reports form), The Visits folder (Reports form) or the Assets folder (Reports form) via the Print Report Options window.
- Print a report, save it to a file or send it over electronic mail.
- Search for any textual information in the report.

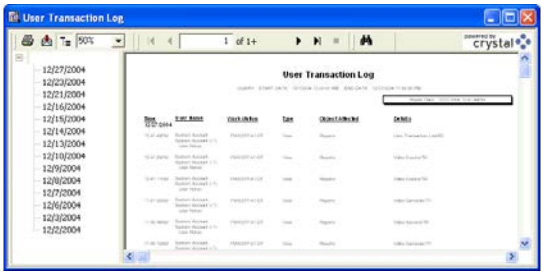
This window is displayed by:

- Clicking on the [Print Preview] button on any form in the Reports folder.
- Clicking on the Print Preview toolbar button when a report is selected on a form in the Reports folder.

Toolbar Shortcut

- Clicking [Print] on the form, selecting the **Print to a Preview Window** radio button on the Print Report Options window, then clicking the [OK] button. (This is how the Report Print Preview form can be viewed from the Reports form in the Cardholders folder, the Visits folder or the Assets folder.)

Report Print Preview Window



Report Print Preview Window Field Table

Report Print Preview Window

Form Element	Comment
Report navigation tree	The display in the left portion of the Report Print Preview window. The report navigation tree lists the records contained in the report, in a hierarchical arrangement. The information is content-sensitive. The report type determines the entries in the tree. For example, the default “User Transaction Log” report is arranged in date order, so the tree will contain a list of dates. The tree for the default “Text Instructions” report lists alarms. The “Access and Denials, by Reader” report has an entry for each queried reader, with subentries by event date. If the tree has branching entries, you can expand the branches of the tree. When you click an entry in the tree, you move to that section or record in the report. When a section or record is selected via the report navigation tree, that section or record will appear in the preview window with a blue box border. For more information, refer to Preview and Print a Report on page 178.
Preview window	The display in the right portion of the Report Print Preview window. The preview window displays up to one full page of the report, depending upon the zoom level set. If a report appears too large for the current window, either adjust the zoom level or use the up, down, left, and right arrow keys to scroll and see the rest of that page of the report. For reports that contain more than one page, use the arrows or the <Page Up>/<Page Down> keys to navigate through the pages.
🖨	Click to displays a Print window from where you can select the page range and number of copies to print, then initiate report printing.
✉	Click to export the report to a file or to your organization’s electronic mail system.
☰	Click to toggle the display of the report navigation tree on or off.
Zoom	From this drop-down list, you can select the magnification level of the preview window contents, with respect to the actual size. Choices include 400%, 300%, 200%, 150%, 100%, 75%, 50%, 25%, Page Width and Whole Page. Selecting either Page Width or Whole Page displays the corresponding percentage in this field. You can also type a number directly into this field, but you must then either press <Tab> or click outside of the field for the number to take effect.
⏮	Click to move to the first page of the report.
◀	Click to move to the previous page of the report. Another way to do this is to click the <Page Up> key.
Page count	This display indicates the page number of the currently displayed page, followed by the total page count for the report. For example: “2 of 4.”
▶	Click to move to the next page of the report. Another way to do this is to click the <Page Down> key.

Report Print Preview Window (Continued)

Form Element	Comment
▶|	Click to move to the last page of the report.
■	Click to terminate the report building process. This button is especially useful if the report is lengthy and you want to view only part of it.
🔍	Click to display the Search window from where you can perform a text search of the report. When you enter text in the **Find what** field (in the Search window) and click [Find Next], the view jumps to the first occurrence of the requested text or a message is displayed if no match was found.

Report Print Preview Window Right-click Options

While viewing a report in the Report Print Preview Window there are a number of right-click options and identifiers that appear depending on what section of the report is highlighted.

- **Field:** Tells you what field is currently selected.
- **Text:** Tells you whether the current selection is text.
- **Copy:** Copy the information into the clipboard.
- **Freeze Pane:** Freezes the section of the pane so you continue to see the information as you scroll.
- **Unfreeze Pane:** Unfreezes the pane so the page scrolls normally

Report Print Preview Window Procedures

Preview and Print a Report

1. Select a report from within the Reports folder.

Note: Reports are also available on the Reports form in the Cardholders folder, Visits folder and Assets folder. However, the Print Preview toolbar button and the [Preview] button on the form are disabled or “grayed out.” Instead, the Print toolbar button or the [Print] button on the form are used to preview and print reports from these forms. For more information, refer to Print a Report on page 183.

2. Select additional criteria if you want the report to include only a specific range of data.
3. Click one of the following:

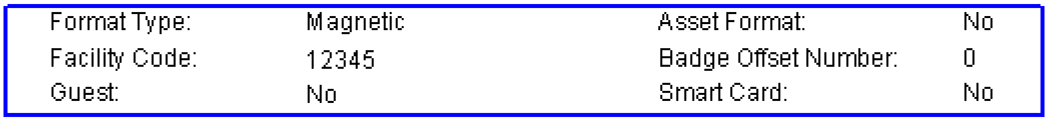
Toolbar Shortcut

Print Preview

- The Print Preview button on the **Main** toolbar.
- The [Print] button, select the **Print to a Preview Window** radio button and then click [OK].
- The [Preview] button on the form.

4. If the chosen report has been password-protected, type the correct password when prompted to do so, then click [OK].

5. The Report Print Preview window is displayed.
   - On the left, the report navigation tree may have branching entries.
     - If the tree has branching entries, expand that branch of the tree.
     - Click an entry in the tree to move to that section or record in the report. When a section or record is selected via the report navigation tree, that section or record will appear in the preview window with a blue box border. For example:



Format Type:	Magnetic	Asset Format:	No
Facility Code:	12345	Badge Offset Number:	0
Guest:	No	Smart Card:	No

   - On the right, the preview window will show the first page of the report as it will look when it is printed. Click a section or record in the preview window. When a section or record is selected in the preview window, that section or record will appear in the preview window with a blue box border.
   - Click and drag the split bar to resize the report navigation tree and the preview window relative to each other.
   - Click the ☰ button to hide the report navigation tree and maximize the space used for the preview window.

6. Use the ⏮, ◀, ▶ and ⏭ buttons or the <Page Down>/<Page Up> keys to view other pages of the report.

7. Select an option from the zoom drop-down list to change the size of the display. You can instead type a number directly into this field, but you must then either press <Tab> or click outside of the field for the number to take

effect. If a report page is still too large for the window, you can use the up, down, left, and right arrow keys to scroll and see the rest of the page.

8. To save the report to a file on your computer or to send the report to someone using your company's electronic mail system, select the ✉ button. The Export window is displayed.
   - Select the format that you want to send the report in from the **Format** drop-down list.
   - In the **Destination** drop-down list, you can choose to export the report to an application, a disk file, an exchange folder, a Lotus Notes database or your electronic mail system (if you have one).
   - Click [OK] and follow the instructions
9. To print the report from within the Report Print Preview window:

   a. Click the 🖨 button. The Print window is displayed from where you can select which pages to print and the number of copies.

   b. Select one of the following:
      - The **All** radio button to print the entire report without user intervention.
      - The **Pages** radio button and enter a page range.

   c. A message box will be displayed to indicate the status of the print operation.

Search a Report for Specific Information

1. To search through the report for specific information, click the 🔍 button.
2. The Search window is displayed. In the **Find what** field, type the word, contiguous words or number you wish to locate in the report.

Note: The search is not case-sensitive.

3. Click [Find Next].
4. One of two things will happen:
   - If the requested information was found, the preview window display will move to the first occurrence of it.
   - If the information is not contained in the report, a message box will be displayed.
5. If the requested information was found, click [Find Next] to move through successive occurrences of it.

Chapter 19: Guard Tour

Guard tour provides a guard (a cardholder who has been specifically chosen to conduct a tour) with a defined set of tasks that must be performed within a specified period of time. Typical tasks include swiping a card at a checkpoint access reader or turning a key connected to an alarm panel input. (Checkpoints are designated stops along a tour.)

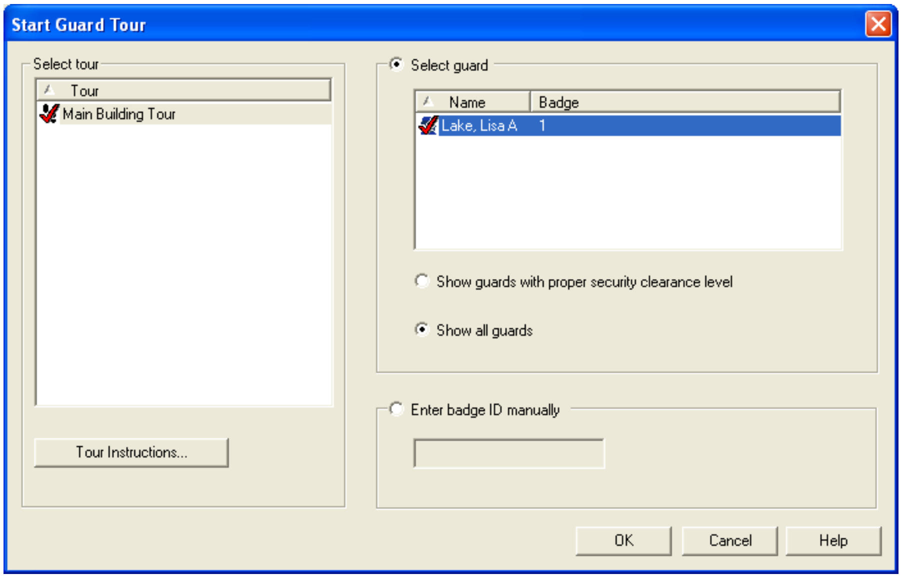
Guard tour records the location and timestamp for each checkpoint visited by the tour guard. The *Checkpoint Time* represents the time it should take to reach a particular checkpoint. All checkpoints have minimum and maximum checkpoint times. A guard tour event is generated if a checkpoint is missed, reached early, on time, late, out of sequence or overdue. A late event means the checkpoint was reached after its maximum time expired. An overdue event means the checkpoint has not yet been reached.

A tour is considered complete when one of the following actions occurs:

- All of the checkpoints on the tour are reached, even if they are reached out of sequence or some checkpoints are missed
- The tour is acknowledged as complete at a monitoring station
- The tour is terminated at a monitoring station

Note: System Administrator procedures to set up a Guard Tour are located in the Guard Tour Folder chapter in the System Administration User Guide.

Start Guard Tour Form



Start Guard Tour

Select tour

Tour
✓ Main Building Tour

● Select guard

Name	Badge
✓ Lake, Lisa A	1

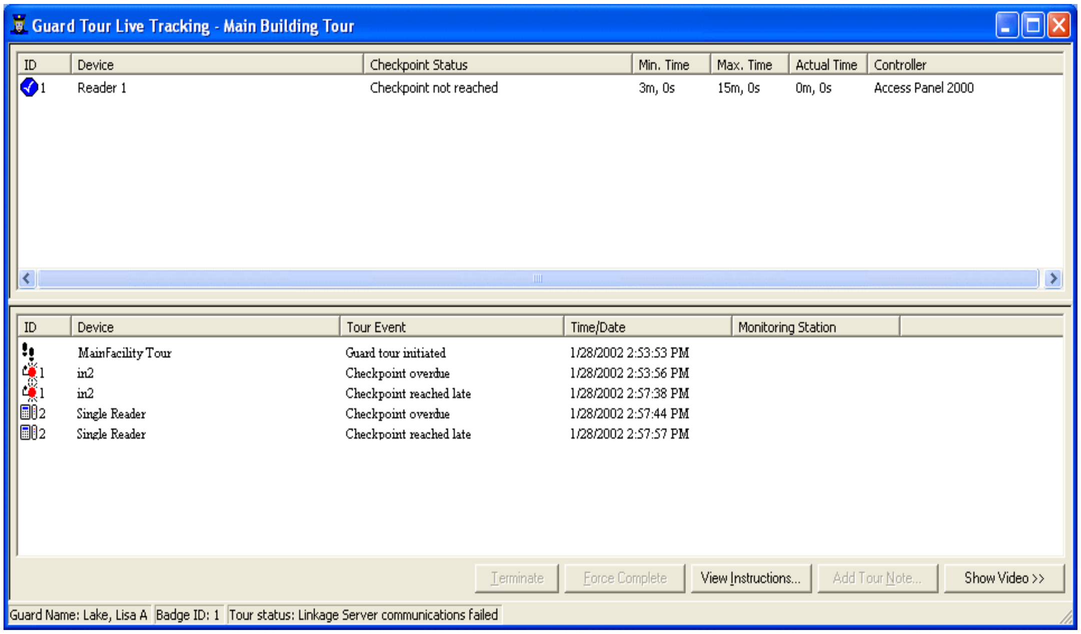
○ Show guards with proper security clearance level

● Show all guards

○ Enter badge ID manually

Button	Function
Select Tour listing window	Displays a list of configured Guard Tours. Click a tour to select it. A checkmark displays beside a tour when it is selected.
Select Guard	Displays a list of guards. Select a guard to perform the Guard Tour. The list of Guards can be filtered by selecting the show guards with proper security clearance level radio button.
Show guards with proper security clearance level	Limits the guards displayed in the Select guard listing to the guards with authorization to perform the selected guard tour.
Show all guards	Displays all the guards in the Select guard listing.
Enter badge ID Manually	Provides you the option to enter the badge ID of the guard instead of selecting a guard from the Select guard list.
Tour Instructions	Displays the Tour Instructions window which contains specific instructions for the selected tour. From the Tour Instructions window you can print the instructions.

Guard Tour Live Tracking Form



Guard Tour Live Tracking - Main Building Tour

ID	Device	Checkpoint Status	Min. Time	Max. Time	Actual Time	Controller
1	Reader 1	Checkpoint not reached	3m, 0s	15m, 0s	0m, 0s	Access Panel 2000

ID	Device	Tour Event	Time/Date	Monitoring Station
	MainFacility Tour	Guard tour initiated	1/28/2002 2:53:53 PM	
1	in2	Checkpoint overdue	1/28/2002 2:53:56 PM	
1	in2	Checkpoint reached late	1/28/2002 2:57:38 PM	
2	Single Reader	Checkpoint overdue	1/28/2002 2:57:44 PM	
2	Single Reader	Checkpoint reached late	1/28/2002 2:57:57 PM	

Guard Name: Lake, Lisa A | Badge ID: 1 | Tour status: Linkage Server communications failed

Button	Function
Terminate	Stops a tour before it is completed (before all of the checkpoints have been reached). When this button is selected, a “Guard Tour Terminated” event is generated.
Force Complete	Manually completes a tour. For example, the [Force Complete] button could be used to end a tour that otherwise could not be completed because of a card that could not be swiped at a reader (a checkpoint) that was in “unlocked” mode.
View Instructions	Displays special instructions that were written for this tour when it was configured in the System Administration application.
Add Tour Note	Adds a note to an event. For example, you can add a note explaining why a particular checkpoint was reached late.
Show Video	Displays live video of the tour as it progresses. (This button is displayed only when the tour is configured to show video.

Guard Tour Events Table

Event	Description
Guard Tour Initiated	Generated when a tour is launched from a monitoring station.
Guard Tour Completed	Generated when all checkpoints on a tour have a “Checkpoint Reached on Time” status. Otherwise, a “Guard Tour Completed with Errors” event is generated.

Guard Tour Events Table

Event	Description
Guard Tour Completed with Errors	Generated when the last checkpoint has been reached but one or more checkpoints were not reached on time or were missed altogether.
Guard Tour Cancelled	Generated when the scheduled automatic guard tour is cancelled before the tour was started.
Guard Tour Terminated	Generated when the [Terminate] button is selected in the Guard Tour Live Tracking window.
Checkpoint reached out of Sequence	Generated when a checkpoint is hit ahead of schedule on a tour (i.e., it is supposed to be hit later in a tour).
Checkpoint Missed	When a checkpoint is assigned a status of "Checkpoint reached out of sequence", the "Checkpoint Missed" event is generated for all previous checkpoints that have a status of "Checkpoint Not Reached."
Checkpoint Reached on Time	Generated when a checkpoint is hit between its minimum and maximum checkpoint times. **Note:** Checkpoint reached events are generated when any inputs that are used as checkpoints are activated.
Checkpoint Reached Early	Generated when a checkpoint is the next checkpoint on a tour and is hit before its minimum checkpoint time has elapsed. **Note:** Checkpoint reached events are generated when any inputs that are used as checkpoints are activated.
Checkpoint Overdue	Generated when a checkpoint's maximum checkpoint time has elapsed and the guard has not yet arrived.
Checkpoint Reached Late	Generated for a checkpoint when its maximum checkpoint time has elapsed and it is then hit. **Note:** Checkpoint reached events are generated when any inputs that are used as checkpoints are activated.

Guard Tour Form Procedures

The following procedures in this section are:

- Launch a Guard Tour
- Schedule an Automatic Guard Tour Action
- Respond to an Automatic Guard Tour
- View a Guard Tour

Launch a Guard Tour

1. Start the Linkage Server by clicking the Start button, then selecting **Programs** > **ReadykeyPRO Unlimited** > **Linkage Server**.

2. Open the Select Guard Tour window by completing one of the following:
   - From the **Control** menu, select **Guard Tour > Launch**.

Toolbar Shortcut

   - Click the down arrow on the Guard Tour toolbar button and select **Launch Tour**.
   - Right-click a tour name in the system status tree and select **Launch Tour**.
3. Select a tour in the **Tour** listing window.

Note: You can click [Tour Instructions] to see if any special instructions exist for this tour. These instructions are written when the tour is configured in System Administration.

4. If you know the badge ID of the tour guard, select the **Enter badge ID manually** radio button and type in their ID.
   Otherwise select the **Select guard** radio button and complete the following:
   a. Select the **Show guards with proper security clearance level** radio button to limit the number of tour guards to choose from or select the **Show all guards** radio button to list all tour guards, regardless of their security clearance levels.
   b. Click a tour guard entry in the Name listing window to select it.
5. Click [OK]. The Guard Tour Live Tracking window opens.
6. At this time, the tour guard can begin the tour. As the tour progresses, the status of checkpoints and generated events display in the Guard Tour Live Tracking window. For more information, refer to Guard Tour Events Table on page 311.

Note: Checkpoints can be predecessors or successors. A predecessor checkpoint is any checkpoint occurring *before* other checkpoints on a tour. For example: a tour has three stops. Checkpoints one and two are the predecessors to checkpoint three. A successor checkpoint is any checkpoint occurring *after* other checkpoints on a tour. For example: a tour has three stops. Checkpoints two and three are successors to checkpoint one.

7. When a tour is completed, the Guard Tour Live Tracking window displays the status of the tour and the events that were generated.

Schedule an Automatic Guard Tour Action

Assuming your System Administrator has configured a Guard Tour (in System Administration) you can schedule an automatic guard tour action (in Alarm Monitoring). This means that using the Scheduler you can set ReadykeyPRO to automatically launch a Guard Tour on at a specific date and time as well as on a regular basis.

1. Open the Scheduler by clicking the Scheduler toolbar button or selecting **Scheduler** from **View** menu.
2. Click [Add].
3. The Add Action Wizard window displays. In the Category pane select **Action Types**. In the Objects pane select **Automatic Guard Tour**.
4. Click [Next].
5. The Automatic Guard Tour Properties window displays. Select a tour or tour group.
6. Select the Monitoring stations to be notified.
7. Click the Schedule tab.
8. Select the World time zone.
9. If the automatic Guard Tour is a single occurrence select the **One time** radio button and set the start date and time.
10. If the automatic Guard Tour will occur several times click the **Recurring** radio button and click [Change].
    a. Set how often you want the Guard Tour to occur and the start and end dates.
    b. Click [OK].
    c. The frequency settings display in the in the Recurring pane on the schedule tab.
11. Click [OK].

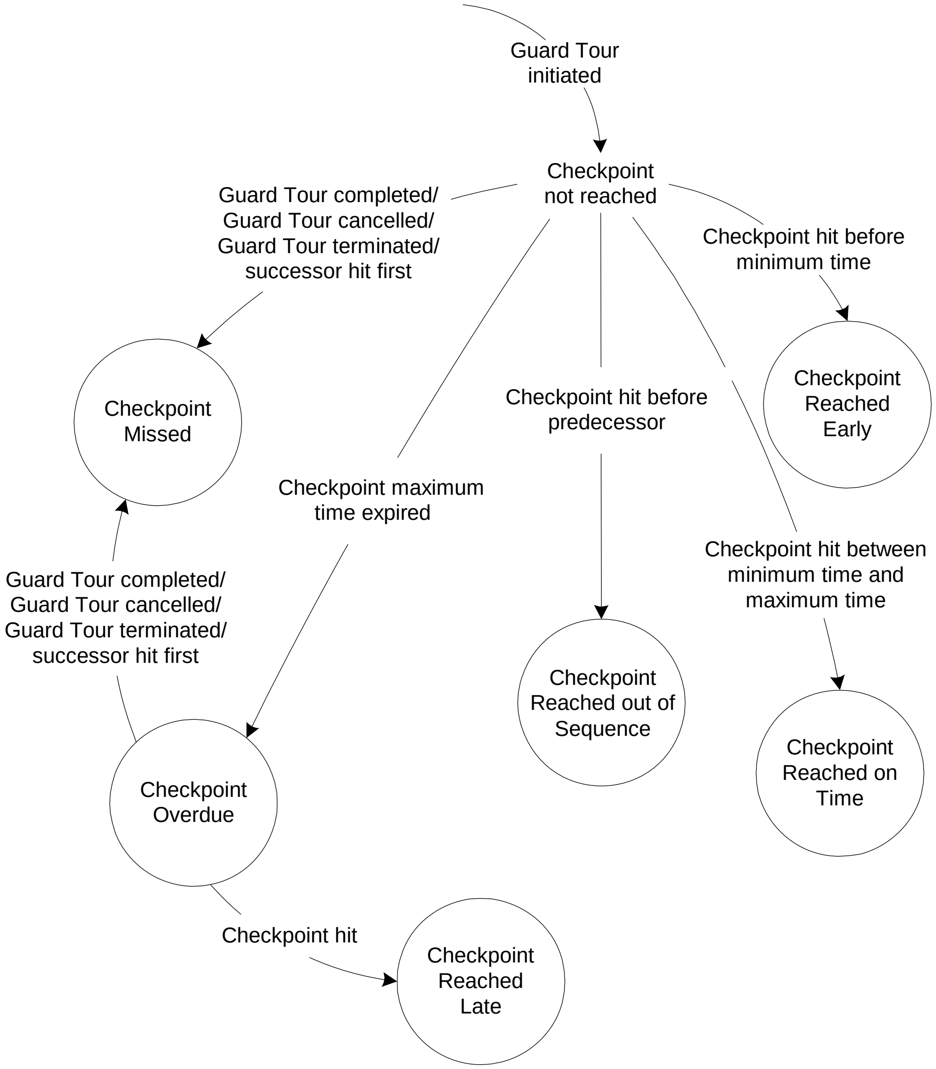
Respond to an Automatic Guard Tour

1. When an automatic Guard Tour is started, Alarm Monitoring displays a *Scheduler Action Executed* alarm and you prompts you to start the Guard Tour.
2. Click [OK].
3. The Start Guard Tour window displays with the guard tour name selected. Select the guard (person) to complete the tour by either selecting the guard from the list provided or entering the guard’s badge ID.
4. Click [OK].
5. While the Guard Tour is active you can monitor the Guard Tour status by selecting **Control** > **Guard Tour** > **View** from the main menu.
6. The Guard Tour Live Tracking window display information such as the badge ID of the person performing the Guard Tour, the checkpoint statuses, tour history as well as the ability to view instructions and video.

View a Guard Tour

1. Start the Linkage Server by clicking the Start button, then selecting **Programs** > **ReadykeyPRO Unlimited** > **Linkage Server**.
2. Open the Select Guard Tour window by completing one of the following:
   - From the **Control** menu, select **Guard Tour > Launch**.
   - Click the down arrow on the Guard Tour toolbar button and select **Launch Tour**.
3. The View Guard Tour window opens. Select the tour and click [OK].

Checkpoint Status and Events Diagram


Guard Tour initiated
Checkpoint not reached
Guard Tour completed/ Guard Tour cancelled/ Guard Tour terminated/ successor hit first
Checkpoint hit before minimum time
Checkpoint Missed
Checkpoint hit before predecessor
Checkpoint Reached Early
Checkpoint maximum time expired
Checkpoint hit between minimum time and maximum time
Guard Tour completed/ Guard Tour cancelled/ Guard Tour terminated/ successor hit first
Checkpoint Reached out of Sequence
Checkpoint Reached on Time
Checkpoint Overdue
Checkpoint hit
Checkpoint Reached Late

Chapter 20: Scheduler Folder

The Scheduler folder contains the Scheduler form with which you can schedule actions.

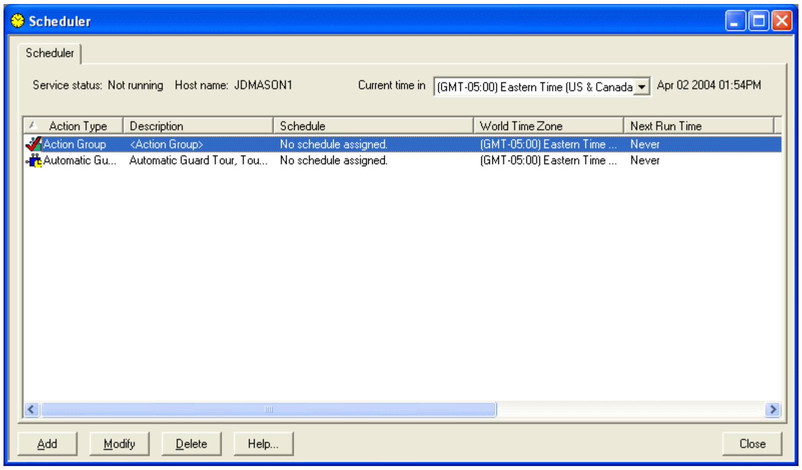
Note: Additional documentation on actions is available in the Actions appendix. For more information, refer to Appendix A: Actions on page 331.

Toolbar Shortcut

This folder is displayed by selecting **Scheduler** from the **View** menu.

Important: For the Scheduler to run and execute action the Linkage Server needs to be configured and running. You can configure the Linkage Server host on the General System Options Form in System Administration.

Scheduler Form



Service status: Not running Host name: JDMASON1 Current time in (GMT-05:00) Eastern Time (US & Canada Apr 02 2004 01:54PM

Action Type	Description	Schedule	World Time Zone	Next Run Time
Action Group	<Action Group>	No schedule assigned.	(GMT-05:00) Eastern Time ...	Never
Automatic Gu...	Automatic Guard Tour, Tou...	No schedule assigned.	(GMT-05:00) Eastern Time ...	Never

Scheduler Folder - Scheduler Form

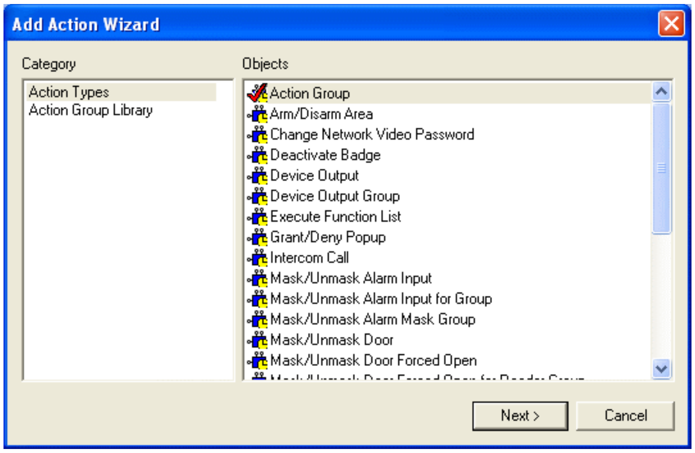
Form Element	Comment
Service status	Lists the status of the LS Linkage Server host and whether it's running or not. This is displayed only when the LS Linkage Server host is configured.
Host name	Lists the name of the host computer. This is displayed only when the Linkage Server host is configured.
Current time in	When scheduling an action, select which time zone you want the action to be scheduled in. The selections in the drop-down list are listed sequentially and each includes: • The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected world time zone is 5 hours ahead of the clock time in Greenwich, England. • The name of one or more countries or cities that are located in that world time zone.
Listing window	Displays a list of all scheduled actions.
Add	Click this button to open the **Add Action Wizard**.
Modify	Click this button to modify the selected scheduled action.
Delete	Click this button to delete the selected scheduled action.
Help	Click this button to display online assistance for this form.
Close	Click this button to close the Scheduler folder.

Scheduler Form Procedures

Add and Schedule an Action

1. Select **Scheduler** from the **View** menu. The Scheduler folder opens.
2. Click [Add]. The **Add Action Wizard** opens.

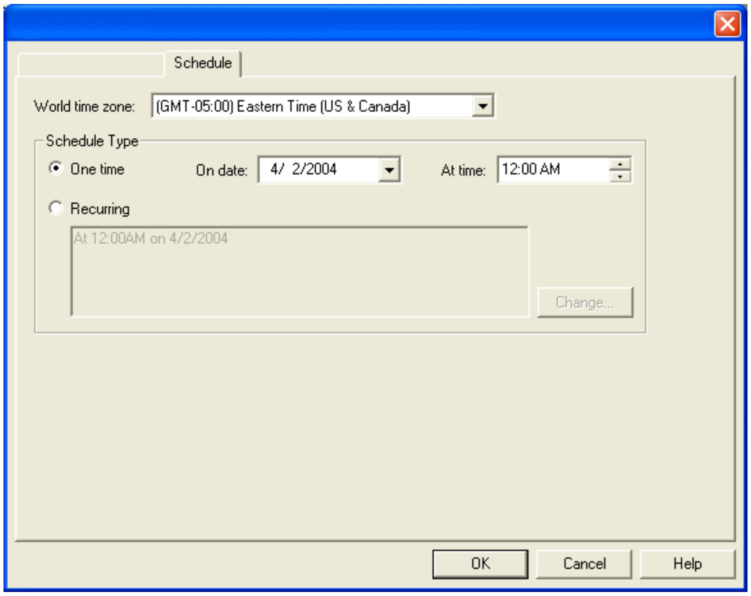
Note: You can also display the **Add Action Wizard** by right-clicking anywhere on the Scheduler form and selecting the **Add Action** menu option.



3. Select either “Action Types” or “Action Group Library” from the **Category** listing window.
   - When “Action Types” is selected, the **Objects** listing window lists all available action types.
   - When “Action Group Library” is selected, the **Objects** listing window lists all action groups which have been either created in or saved to the

action group library. For more information refer to the Action Group Library Folder chapter in the System Administration User Guide.

4. Click on an entry in the **Objects** listing window to select it.
5. Click [Next]. Depending on which Category/Object combination you chose in steps 3 and 4, a corresponding action properties window will open.
   For example, if you selected "Action Types" in the **Category** listing window and "Archive/Purge Database" in the **Objects** listing window, then the **Archive/Purge Database Properties** window would open.
6. Click the Schedule tab. The Schedule form is displayed.
   The Schedule form is the same in every action properties window that is accessed via the Scheduler folder.



Schedule

World time zone: (GMT-05:00) Eastern Time (US & Canada)

Schedule Type

● One time   On date: 4/ 2/2004   At time: 12:00 AM

○ Recurring

At 12:00AM on 4/2/2004

7. From the **World time zone** drop-down list, select which time zone you want the action to be scheduled in. The selections in the drop-down list are listed sequentially and each includes:
   - The world time zone's clock time relative to Greenwich Mean Time. For example, (GMT+05:00) indicates that the clock time in the selected

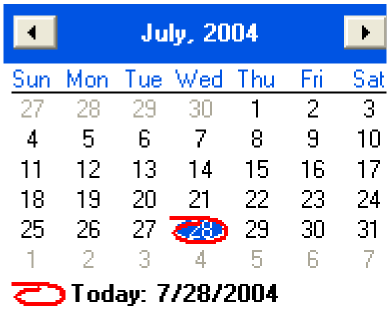
world time zone is 5 hours ahead of the clock time in Greenwich, England.

- The name of one or more countries or cities that are located in that world time zone.

8. If you want to schedule the action to occur more than once, skip this step and proceed to step 9. If you want to schedule the action to occur once:

   a. Select the **One time** radio button.

   b. In the **On date** field, the current date is entered by default, but you can change this value by typing a numeric date into the field or by selecting a date from the drop-down calendar.



◄ July, 2004 ►

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Today: 7/28/2004

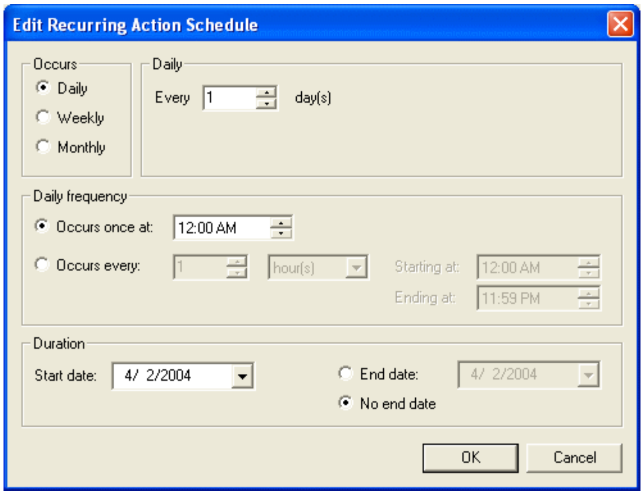
- To select a month, click on the ◄ and ► navigation buttons.
- You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.
- Navigate to a year by clicking on the displayed year to access the year spin buttons 2003 ⬍.
- Once you have selected a month and a year, click on the day that you want the action to occur.

   c. In the **At time** field, select the time when you want this action to occur. Proceed to step 10.

9. If you want to schedule the action to occur more than once:

   a. Select the **Recurring** radio button.

   b. Click [Change]. The **Edit Recurring Action Schedule** window opens.


Edit Recurring Action Schedule

Occurs
● Daily
○ Weekly
○ Monthly

Daily
Every 1 day(s)

Daily frequency
● Occurs once at: 12:00 AM
○ Occurs every: 1 hour(s) Starting at: 12:00 AM
Ending at: 11:59 PM

Duration
Start date: 4/ 2/2004
○ End date: 4/ 2/2004
● No end date

c. Do one of the following:

- Select the **Daily** radio button in the Occurs section if you want the action to occur on a daily basis.

  If you want the action to occur every day, in the Daily section, type the number 1 in the **Every___day(s)** field. If you want the action to occur every other day, type the number 2 and so on.

- Select the **Weekly** radio button in the Occurs section if you want the action to occur on a weekly basis.

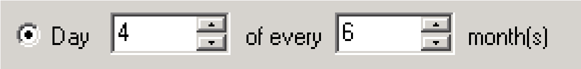
  If you want the action to occur every week, in the Weekly section, type the number 1 in the **Every___week(s) on** field. If you want the action to occur every other week, type the number 2 and so on. You must also select the check box that corresponds with the day of the week that you want the action to occur.

  For example, if you want the action to occur every other Monday, type the number 2 in the **Every___week(s) on** field and select the **Mon** check box.

- Select the **Monthly** radio button in the Occurs section if you want the action to occur on a monthly basis. Then, do one of the following:

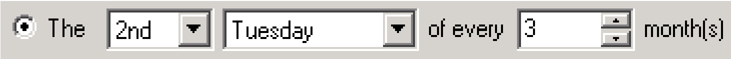
  Select the **Day___of every___month(s)** radio button and type in which day of how many months you want the action to occur.

  The following example shows an action being scheduled to occur on the 4th day of every 6th month.


● Day 4 of every 6 month(s)

  Select the **The___of every___month(s)** radio button and enter which day of how many months you want the action to occur.

The following example shows an action being scheduled to occur of the 2nd Tuesday of every 3rd month.

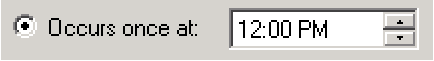


● The 2nd ▼ Tuesday ▼ of every 3 month(s)

d. In the Daily frequency section, do one of the following:

- If you want the action to occur only once on its scheduled day(s), select the **Occurs once at___** radio button and enter a time.

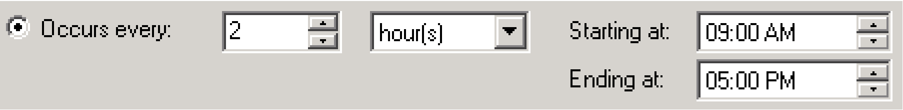
  The following example shows an action being scheduled to occur at 12:00 PM.



● Occurs once at: 12:00 PM

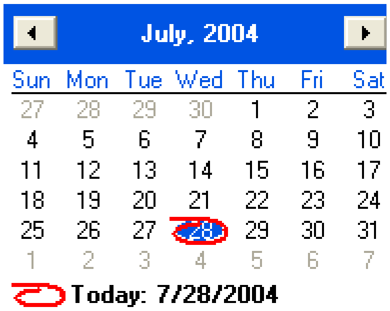
- If you want the action to occur more than once on its scheduled day(s), select the **Occurs every___Starting at___Ending at___** radio button and enter the hours that you want the action to occur.

The following example shows an action being scheduled to occur every 2 hours, starting at 9:00 AM and ending at 5:00 PM.



● Occurs every: 2 hour(s) Starting at: 09:00 AM
Ending at: 05:00 PM

e. Enter the action’s **Start date**. The current date is entered by default, but you can change this value by typing a numeric date into the field or by selecting a date from the drop-down calendar.



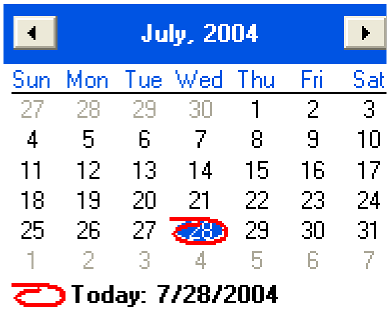
◀ July, 2004 ▶

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Today: 7/28/2004

- To select a month, click on the ◀ and ▶ navigation buttons.
- You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.
- Navigate to a year by clicking on the displayed year to access the year spin buttons 2003 ⬍.
- Once you have selected a month and a year, click on the day that you want the action to begin occurring.

f. Enter the action’s **End date**. The current date is entered by default, but you can change this value by typing a numeric date into the field or by selecting a date from the drop-down calendar.



◀ July, 2004 ▶

Sun	Mon	Tue	Wed	Thu	Fri	Sat
27	28	29	30	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31
1	2	3	4	5	6	7

Today: 7/28/2004

- To select a month, click on the ◀ and ▶ navigation buttons.
- You can also select a month by clicking on the displayed month to access a drop-down list of months. Highlight the month you want to select it.

- Navigate to a year by clicking on the displayed year to access the year spin buttons 2003.
- Once you have selected a month and a year, click on the day that you want the action to stop occurring.

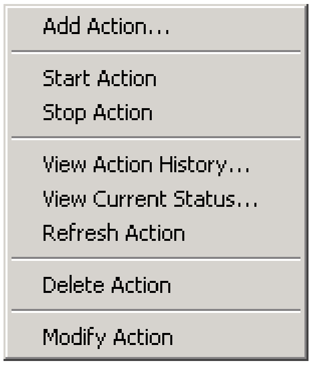
Note: You do not have to select an end date. If you do not want to set an end date, select the **No end date** radio button.

g. Click [OK].

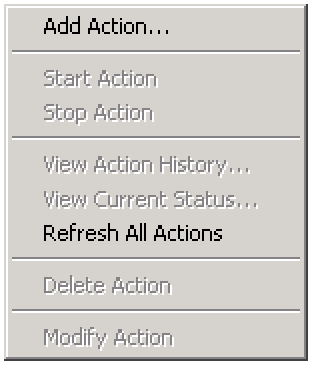
10. Now you must configure the action that you have just scheduled. Select the tab to the left of the Schedule tab (this tab will correspond to the specific action properties window which you are viewing). For more information, refer to Appendix A: Actions on page 331.

Display the Scheduler Right-Click Menu

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.



Note: If you right-click anywhere on the Scheduler form when a scheduled action is not selected in the listing window, the scheduler right-click menu will look like this:



Add and Schedule an Action Using the Scheduler Right-Click Menu

1. Right-click anywhere on the Scheduler form. The scheduler right-click menu is displayed.
2. Select the **Add Action** menu option. The **Add Action Wizard** opens.
3. Proceed to step 3 of the “Add and Schedule an Action” procedure in this chapter.

Start an Action

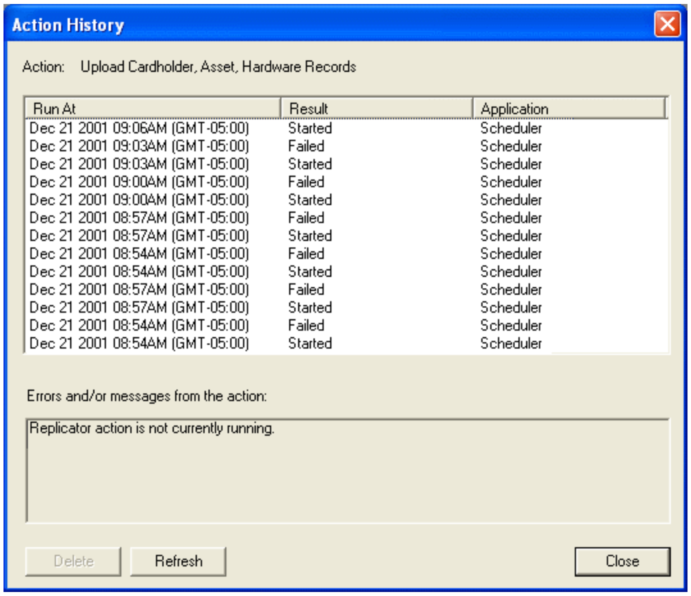
1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **Start Action** menu option to start the selected action immediately.

Stop an Action

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **Stop Action** menu option to stop the selected action immediately.

View Action History

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **View Action History** menu option. The Action History window opens and the name of the action, when the action was run, the result, the application and any errors or messages that resulted from the action are all displayed.



Action: Upload Cardholder, Asset, Hardware Records

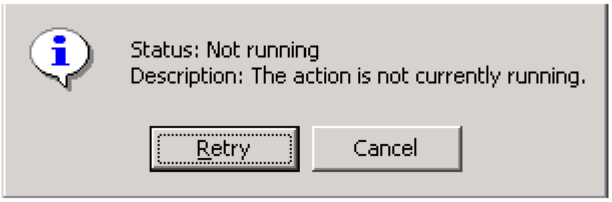
Run At	Result	Application
Dec 21 2001 09:06AM (GMT-05:00)	Started	Scheduler
Dec 21 2001 09:03AM (GMT-05:00)	Failed	Scheduler
Dec 21 2001 09:03AM (GMT-05:00)	Started	Scheduler
Dec 21 2001 09:00AM (GMT-05:00)	Failed	Scheduler
Dec 21 2001 09:00AM (GMT-05:00)	Started	Scheduler
Dec 21 2001 08:57AM (GMT-05:00)	Failed	Scheduler
Dec 21 2001 08:57AM (GMT-05:00)	Started	Scheduler
Dec 21 2001 08:54AM (GMT-05:00)	Failed	Scheduler
Dec 21 2001 08:54AM (GMT-05:00)	Started	Scheduler
Dec 21 2001 08:57AM (GMT-05:00)	Failed	Scheduler
Dec 21 2001 08:57AM (GMT-05:00)	Started	Scheduler
Dec 21 2001 08:54AM (GMT-05:00)	Failed	Scheduler
Dec 21 2001 08:54AM (GMT-05:00)	Started	Scheduler

Errors and/or messages from the action:

Replicator action is not currently running.

View the Current Status of an Action

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **View Current Status** menu option. A message similar to the following will be displayed:



Status: Not running
Description: The action is not currently running.

Refresh an Action

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **Refresh Action** menu option. The listing window will be updated to display the most current information for the selected action.

Refresh all Actions

1. Right-click anywhere on the Scheduler form except on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **Refresh All Actions** menu option. The listing window will be updated to display the most current information for all of the scheduled actions.

Delete a Scheduled Action using the Scheduler Right-Click Menu

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **Delete Action** menu option. A confirmation message is displayed.
3. Click [Yes].

Note: Selecting the **Delete Action** right-click menu option does the same thing as selecting an action in the listing window, and then clicking [Delete] on the Scheduler form.

Modify a Scheduled Action using the Scheduler Right-Click Menu

1. Right-click on a scheduled action in the listing window. The scheduler right-click menu is displayed.
2. Select the **Modify Action** menu option. Depending on which action you selected in the listing window, a corresponding action properties window will open.
3. Make the changes you want to the fields. For more information, refer to Appendix A: Actions on page 331.
4. Click [OK].

Note: Selecting the **Modify Action** right-click menu option does the same thing as selecting an action in the listing window, then clicking the [Modify] button on the Scheduler form.

Appendices

Appendix A: Actions

Actions can be added (configured) through the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O folders in System Administration. Actions can also be added through the Scheduler in Alarm Monitoring.

If you add an action through the Scheduler or Guard Tour folder, you can also schedule the action to execute routinely or once. To manually execute an action you can right-click a device in Alarm Monitoring > System Status window.

This appendix describes how to add (configure) an action to your ReadykeyPRO system.

Important: For the Scheduler to be able to execute actions the Linkage Server must be configured and running. You can configure the Linkage Server host on the General System Options form in the System Options folder in System Administration or ID CredentialCenter.

General Actions Procedures

Specify the Number of Simultaneous Actions

Important: Some operating systems require you to run the **ACS.INI** file as the administrator to modify it.

Occasional problems may occur when running a large number of actions at once. ReadykeyPRO defaults the limit of simultaneous actions to fifty but that can be changed in the **ACS.INI** file.

To change the ACS.INI file to override the default limit on simultaneous actions:

1. In the Windows start menu click run.
2. In the Run dialog box type “ACS.INI” without the quotes.
3. In the ACS.INI file find the [Service] section and add the line: “MaxNumberActionThreads=<Number of actions>” without the quotes and where the “Number of actions” equals the number of simultaneous actions you want to occur.

Open an Action Properties Window

Refer to the following procedures to open an action properties window through various folders in System Administration and Alarm Monitoring.

Using Action Group Library

Note: The Action Group Library folder can be used to group actions. To schedule a group of actions or configure a group of actions based on incoming events, guard tour related conditions, or acknowledged alarms, you can use the action type called “Action group” which is available using the Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O folders. For more information, refer to Add an Action Group on page 336.

1. In System Administration, select **Action Group Library** from the **Administration** menu.
2. Click [Add].
3. The Action Group Properties window displays.
4. Enter an action group name and click [Add].
5. The Select Action Type window opens. Select the appropriate action and click [Next]. The Action Properties window opens.

Using the Scheduler

The Scheduler folder can be used to configure actions to occur on a schedule (reoccurring or one time only). For more information, refer to Chapter 20: Scheduler Folder on page 317.

Toolbar Shortcut

1. In System Administration, select **Scheduler** from the **Administration** menu. In Alarm Monitoring, click the Scheduler toolbar button.
2. Click [Add]. The Add Action Wizard window displays.
3. In the Category listing window, select “Action Types” and in the Objects listing window, select the appropriate action.
4. Click [Next]. The Action Properties window opens.

Using Global I/O

The Global I/O folder can be used to configure actions to occur based on an incoming event. For more information, refer to the Global I/O Folder chapter in the System Administration User Guide.

1. In System Administration, select **Global I/O** from the **Access Control** menu.
2. Select a global linkage.
3. Click [Modify].
4. On the Output Action tab, click [Add].
5. The Add Action Wizard window displays. In the Category listing window, select “Action Types” and in the Objects listing window, select the appropriate action.
6. Click [Next]. The Action Properties window opens.

Using Guard Tour

The Guard Tour folder can be used to configure actions to occur under certain conditions related to a guard tour. For more information, refer to the Guard Tour Folder chapter in the System Administration User Guide.

1. In System Administration, select **Guard Tour** from the **Monitoring** menu. You cannot configure an action using the Guard Tour option available in Alarm Monitoring.
2. On the Tours tab, highlight a tour.
3. Click [Modify].
4. The Tour Wizard window opens. Select (place a checkmark beside) an ID/ hardware device.
5. Click [Next].
6. Click [Add].
7. The Add Action Wizard window displays. In the Category listing window, select “Action Types” and in the Objects listing window, select the appropriate action.
8. Click [Next]. The Action Properties window opens.

Using Acknowledgment Actions

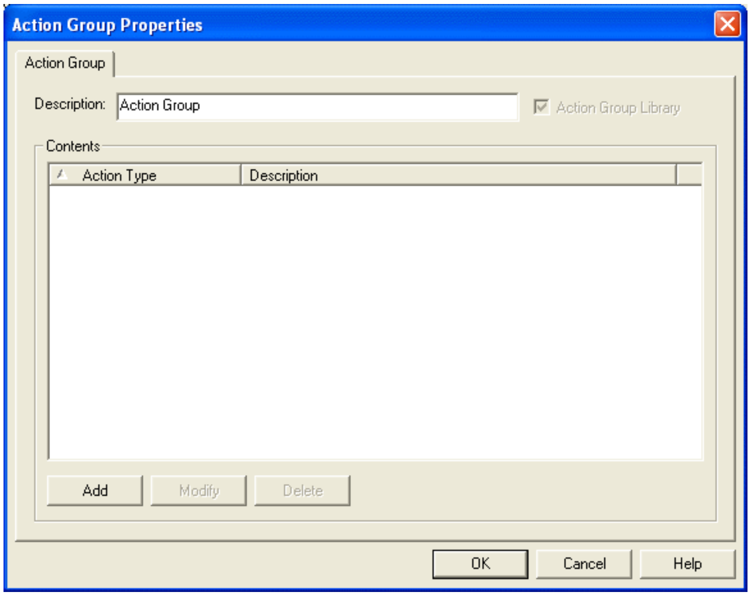
The Acknowledgment Actions folder can be used to configure actions to occur when an alarm is acknowledged. For more information, refer to the Alarm Configuration Folder chapter in the System Administration User Guide.

1. In System Administration, select **Alarms** from the **Monitoring** menu.
2. Click the Acknowledgment Actions tab.
3. Select (place a checkmark beside) an alarm.
4. Click [Modify].
5. In the Actions section, click [Add].
6. The Add Action Wizard window displays. In the Category listing window, select “Action Types” and in the Objects listing window, select the appropriate action.
7. Click [Next]. The Action Properties window opens.

Action Group Properties Window

The Action Group Properties action executes multiple actions simultaneously.

You can display the Action Group Properties window using the Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O forms. For more information, refer to Open an Action Properties Window on page 331.



Description: Action Group

☑ Action Group Library

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Action Group Properties Window Field Table

Form Element	Comment
Description	When adding or modifying an action group, you can enter a description of the action group that is being configured.
Action Group Library	When selected, the action group that you are adding or modifying will be available for selection in the Action Group Library. For more information, refer to “Action Groups Overview” in the Action Group Library Folder chapter in the System Administration User Guide.
Action Type listing window	Displays the action types which have been assigned to the selected action group.
Add	Click this button to add an action type.
Modify	Click this button to modify the action type that is selected in the Action Type listing window.
Delete	Click this button to delete the action type that is selected in the Action Type listing window from the selected action group.
OK	Click this button to save your changes and exit out of the Action Group Properties window.
Cancel	Click this button to exit the Action Group Properties window without saving your changes.
Help	Click this button to display online help for this window.

Action Group Properties Window Procedures

Add an Action Group

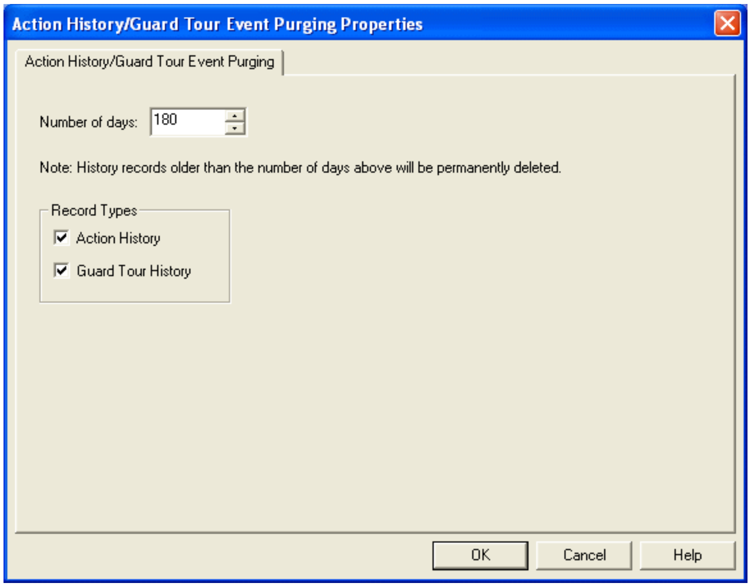
1. Open the Action Group Properties window using the Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. In the **Description** field, enter a description of the action group that is being configured.
3. Select the **Action Group Library** check box if you want this action group to be available for selection in the Action Group Library. For more information, refer to the Action Group Library Folder chapter in the System Administration User Guide.
4. Click [Add]. The Select Action Type window opens.
5. Select an action type and then click [Next]. Depending on which action type you chose, a corresponding action properties window will open.
6. Configure the action type you selected in step 5. To do this, you must refer to the action properties windows sections in this chapter for information on each action properties window.
7. Repeat steps 4-6 for each action type you want to assign to this group.
8. Click [OK].

Action History/Guard Tour Event Purging Properties Window

The Action History/Guard Tour Event Purging action allows you to create an action that will automatically delete certain records after they are a specified number of days old. For example, you can have all Guard Tour History record types deleted when they are 180 days old.

You can display the Action History/Guard Tour Event Purging Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 331.

Note: In segmented systems, the Action History/Guard Tour Event Purging action must be applied to all segments.


Action History/Guard Tour Event Purging Properties
Action History/Guard Tour Event Purging
OK
Cancel
Help

Number of days: 180

Note: History records older than the number of days above will be permanently deleted.

Record Types
☑ Action History
☑ Guard Tour History

Action History/Guard Tour Event Purging Properties Window

Form Element	Comment
Number of Days	The history records older than the number of days selected will be permanently deleted when the action runs.
Action History	Select this check box if you want Action History records deleted that are older than the Number of days setting.
Guard Tour History	Select this check box if you want Guard Tour History records deleted that are older than the Number of days setting.
OK	Click this button to add the action and exit out of the Action History/Guard Tour Event Purging Properties window.
Cancel	Click this button to exit the Action History/Guard Tour Event Purging Properties window without adding the action.

Action History/Guard Tour Event Purging Properties Window

Form Element	Comment
Help	Click this button to display online help for this window.

Action History/Guard Tour Event Purging Properties Window Procedures

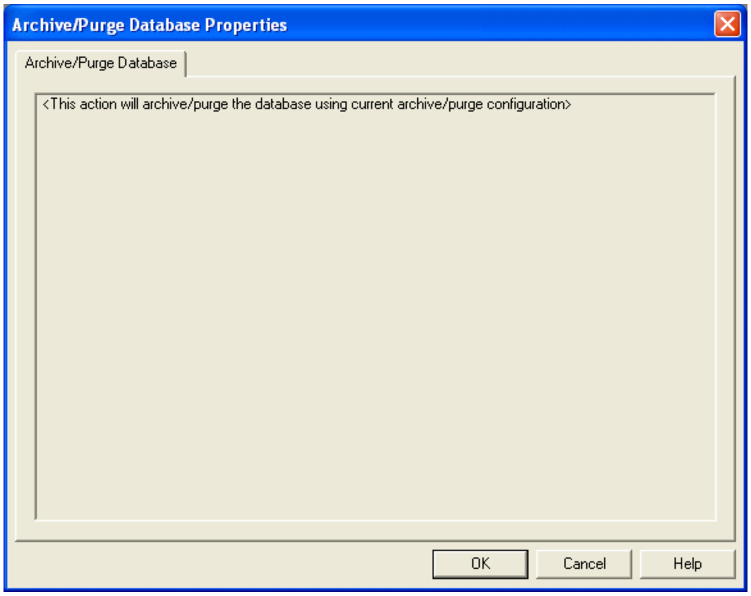
Add an Action History/Guard Tour Event Purging Action

1. Open the Action History/Guard Tour Event Purging Properties window using the Scheduler. For more information, refer to Open an Action Properties Window on page 331.
2. Enter how old (number of days) records can be before they are purged.
3. Choose the type of records you want to delete.
4. Click [OK]. This action is now configured to archive/purge the database using your current archive/purge configurations.

Archive/Purge Database Properties Window

You can display the Archive/Purge Database Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 331.

Note: In segmented systems, the Archive/Purge Database Properties action must be applied to all segments.



<This action will archive/purge the database using current archive/purge configuration>

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Archive/Purge Database Properties Window Field Table

Form Element	Comment
Listing window	Displays the following message: "<This action will archive/purge the database using current archive/purge configuration>"
OK	Click this button to add the action and exit out of the Archive/Purge Database Properties window.
Cancel	Click this button to exit the Archive/Purge Database Properties window without adding the action.
Help	Click this button to display online help for this window.

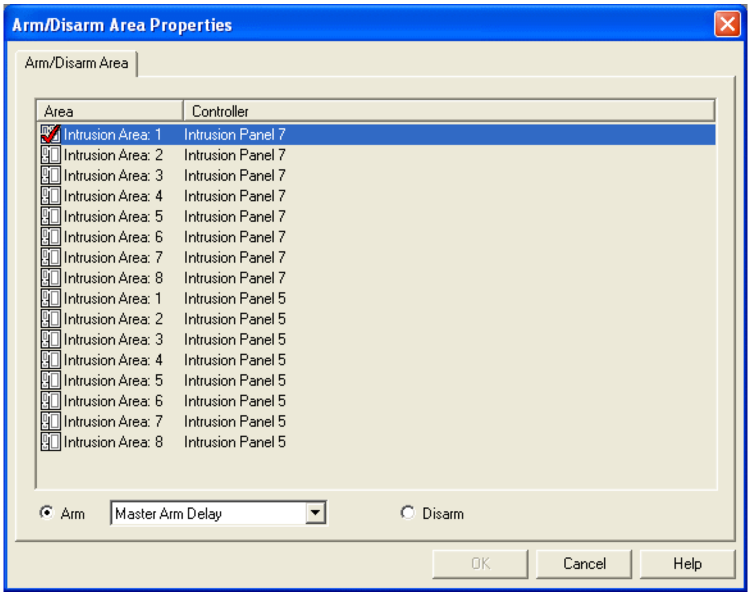
Archive/Purge Database Properties Window Procedures

Add an Archive/Purge Database Action

1. Open the Archive/Purge Database Properties window using the Scheduler. For more information, refer to Open an Action Properties Window on page 331.
2. Click [OK]. This action is now configured to archive/purge the database using your current archive/purge configurations. For more information, refer to the Archives Folder chapter in the System Administration User Guide.

Arm/Disarm Area Properties Window

You can display the Arm/Disarm Area Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Area	Controller
☑ Intrusion Area: 1	Intrusion Panel 7
☐ Intrusion Area: 2	Intrusion Panel 7
☐ Intrusion Area: 3	Intrusion Panel 7
☐ Intrusion Area: 4	Intrusion Panel 7
☐ Intrusion Area: 5	Intrusion Panel 7
☐ Intrusion Area: 6	Intrusion Panel 7
☐ Intrusion Area: 7	Intrusion Panel 7
☐ Intrusion Area: 8	Intrusion Panel 7
☐ Intrusion Area: 1	Intrusion Panel 5
☐ Intrusion Area: 2	Intrusion Panel 5
☐ Intrusion Area: 3	Intrusion Panel 5
☐ Intrusion Area: 4	Intrusion Panel 5
☐ Intrusion Area: 5	Intrusion Panel 5
☐ Intrusion Area: 6	Intrusion Panel 5
☐ Intrusion Area: 7	Intrusion Panel 5
☐ Intrusion Area: 8	Intrusion Panel 5

● Arm Master Arm Delay ○ Disarm

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Arm/Disarm Area Properties Window Field Table

Form Element	Comment
Listing window	Lists currently enabled intrusion areas. Intrusion areas are configured on the Areas form in the Intrusion Detection Configuration folder.
Arm	When configuring an area as an action, select this radio button if you want the action to be that the area will be armed. When an area is armed, protection for this area is “turned on.” Alarms will be reported within the area (the zones within the area will report alarms when activated). For example, consider a home burglar system that has sensors on the windows and doors and motion detectors inside. When the owner leaves the home, they arm the system. Alarms will be reported if those windows/doors are opened or if motion is detected.
Arm	You must also select an option from the drop-down list. The following terms will help you choose an option. *Instant arm* - some intrusion panels support the notion of both delay arm and instant arm. With instant arm, the area is armed immediately. *Interior* and *Perimeter*- in higher end intrusion panels, there is the concept of an interior and a perimeter of an area. Various zones within the area are associated with either the interior or the perimeter. Zones that might be associated with the interior are motion detectors placed in the hallways of an office building. Zones that might be associated with the perimeter are sensors on external windows and doors. *Master arm* - when an area is master armed, the entire area is armed. This includes both the perimeter and the interior. *Perimeter arm* - when an area is perimeter armed, only the perimeter is armed. This means that those zones associated with the interior will continue to generate alarms, but those associated with the perimeter will not. This type of arming may be used when an authorized person is inside a building at off hours. They don’t want the interior armed and reporting alarms since they will be moving throughout the interior. However, if somebody else breaches the perimeter of the building (forces open a door, breaks a window, etc.), alarms will be reported. (*continued on next page*) *Partial arm* - arms only those zones that have been configured for partial arming. All other zones in the area will not be armed.

Form Element	Comment
Arm (continued)	For Detection Systems intrusion detection panel types, choices include: • Arm Entire Partition - arms both the interior and perimeter of the area. • Perimeter Arm - arms the perimeter of the area. For Bosch intrusion detection panel types, choices include: • Master Arm Delay - master (both perimeter and interior) arm (with exit and entry delays) the area. • Master Arm Instant - master (both perimeter and interior) arms (no delays) the area. • Perimeter Delay Arm - delay arms all perimeter points in the area. • Perimeter Instant Arm - instantly arms all perimeter points (no delays) in the area. For Galaxy intrusion detection panel types, choices include: • Arm Entire Partition - arms both the interior and perimeter of the area. • Partial Arm - arms only those zones that have been configured for partial arming. All other zones in the area will not be armed.
Disarm	When configuring an area as an action, select this radio button if you want the action to be that the area will be disarmed. When an area is disarmed, protection for this area is “turned off.” Alarms will not be reported within the area. For example, consider a home burglar system that has sensors on the windows and doors and motion detectors inside. When the owner arrives home, he/she disarms the system so that alarms won’t be reported as they walk around the house.
OK	Click this button to add the action and exit out of the Arm/Disarm Area Properties window.
Cancel	Click this button to exit the Arm/Disarm Area Properties window without adding the action.
Help	Click this button to display online help for this window.

Arm/Disarm Area Properties Window Procedures

Add an Arm/Disarm Area Action

1. Open the Arm/Disarm Area Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O.

For more information, refer to Open an Action Properties Window on page 331.

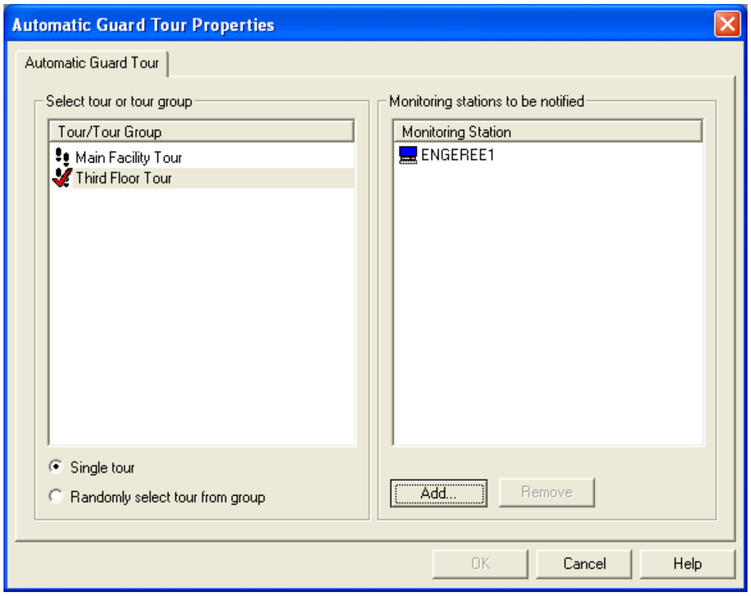
2. From the listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Arm** radio button if you want the action to be that the area will be armed. You must also select an option from the drop-down list.
   - Select the **Disarm** radio button if you want the action to be that the area will be disarmed.

Important: Refer to the Arm/Disarm Area Properties Window Field Table table on page 342 for detailed information on arming and disarming areas.

4. Click [OK].

Automatic Guard Tour Properties Window

You can display the Automatic Guard Tour Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 331.



Note: If you have accessed the Automatic Guard Tour Properties window via the Scheduler form, the window will contain both the Automatic Guard Tour form and the Scheduler form.

Automatic Guard Tour Properties Window Field Table

Form Element	Comment
Tour/Tour Group listing window	Displays a list of the tours and tour groups which have been configured in the system. Tours and tour groups are configured in the Guard Tour folder.
Single tour	Select this radio button if you want to configure an automatic guard tour for a single tour. When selected, only single tours will be listed in the Tour/Tour Group listing window.
Randomly select tour from group	Select this radio button if you want to configure an automatic guard tour that will be randomly selected from a tour group. When selected, only tours groups that are configured as random tour lists will be listed in the Tour/Tour Group listing window. Tour groups are configured on the Tour Groups form of the Guard Tour folder. A tour group is considered a random tour list when the **Random Tour List** check box is selected on the Tour Groups form.
Monitoring Station listing window	Displays a list of the monitoring stations which are assigned to the selected tour. These monitoring stations will be notified when the automatic guard tour is scheduled to begin.
Add	Click this button to display the Select Monitoring Station window and add a monitoring station to the Monitoring Station listing window.
Remove	Click this button to remove the selected monitoring station from the Monitoring Station listing window.
OK	Click this button to add the action and exit out of the Automatic Guard Tour Properties window.
Cancel	Click this button to exit the Automatic Guard Tour Properties window without adding the action.
Help	Click this button to display online help for this window.

Automatic Guard Tour Properties Window Procedures

Add an Automatic Guard Tour Action

1. Open the Automatic Guard Tour Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 331.
2. Do one of the following:
   - Select the **Single Tour** radio button if you want to configure an automatic guard tour for a single tour. When selected, only single tours will be listed in the Tour/Tour Group listing window.
   - Select the **Randomly select tour from group** radio button if you want to configure an automatic guard tour that will be randomly selected from a tour group. When selected, only tours groups that are configured

as random tour lists will be listed in the Tour/Tour Group listing window.

3. The monitoring stations that have been assigned to the selected tour or tour group will be displayed in the Monitoring Station listing window. Do one of the following:
   - If no monitoring stations have been assigned or if you want to assign an additional monitoring station, then click [Add]. The Select Monitoring Station window opens.
   - If you do not want to assign a monitoring station, proceed to step 7.
4. Click on a monitoring station to select it.
5. Click [OK]. The monitoring station you selected will be listing in the Monitoring Station listing window. All monitoring stations in the Monitoring Station listing window will, in the Alarm Monitoring application, receive a notification message when the tour is scheduled to begin.
6. Repeat steps 3-5 for each monitoring station you want to add.

Note: If you want to remove a monitoring station from the Monitoring Station listing window, click on an entry to select it and then click [Remove].

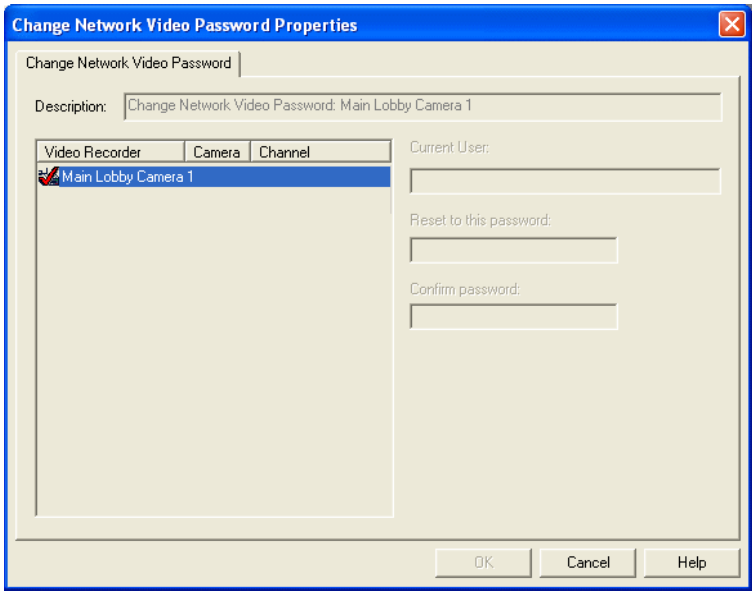
7. Click [OK].

Note: If you have accessed the Automatic Guard Tour Properties window via the Scheduler folder or the Scheduler form in the Guard Tour folder, the window will contain both the Automatic Guard Tour form and the Schedule form. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Change Network Video Password Properties Window

The Change Network Video Password action allows you to schedule automatic password changes for video recorders. You can make the change a one-time event or to schedule it daily, weekly, or monthly with the Edit Recurring Action Schedule. For more information, refer to Chapter 20: Scheduler Folder on page 317.

You can display the Change Network Video Password Properties window using the Action Group Library, Scheduler, or Global I/O. Only the Scheduler will let you set up the password to be changed at a later date. For more information, refer to Open an Action Properties Window on page 331.



Change Network Video Password Properties

Change Network Video Password

Description: Change Network Video Password: Main Lobby Camera 1

Video Recorder	Camera	Channel
Main Lobby Camera 1		

Current User:

Reset to this password:

Confirm password:

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Change Network Video Password Properties Window Field Table

Form Element	Comment
Description	Names the video device you are currently changing the password for.
Listing Window	Select the recorders and/or cameras you want to modify.
Current User	The name of the user account. This field automatically populates if a user name was initially populated on the Video Recorder/Camera forms.

Change Network Video Password Properties Window Field Table

Form Element	Comment
Reset to this password	Enter the password in the text box. The following restrictions apply: • Axis cameras allow up to 10 character passwords using A through Z, a through z, 0 - 9, !, #' - ', -, ., ^, _, ~, $ • Sony cameras allow up to 16 character passwords using A through Z, a through z, 0 - 9 **Note:** In addition to these restrictions, ReadykeyPRO includes strong password enforcement, which checks the user's password against password standards. For more information, refer to Chapter 1: Introduction on page 27.
Confirm password	Enter the password a second time for verification.
OK	Adds the action and exits out of the Change Network Video Properties window.
Cancel	Exits the Change Network Video Password Properties window without adding the action.
Help	Displays online help for this window.

Change Network Video Password Properties Window Procedures

Change the Network Video Password

1. Open the Change Network Video Password Properties window using the Action Group Library or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. On the Change Network Video Password tab, enter the new password and confirm the password by typing it again.
3. Click [OK].

Schedule a One-Time Password Change

1. Open the Change Network Video Password Properties window using the Scheduler. For more information, refer to Open an Action Properties Window on page 331.
2. On the Change Network Video Password tab, enter the new password and confirm the password by typing it again.
3. On the Schedule tab, select the **One time** radio button.
4. Select the date and time you wish the password to change.
5. Click [OK].

Schedule a Recurring Password Change

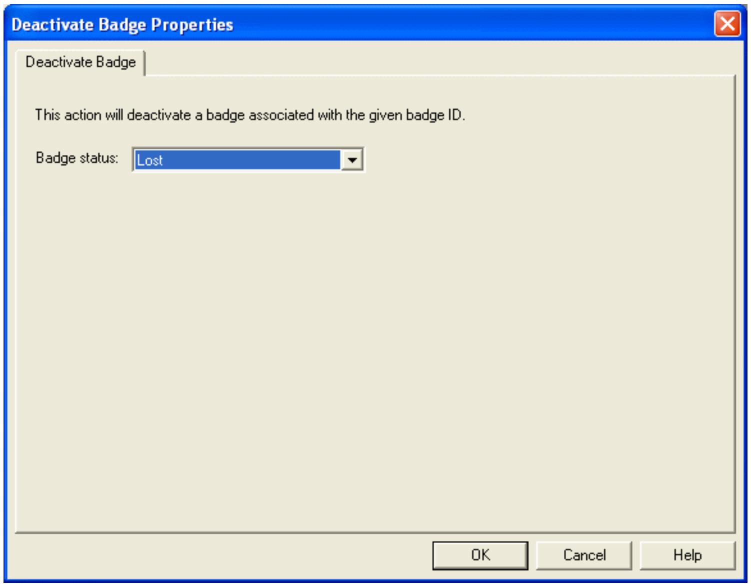
1. Open the Change Network Video Password Properties window using the Scheduler. For more information, refer to Open an Action Properties Window on page 331.
2. On the Change Network Video Password tab, enter the new password and confirm the password by typing it again
3. On the Schedule sub-tab, select the **Recurring** radio button.
4. Click [Change]. The Edit Recurring Action Schedule form displays.
5. Choose the time and date intervals that best suit your needs.
6. Click [OK] on the Edit Recurring Action Schedule form.
7. Click [OK] on the Change Network Video Password Properties window.

Deactivate Badge Properties Window

The Deactivate Badge action allows you to deactivate a cardholder's badge when it is either lost or returned.

You can display the Deactivate Badge Properties window using Global I/O. For more information, refer to Open an Action Properties Window on page 331.

Note: In segmented systems, the Action History/Guard Tour Event Purging action must be applied to all segments.



This action will deactivate a badge associated with the given badge ID.

Badge status: Lost

Deactivate Badge Properties Window Field Table

Form Element	Comment
Badge Status	Use to select the status of a badge that will be deactivated. Choices are Lost and Returned.
OK	Click this button to add the action and exit out of the Deactivate Badge Properties window.
Cancel	Click this button to exit the Deactivate Badge Properties window without adding the action.
Help	Click this button to display online help for this window.

Deactivate Badge Properties Window Procedures

Add a Deactivate Badge Action

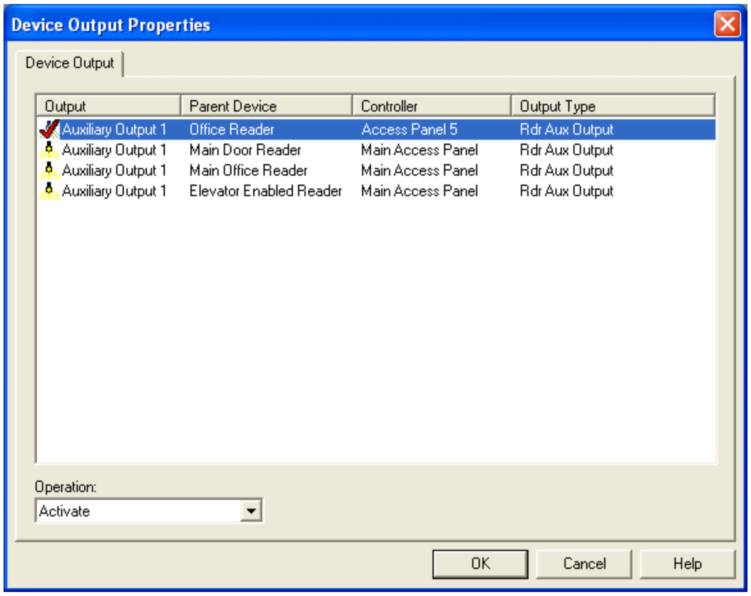
1. Open the Deactivate Badge Properties window using Global I/O. For more information, refer to Open an Action Properties Window on page 331.

Note: In order to execute the action, Global I/O should have a linkage configured on a device, event, and badge ID that is passed to the action at runtime.

2. Click [Add].
3. Click the Output Action sub-tab.
4. Click [Add]. The Add Action Wizard window opens.
5. Select “Deactivate Badge” from the Objects listing window.
6. Click [Next]. The Deactivate Badge Properties window appears.
7. Choose the type of badge you want to deactivate.
8. Click [OK].
9. Click [OK] again.

Device Output Properties Window

You can display the Device Output Properties window using Action Group Library, Scheduler, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Output	Parent Device	Controller	Output Type
Auxiliary Output 1	Office Reader	Access Panel 5	Rdr Aux Output
Auxiliary Output 1	Main Door Reader	Main Access Panel	Rdr Aux Output
Auxiliary Output 1	Main Office Reader	Main Access Panel	Rdr Aux Output
Auxiliary Output 1	Elevator Enabled Reader	Main Access Panel	Rdr Aux Output

Operation: Activate

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Form Element	Comment
Output listing window	Displays a list of available device outputs which have been configured in the system.
Activate	When configuring a device output as an action, select this from the drop-down menu if you want the action to be that the device output will activate. When a device output is activated, that means it is in an “on” state.
Deactivate	When configuring a device output as an action, select this from the drop-down menu if you want the action to be that the device output will deactivate. When a device output is deactivated, that means it is in an “off” state.
Pulse	When configuring a device output as an action, select this from the drop-down menu if you want the action to be that the device output will pulse (turn on and then turn off again).

Form Element	Comment
Toggle	When configuring a device output as an action, select this from the drop-down menu if you want to toggle the state of the relay. For example, if the relay is on (activated), toggling deactivates it. If the relay is off (deactivated), toggling activates it. **Note:** Only offboard relays on the Bosch (7412 and 9412) intrusion panels support the toggle option.
OK	Click this button to add the action and exit out of the Device Output Properties window.
Cancel	Click this button to exit the Device Output Properties window without adding the action.
Help	Click this button to display online help for this window.

Device Output Properties Window Procedures

Add a Device Output Action

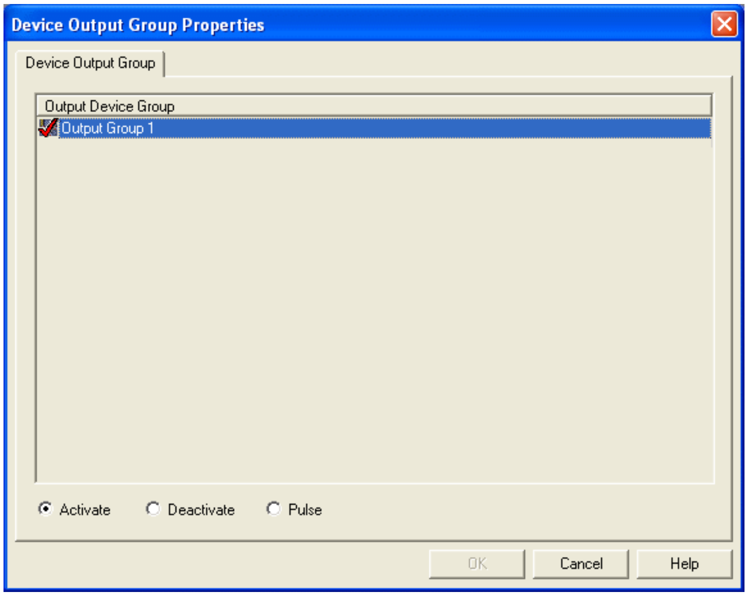
1. Open the Device Output Properties window using the Action Group Library, Scheduler, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) an entry in the Output listing window.
3. Do one of the following:
   - Select **Activate** from the drop-down menu if you want this action to be that the device output will activate. When a device output is activated, that means it is in an “on” state.
   - Select **Deactivate** from the drop-down menu if you want this action to be that the device output will deactivate. When a device output is deactivated, that means it is in an “off’ state.
   - Select **Pulse** from the drop-down menu if you want this action to be that the device output will pulse (turn on and then turn off again).
   - Select **Toggle** from the drop-down menu in you want this action to be that the device output will toggle the state of the relay. For example, if the relay is on (activated), toggling deactivates it. If the relay is off (deactivated), toggling activates it.

Note: Only offboard relays on the Bosch (7412 and 9412) intrusion panels support the toggle option.

4. Click [OK].

Device Output Group Properties Window

You can display the Device Output Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Device Output Group Properties Window Field Table

Form Element	Comment
Output Device Group listing window	Displays a list of available output device groups which have been configured in the system.
Activate	When configuring an output device group as an action, select this radio button if you want the action to be that the device outputs in the group will activate. When device outputs are activated, that means they are in an “on” state.
Deactivate	When configuring an output device group as an action, select this radio button if you want the action to be that the device outputs in the group will deactivate. When device outputs are deactivated, that means they are in an “off” state.
Pulse	When configuring an output device group as an action, select this radio button if you want the action to be that the device outputs in the group will pulse (they will turn on and then turn off again).
OK	Click this button to add the action and exit out of the Device Output Group Properties window.
Cancel	Click this button to exit the Device Output Group Properties window without adding the action.
Help	Click this button to display online help for this window.

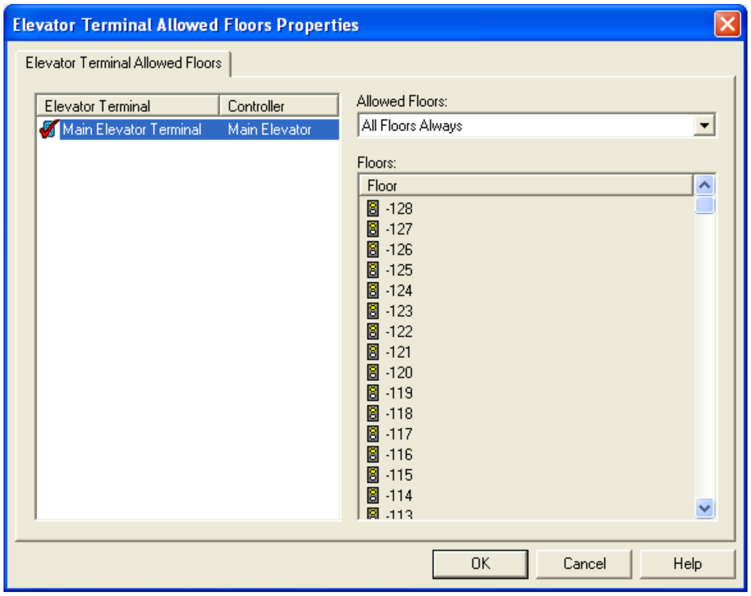
Device Output Group Properties Window Procedures

Add a Device Output Group Action

1. Open the Device Output Group Properties window, using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) a group in the Output Device Group listing window.
3. Do one of the following:
   - Select the **Activate** radio button if you want this action to be that the device outputs in the group will activate. When device outputs are activated, that means they are in an “on” state.
   - Select the **Deactivate** radio button if you want this action to be that the device outputs in the group will deactivate. When device outputs are deactivated, that means they are in an “off’ state.
   - Select the **Pulse** radio button if you want this action to be that the device outputs in the group will pulse (they will turn on and then turn off again).
4. Click [OK].

Elevator Terminal Allowed Floors Properties Window

You can display the Elevator Terminal Allowed Floors Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.


Elevator Terminal Allowed Floors Properties
Elevator Terminal Allowed Floors
OK
Cancel
Help

Elevator Terminal	Controller
Main Elevator Terminal	Main Elevator

Allowed Floors: All Floors Always

Floors:

Floor
-128
-127
-126
-125
-124
-123
-122
-121
-120
-119
-118
-117
-116
-115
-114
-113

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Elevator Terminal Allowed Floors Properties Window Field Table

Form Element	Comment
Allowed Floors	Allowed floors are floors that can be accessed via the elevator terminal without supplying security credentials. Your options include: • **All Floors Always** - the elevator is allowed to all floors no matter the security credentials presented. • **No Floors** - The elevator is allowed to no floors without security credentials being presented.
Floors	Lists the floors the elevator is capable of traveling to.

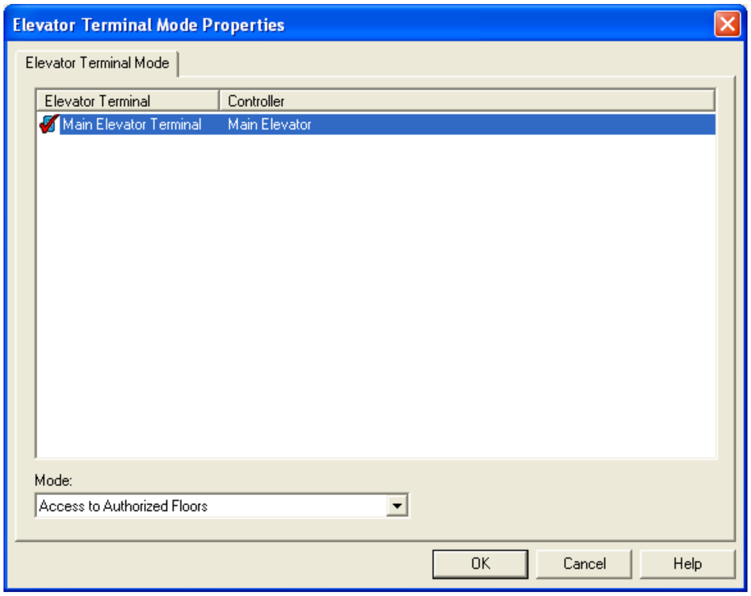
Elevator Terminal Allowed Floors Properties Window Procedures

Add an Elevator Terminal Allowed Floors Action

1. Open the Elevator Terminal Allowed Floors Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 331.
2. Select an elevator terminal in the listing window.
3. Select an option in the **Allowed Floors** drop-down box.
4. Click [OK].

Elevator Terminal Mode Properties Window

You can display the Elevator Terminal Mode Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Elevator Terminal	Controller
✓ Main Elevator Terminal	Main Elevator

Mode: Access to Authorized Floors

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Elevator Terminal Mode Properties Window Field Table

Form Element	Comment
Elevator Terminal Mode listing window	Lists the current elevator terminals and elevator controllers.
Mode	Refers to operational modes which dictate how the terminal interacts with the cardholder. Choose from: • Access to Authorized Floors • Default Floor Only • Default Floor or User Entry of Destination Floor • User Entry of Destination Floor

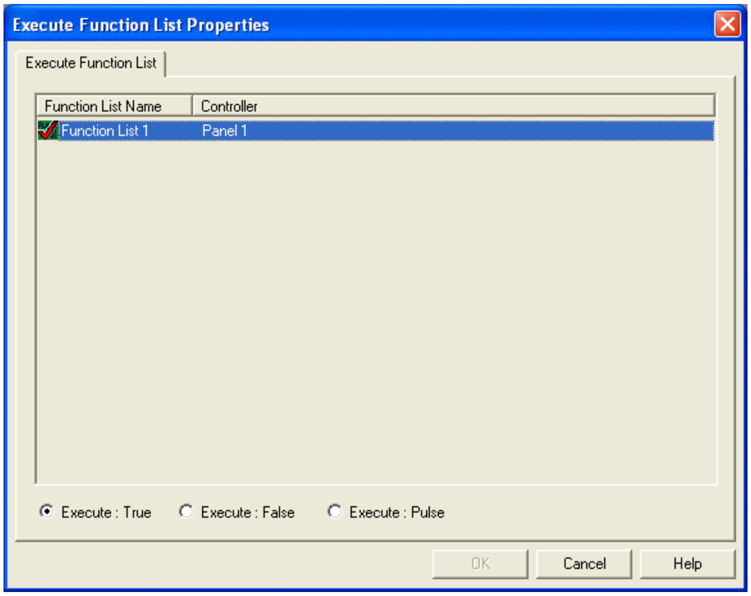
Elevator Terminal Mode Properties Window Procedures

Add an Elevator Terminal Mode Action

1. Open the Elevator Terminal Mode Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 331.
2. Select an elevator terminal in the listing window.
3. Select an option in the **Mode** drop-down box.
4. Click [OK].

Execute Function List Properties Window

You can display the Execute Function List Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Function List Name	Controller
✓ Function List 1	Panel 1

● Execute : True ○ Execute : False ○ Execute : Pulse

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Execute Function List Properties Window Field Table

Form Element	Comment
Function List listing window	Displays a list of available function lists which have been configured in the system.
Execute: True	When configuring a function list as an action, select this radio button if you want the action to execute the function list with an argument of "True."
Execute: False	When configuring a function list as an action, select this radio button if you want the action to execute the function list with an argument of "False."
Execute: Pulse	When configuring a function list an action, select this radio button if you want the action to execute the function list with an argument of "Pulse."
OK	Click this button to add the action and exit out of the Execute Function List Properties window.
Cancel	Click this button to exit the Execute Function List Properties window without adding the action.
Help	Click this button to display online help for this window.

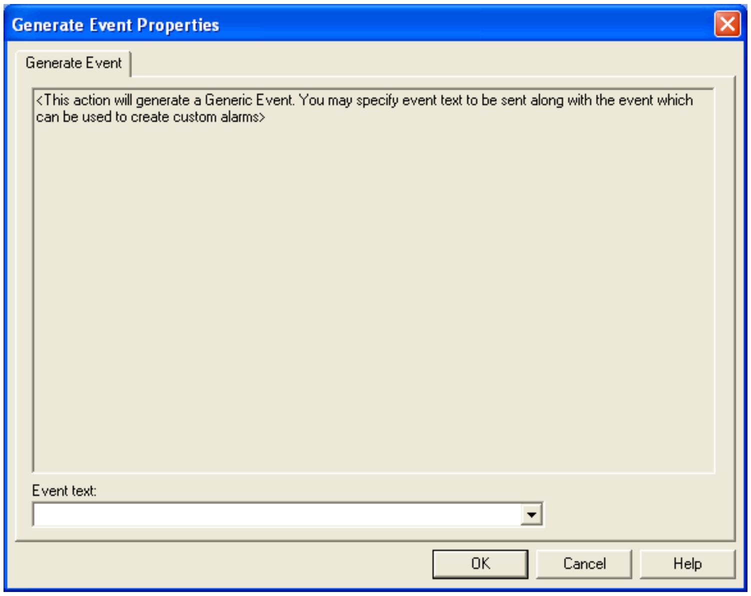
Execute Function List Properties Window Procedures

Add an Execute Function List Action

1. Open the Execute Function List Properties window, using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) an entry in the Function List listing window.
3. Do one of the following:
   - Select the **Execute: True** radio button if you want this action to execute the function list with an argument of "True."
   - Select the **Execute: False** radio button if you want this action to execute the function list with an argument of "False."
   - Select the **Execute: Pulse** radio button if you want this action to execute the function list with an argument of "Pulse."
4. Click [OK].

Generate Event Properties Window

You can display the Generate Event Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 331.



<This action will generate a Generic Event. You may specify event text to be sent along with the event which can be used to create custom alarms>

Generate Event Properties Window Field Table

Form Element	Comment
Event text	Type your custom event text here. You must create your own event text for this event.
OK	Click this button to add the action and exit out of the window.
Cancel	Click this button to exit the window without adding the action.
Help	Click this button to display online help for this window.

Elevator Terminal Mode Properties Window Procedures

Add an Elevator Mode Action

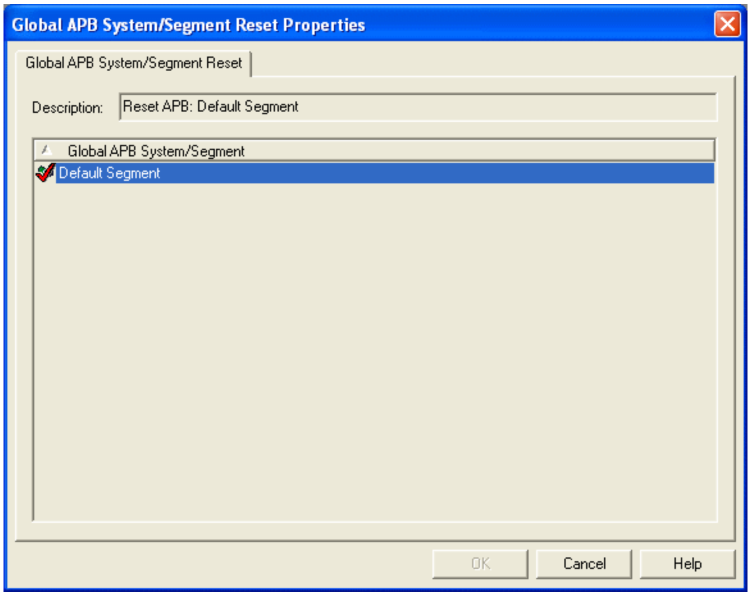
1. Open the Elevator Terminal Mode Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action

Properties Window on page 331.

2. Select an elevator terminal in the listing window.
3. Select an option in the **Mode** drop-down box.
4. Click [OK].

Global APB System/Segment Reset Properties Window

You can display the Global APB System/Segment Reset Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 331.



Global APB System/Segment Reset Properties

Description: Reset APB: Default Segment

Global APB System/Segment
✓ Default Segment

Global APB System/Segment Reset Properties Window Field Table

Form Element	Comment
Description	Displays a description of the selected global APB system/segment.
Global APB System/Segment listing window	Displays a list of the segments available for this action.
OK	Click this button to add the action and exit out of the Global APB System/Segment Reset Properties window.
Cancel	Click this button to exit the Global APB System/Segment Reset Properties window without adding the action.
Help	Click this button to display online help for this window.

Global APB System/Segment Reset Properties Window Procedures

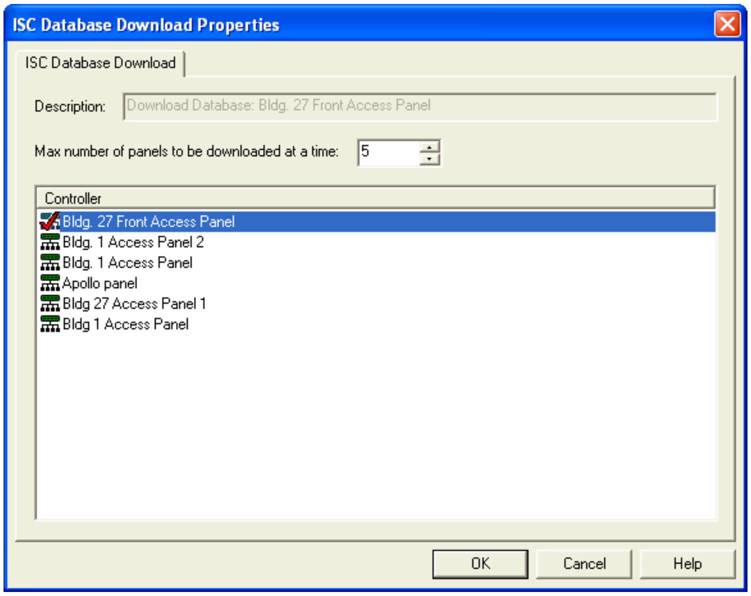
Add a Global APB System/Segment Reset Action

Note: Global APB must be configured on your system in order to add this action.

1. Open the Global APB System/Segment Reset Properties window, using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) a segment from the Global APB System/ Segment listing window.
3. Click [OK]. If segmentation is enabled, this action will reset APB for the selected segment. If segmentation is not enabled, this action will reset APB for your entire system.
4.
5. In the Monitoring stations to be notified listing window select the monitoring stations to be notified of a grant/deny popup action.
   a. Click [Edit Stations] to select specific monitoring stations or select the **Use all available monitoring stations** check box to select all of the monitoring stations.

ISC Database Download Properties Window

You can display the ISC Database Download Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 331.



Description: Download Database: Bldg. 27 Front Access Panel

Max number of panels to be downloaded at a time: 5

Controller
- ✓ Bldg. 27 Front Access Panel
- Bldg. 1 Access Panel 2
- Bldg. 1 Access Panel
- Apollo panel
- Bldg 27 Access Panel 1
- Bldg 1 Access Panel

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

ISC Database Download Properties Window Field Table

Form Element	Comment
Description	Displays a description of the access panel which is selected in the Access Panel listing window. **Note:** This field only displays a description when one and only one access panel is selected.
Max number of panels to be downloaded at a time	When configuring a database download as an action, select the maximum number of access panels that can be downloaded at a time.
Controller listing window	Displays a list of available controllers that have been configured in the system.
OK	Click this button to add the action and exit out of the ISC Database Download Properties window.
Cancel	Click this button to exit the ISC Database Download Properties window without adding the action.
Help	Click this button to display online help for this window.

ISC Database Download Properties Window Procedures

Add an ISC Database Download Action

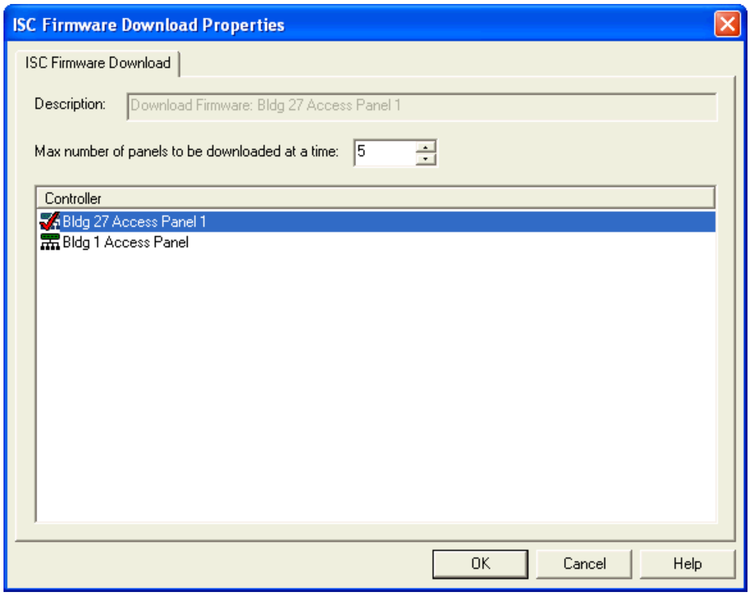
1. Open the ISC Database Download Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 331.
2. Select the max number of panels to be downloaded at a time.
3. From the Access Panel listing window, click on an entry to select it.

Note: You can select multiple entries.

4. Click [OK].

ISC Firmware Download Properties Window

You can display the ISC Firmware Download Properties window using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 331.



Description: Download Firmware: Bldg 27 Access Panel 1

Max number of panels to be downloaded at a time: 5

Controller
✓ Bldg 27 Access Panel 1
Bldg 1 Access Panel

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

ISC Firmware Download Properties Window Field Table

Form Element	Comment
Description	Displays a description of the access panel which is selected in the Access Panel listing window. **Note:** This field only displays a description when one and only one access panel is selected.
Max number of panels to be downloaded at a time	When configuring a firmware download as an action, select the maximum number of access panels that can be downloaded at a time.
Controller listing window	Displays a list of available controllers that have been configured in the system.
OK	Click this button to add the action and exit out of the ISC Firmware Download Properties window.
Cancel	Click this button to exit the ISC Firmware Download Properties window without adding the action.
Help	Click this button to display online help for this window.

ISC Firmware Download Properties Window Procedures

Add an ISC Firmware Download Action

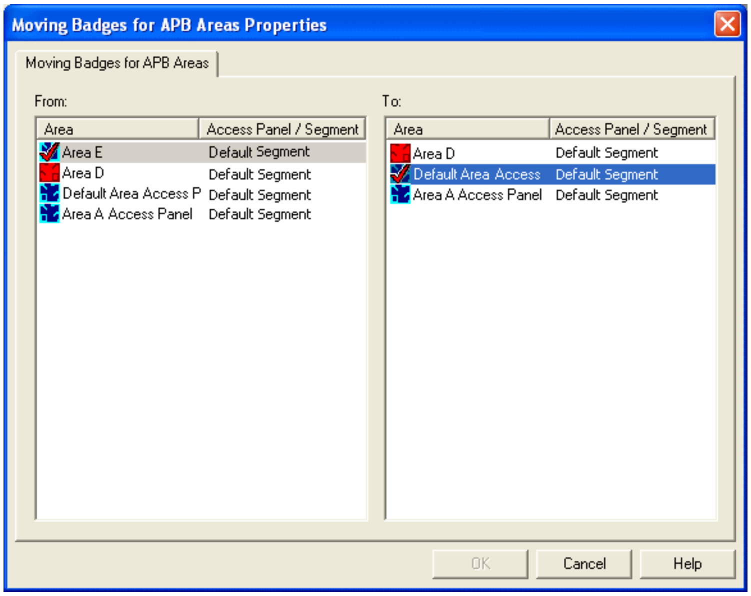
1. Open the ISC Firmware Download Properties window, using the Action Group Library or Scheduler. For more information, refer to Open an Action Properties Window on page 331.
2. Select the max number of panels to be downloaded at a time.
3. From the Access Panel listing window, click on an entry to select it.

Note: You can select multiple entries.

4. Click [OK].

Moving Badges for APB Areas Properties Window

You can display the Moving Badges for APB Areas Properties window using Action Group Library, Scheduler, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Moving Badges for APB Areas Properties

Moving Badges for APB Areas

From:

Area	Access Panel / Segment
Area E	Default Segment
Area D	Default Segment
Default Area Access P	Default Segment
Area A Access Panel	Default Segment

To:

Area	Access Panel / Segment
Area D	Default Segment
Default Area Access	Default Segment
Area A Access Panel	Default Segment

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Form Element	Comment
From listing window	Displays a list of areas that are available for selection.
To listing window	Displays a list of areas that are available for selection.
OK	Click this button to add the action and exit out of the Moving Badges for APB Areas Properties window.
Cancel	Click this button to exit the Moving Badges for APB Areas Properties window without adding the action.
Help	Click this button to display online help for this window.

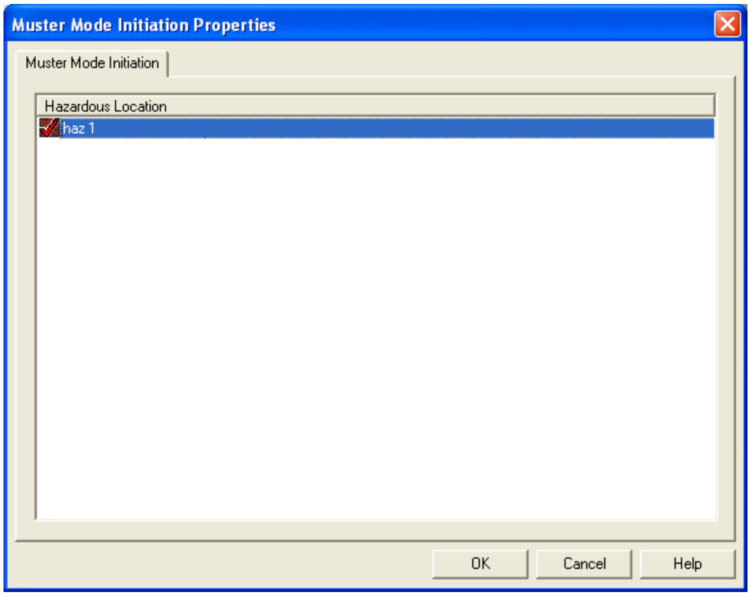
Moving Badges for APB Areas Properties Window Procedures

Add a Moving Badges for APB Areas Action

1. Open the Moving Badges for APB Areas Properties window using the Action Group Library, Scheduler, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. In the From listing window, select (place a checkmark beside) the area that you want to move badges from when this action is executed.
3. In the To listing window, select (place a checkmark beside) the area that you want to move badges to when this action is executed.
4. Click [OK].

Muster Mode Initiation Properties Window

You can display the Muster Mode Initiation Properties window using the Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Form Element	Comment
Hazardous Location listing window	Displays a list of available hazardous locations that have been configured in the system.
OK	Click this button to add the action and exit out of the Muster Mode Initiation Properties window.
Cancel	Click this button to exit the Muster Mode Initiation Zone Properties window without adding the action.
Help	Click this button to display online help for this window.

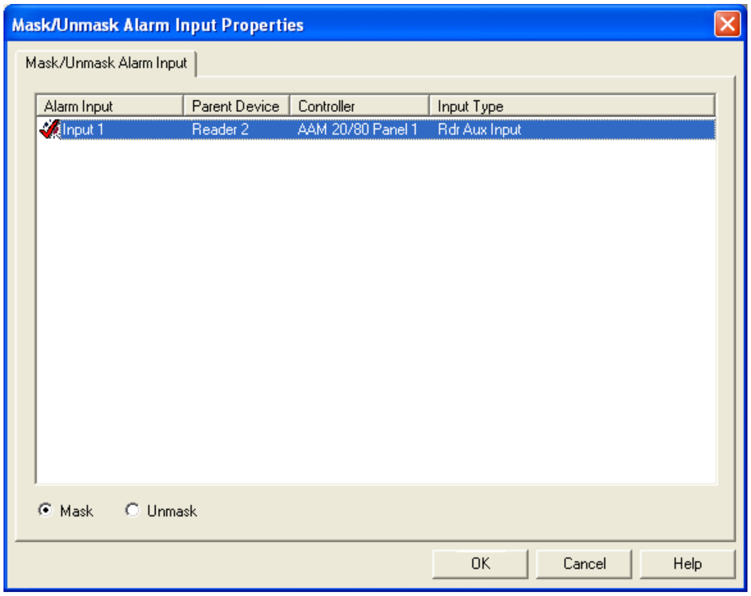
Muster Mode Initiation Properties Window Procedures

Add a Muster Mode Initiation Action

1. Open the Muster Mode Initiation Properties window using Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. From the listing window, click on an entry to select it.
3. Click [OK]. This action is now configured to initiate muster mode in the selected hazardous location. (Refer to the Areas folder chapter in this user guide for more information on mustering.)

Mask/Unmask Alarm Input Properties Window

You can display the Mask/Unmask Alarm Input Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O.



Alarm Input	Parent Device	Controller	Input Type
Input 1	Reader 2	AAM 20/80 Panel 1	Rdr Aux Input

● Mask ○ Unmask

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Alarm Input Properties Window Field Table

Form Element	Comment
Alarm Input listing window	Displays a list of available alarm inputs which have been configured in the system.
Mask	When configuring a mask/unmask alarm input action, select this radio button if you want the alarm input to be masked. When alarm inputs are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	When configuring a mask/unmask alarm input action, select this radio button if you want the alarm input to be unmasked. When alarm inputs are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	Click this button to add the action and exit out of the Mask/Unmask Alarm Input Properties window.
Cancel	Click this button to exit the Mask/Unmask Alarm Input Properties window without adding the action.
Help	Click this button to display online help for this window.

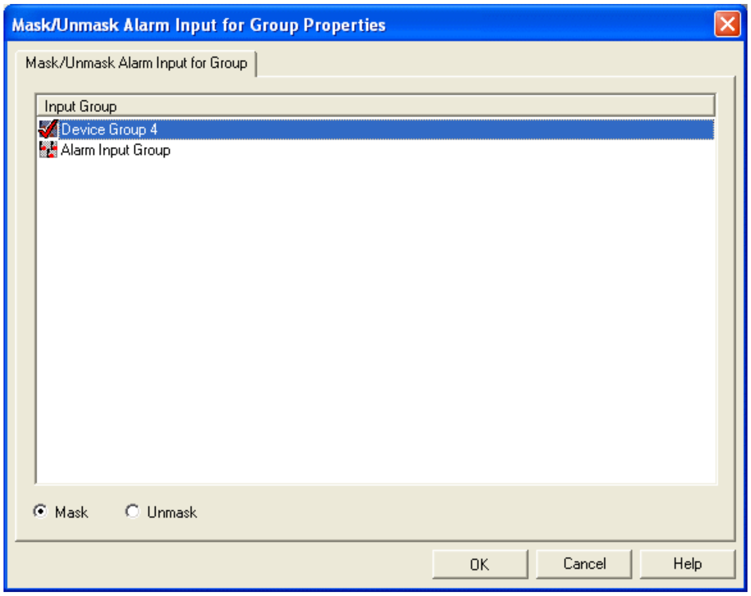
Mask/Unmask Alarm Input Properties Window Procedures

Add a Mask/Unmask Alarm Input Action

1. Open the Mask/Unmask Alarm Input Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. From the Alarm Input listing window, click on an entry to select it.
3. Do one of the following:
    - Select the **Mask** radio button if you want the alarm input to be masked. When alarm inputs are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
    - Select the **Unmask** radio button if you want the alarm input to be unmasked. When alarm inputs are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Alarm Input for Group Properties Window

You can display the Mask/Unmask Alarm Input for Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Mask/Unmask Alarm Input for Group Properties

Mask/Unmask Alarm Input for Group

Input Group
- ✓ Device Group 4
- Alarm Input Group

● Mask ○ Unmask

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Alarm Input for Group Properties Window Field Table

Form Element	Comment
Input Group listing window	Displays a list of available alarm input groups which have been configured in the system.
Mask	When configuring a mask/unmask alarm input for group action, select this radio button if you want the group of alarm inputs to be masked. When alarm input groups are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	When configuring a mask/unmask alarm input for group action, select this radio button if you want the group of alarm inputs to be unmasked. When alarm input groups are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	Click this button to add the action and exit out of the Mask/Unmask Alarm Input for Group Properties window.
Cancel	Click this button to exit the Mask/Unmask Alarm Input for Group Properties window without adding the action.
Help	Click this button to display online help for this window.

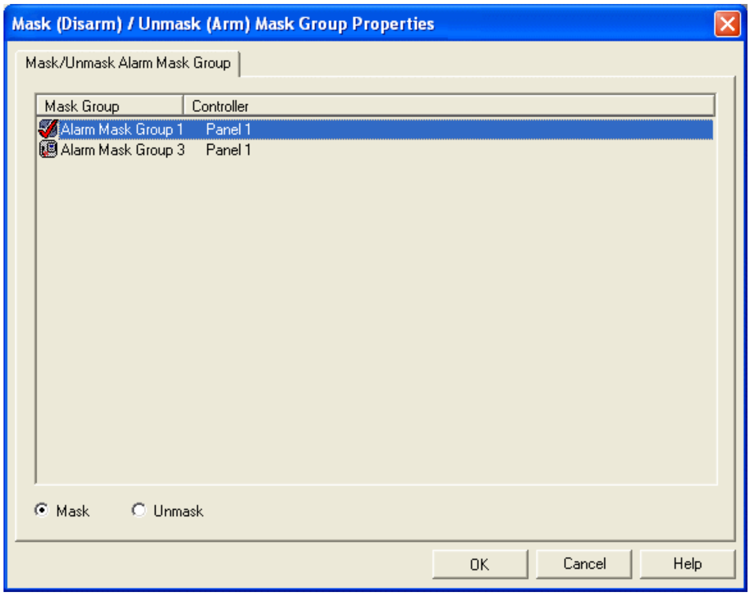
Mask/Unmask Alarm Input for Group Properties Window Procedures

Add a Mask/Unmask Alarm Input for Group Action

1. Open the Mask/Unmask Alarm Input for Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. From the Input Group listing window, click on an entry to select it.
3. Do one of the following:
    - Select the **Mask** radio button if you want the alarm inputs in the group to be masked. When alarm inputs are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
    - Select the **Unmask** radio button if you want the alarm inputs in the group to be unmasked. When alarm inputs are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask (Disarm) / Unmask (Arm) Mask Group Properties Window

You can display the Mask/Unmask Alarm Mask for Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Mask (Disarm) / Unmask (Arm) Mask Group Properties

Mask/Unmask Alarm Mask Group

Mask Group	Controller
✓ Alarm Mask Group 1	Panel 1
Alarm Mask Group 3	Panel 1

● Mask ○ Unmask

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask(Disarm)/Unmask(Arm) Mask Group Properties Window Field Table

Form Element	Comment
Mask Group listing window	Displays a list of available alarm mask groups which have been configured in the system.
Mask	When configuring a Mask (Disarm) / Unmask (Arm) Mask Group action, select this radio button if you want the mask group to be masked. When alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	When configuring a Mask (Disarm) / Unmask (Arm) Mask Group action, select this radio button if you want the mask group to be unmasked. When alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	Click this button to add the action and exit out of the Mask (Disarm) / Unmask (Arm) Mask Group Properties window.
Cancel	Click this button to exit the Mask (Disarm) / Unmask (Arm) Mask Group Properties window without adding the action.
Help	Click this button to display online help for this window.

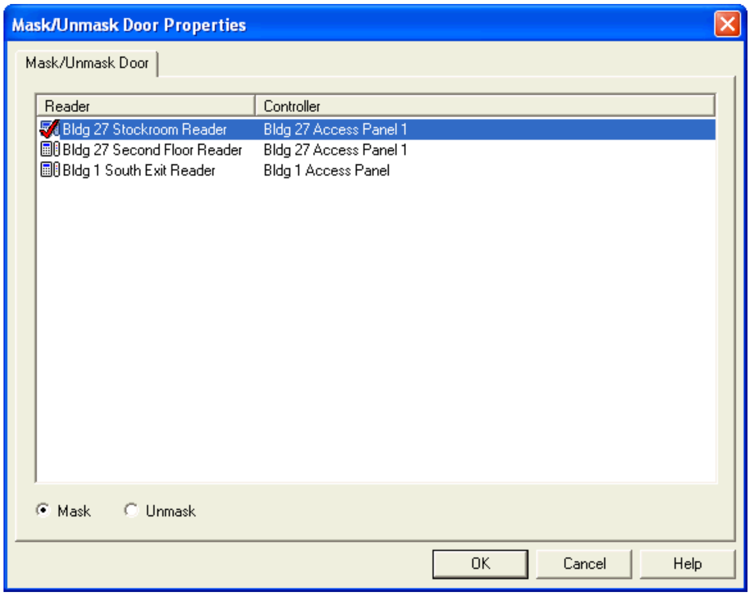
Mask (Disarm) / Unmask (Arm) Mask Group Properties Window Procedures

Add a Mask (Disarm) / Unmask (Arm) Mask Group Action

1. Open the Mask/Unmask Alarm Mask for Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) and entry in the Mask Group listing window.
3. Do one of the following:
   - Select the **Mask** radio button if you want the mask group to be masked. When alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the mask group to be unmasked. When alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Properties Window

You can display the Mask/Unmask Door Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Reader	Controller
Bldg 27 Stockroom Reader	Bldg 27 Access Panel 1
Bldg 27 Second Floor Reader	Bldg 27 Access Panel 1
Bldg 1 South Exit Reader	Bldg 1 Access Panel

● Mask ○ Unmask

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Door Form Properties Window Table

Form Element	Comment
Reader/Controller listing window	Displays a list of readers that are available for selection and the controllers that are associated with each.
Mask	When configuring a mask/unmask door action, select this radio button if you want the action to be that the door is masked. When masked doors generate alarms, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	When configuring a mask/unmask door action, select this radio button if you want the action to be that the door is unmasked. When unmasked doors generate alarms, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	Click this button to add the action and exit out of the Mask/Unmask Door Properties window.
Cancel	Click this button to exit the Mask/Unmask Door Properties window without adding the action.
Help	Click this button to display online help for this window.

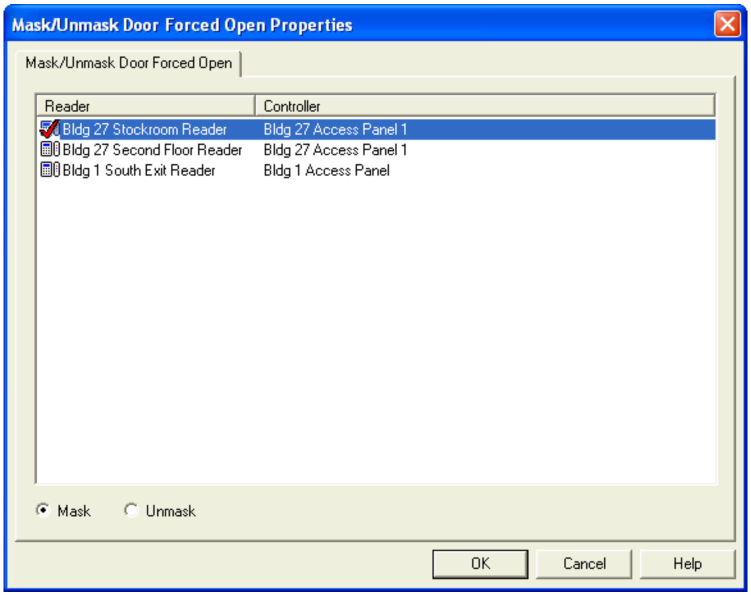
Mask/Unmask Door Properties Window Procedures

Add a Mask/Unmask Door Action

1. You can display the Mask/Unmask Door Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) and entry in the Reader/Controller listing window.
3. Do one of the following:
   - Select the **Mask** radio button if you want the action to be that the door is masked. When masked doors generate alarms, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the action to be that the door is unmasked. When unmasked doors generate alarms, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Forced Open Properties Window

You can display the Mask/Unmask Door Forced Open Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Mask/Unmask Door Forced Open Properties
Mask/Unmask Door Forced Open
OK
Cancel
Help

Reader	Controller
✓ Bldg 27 Stockroom Reader	Bldg 27 Access Panel 1
Bldg 27 Second Floor Reader	Bldg 27 Access Panel 1
Bldg 1 South Exit Reader	Bldg 1 Access Panel

● Mask ○ Unmask

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Door Forced Open Properties Window Field Table

Form Element	Comment
Reader/Controller listing window	Displays a list of available readers which have been configured in the system and the controllers that are associated with each.
Mask	When configuring a mask/unmask door forced open action, select this radio button if you want the door forced open alarm to be masked. When door forced open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	When configuring a mask/unmask door forced open action, select this radio button if you want the door forced open alarm to be unmasked. When door forced open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	Click this button to add the action and exit out of the Mask/Unmask Door Forced Open Properties window.
Cancel	Click this button to exit the Mask/Unmask Door Forced Open Properties window without adding the action.
Help	Click this button to display online help for this window.

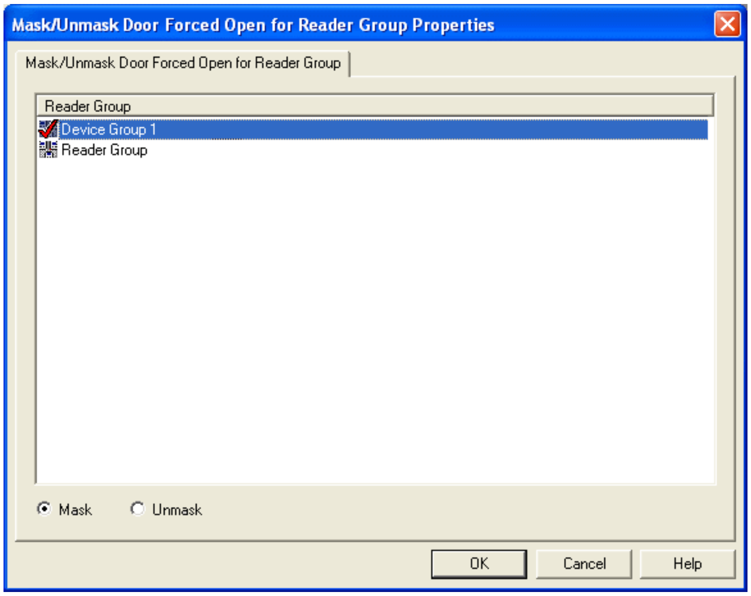
Mask/Unmask Door Forced Open Properties Window Procedures

Add a Mask/Unmask Door Forced Open Action

1. Open the Mask/Unmask Door Forced Open Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) and entry in the Reader/Controller listing window.
3. Do one of the following:
    - Select the **Mask** radio button if you want door forced open alarms for the selected reader to be masked. When door forced open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
    - Select the **Unmask** radio button if you want the door forced open alarms for the selected reader to be unmasked. When door forced open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Forced Open for Reader Group Properties Window

You can display the Mask/Unmask Door Forced Open for Reader Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.


Mask/Unmask Door Forced Open for Reader Group Properties
Mask/Unmask Door Forced Open for Reader Group
Reader Group
Device Group 1
Reader Group
● Mask
○ Unmask
OK
Cancel
Help

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Door Forced Open for Reader Group Field Table

Form Element	Comment
Reader Group listing window	Displays a list of available reader groups which have been configured in the system.
Mask	When configuring a mask/unmask door forced open for reader group action, select this radio button if you want the door forced open alarms to be masked. When door forced open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	When configuring a mask/unmask door forced open for reader group action, select this radio button if you want the door forced open alarms to be unmasked. When door forced open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	Click this button to add the action and exit out of the Mask/Unmask Door Forced Open for Reader Group Properties window.
Cancel	Click this button to exit the Mask/Unmask Door Forced Open for Reader Group Properties window without adding the action.
Help	Click this button to display online help for this window.

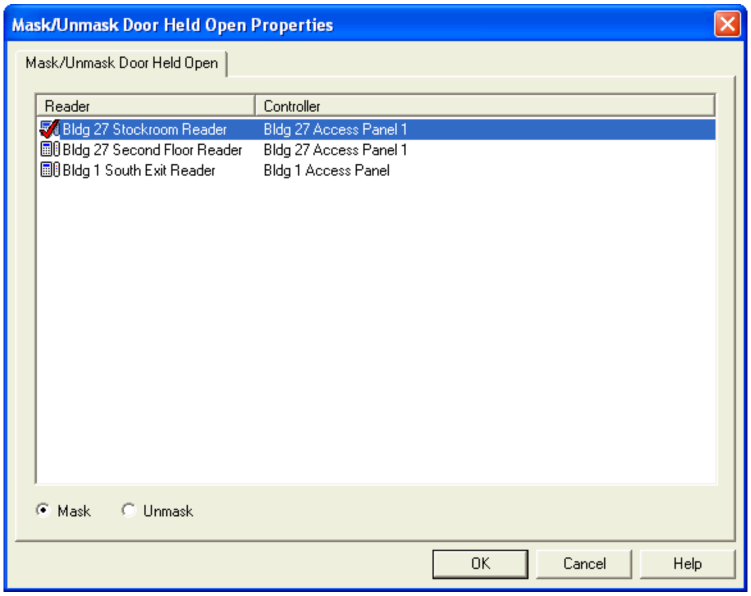
Mask/Unmask Door Forced Open for Reader Group Properties Window Procedures

Add a Mask/Unmask Door Forced Open for Reader Group Action

1. Open the Mask/Unmask Door Forced Open for Reader Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) and entry in the Reader Group listing window.
3. Do one of the following:
   - Select the **Mask** radio button if you want door forced open alarms for the selected reader group to be masked. When door forced open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the door forced open alarms for the selected reader group to be unmasked. When door forced open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Held Open Properties Window

You can display the Mask/Unmask Door Held Open Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Mask/Unmask Door Held Open Properties
Mask/Unmask Door Held Open
OK
Cancel
Help

Reader	Controller
☑ Bldg 27 Stockroom Reader	Bldg 27 Access Panel 1
Bldg 27 Second Floor Reader	Bldg 27 Access Panel 1
Bldg 1 South Exit Reader	Bldg 1 Access Panel

● Mask ○ Unmask

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Door Held Open Properties Window Field Table

Form Element	Comment
Reader/Controller listing window	Displays a list of available readers which have been configured in the system and the controllers that are associated with each.
Mask	When configuring a mask/unmask door held open action, select this radio button if you want the door held open alarm to be masked. When door held open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	When configuring a mask/unmask door held open action, select this radio button if you want the door held open alarm to be unmasked. When door held open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	Click this button to add the action and exit out of the Mask/Unmask Door Held Open Properties window.
Cancel	Click this button to exit the Mask/Unmask Door Held Open Properties window without adding the action.
Help	Click this button to display online help for this window.

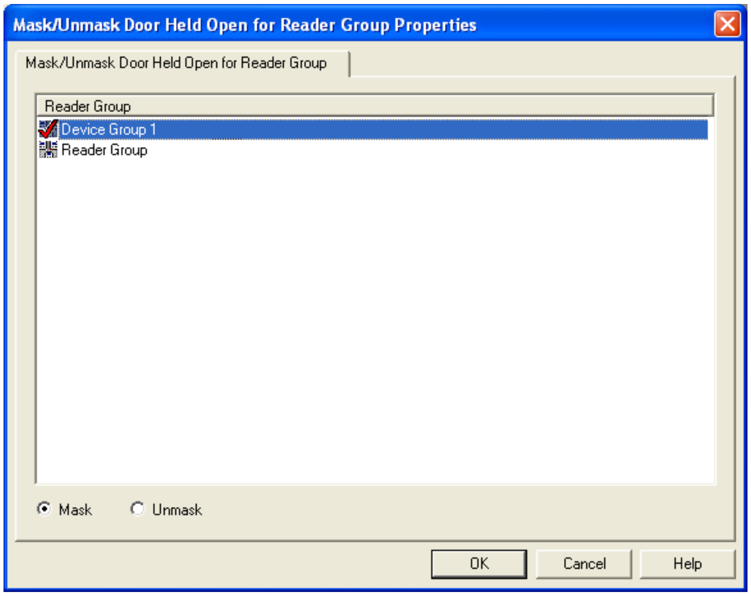
Mask/Unmask Door Held Open Properties Window Procedures

Add a Mask/Unmask Door Held Open Action

1. Open the Mask/Unmask Door Held Open Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) and entry in the Reader/Controller listing window.
3. Do one of the following:
   - Select the **Mask** radio button if you want door held open alarms for the selected reader to be masked. When door held open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the door held open alarms for the selected reader to be unmasked. When door held open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Mask/Unmask Door Held Open for Reader Group Properties Window

You can display the Mask/Unmask Door Held Open for Reader Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.


Mask/Unmask Door Held Open for Reader Group Properties
Mask/Unmask Door Held Open for Reader Group
Reader Group
Device Group 1
Reader Group
● Mask
○ Unmask
OK
Cancel
Help

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Mask/Unmask Door Held Open for Reader Group Field Table

Form Element	Comment
Reader Group listing window	Displays a list of available reader groups which have been configured in the system.
Mask	When configuring a mask/unmask door held open for reader group action, select this radio button if you want the door held open alarms to be masked. When door held open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
Unmask	When configuring a mask/unmask door held open for reader group action, select this radio button if you want the door held open alarms to be unmasked. When door held open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
OK	Click this button to add the action and exit out of the Mask/Unmask Door Held Open for Reader Group Properties window.
Cancel	Click this button to exit the Mask/Unmask Door Held Open for Reader Group Properties window without adding the action.
Help	Click this button to display online help for this window.

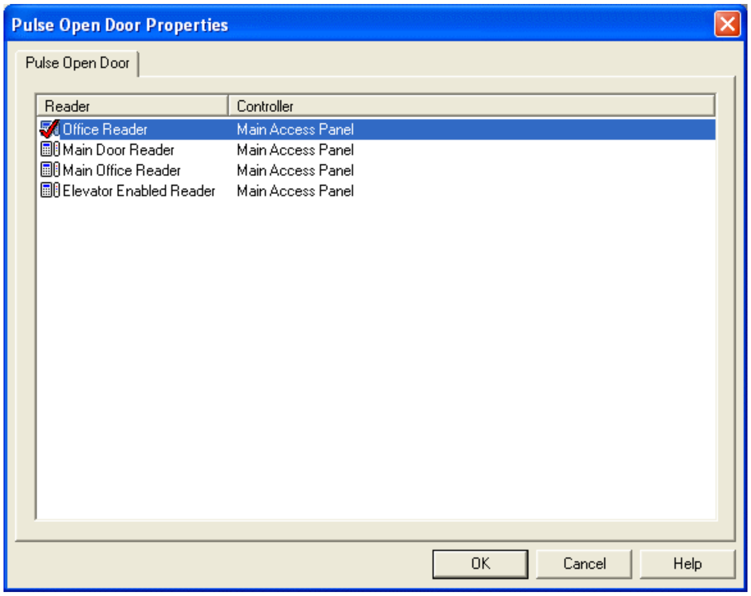
Mask/Unmask Door Held Open for Reader Group Properties Window Procedures

Add a Mask/Unmask Door Held Open for Reader Group Action

1. Open the Mask/Unmask Door Held Open for Reader Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. From the Reader Group listing window, click on an entry to select it.
3. Do one of the following:
   - Select the **Mask** radio button if you want door held open alarms for the selected reader group to be masked. When door held open alarms are masked, they are not reported to the Alarm Monitoring application or stored in the database for later event reporting.
   - Select the **Unmask** radio button if you want the door held open alarms for the selected reader group to be unmasked. When door held open alarms are unmasked, they are reported to the Alarm Monitoring application and are stored in the database for later event reporting.
4. Click [OK].

Pulse Open Door Properties Window

You can display the Pulse Open Door Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Reader	Controller
✓ Office Reader	Main Access Panel
Main Door Reader	Main Access Panel
Main Office Reader	Main Access Panel
Elevator Enabled Reader	Main Access Panel

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Pulse Open Door Properties Window Field Table

Form Element	Comment
Reader/controller listing window	Displays a list of available readers which have been configured in the system and the controllers that are associated with each.
OK	Click this button to add the action and exit out of the Pulse Open Door Properties window.
Cancel	Click this button to exit the Pulse Open Door Properties window without adding the action.
Help	Click this button to display online help for this window.

Pulse Open Door Properties Window Procedures

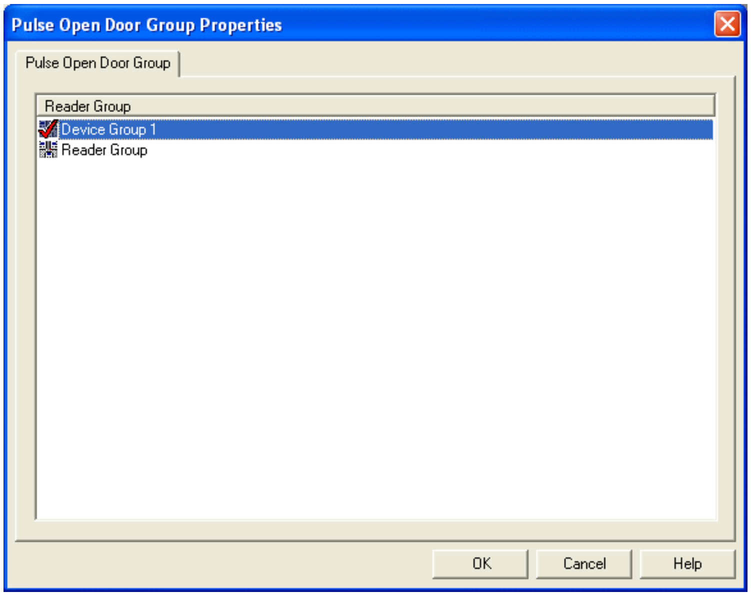
Add a Pulse Open Door Action

Note: The open door commands will not be available for those using Schlage Wireless Access readers, because those types of readers are not in constant communication with the PIM device. For more information, refer to “Action Groups Overview” in the Action Group Library Folder chapter in the System Administration User Guide.

1. Open the Pulse Open Door Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) and entry in the listing window.
3. Click [OK]. The pulse open door action (the door opens and then closes) is now configured for the selected reader.

Pulse Open Door Group Properties Window

You can display the Pulse Open Door Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Pulse Open Door Group Properties Window Field Table

Form Element	Comment
Reader Group listing window	Displays a list of available readers groups which have been configured in the system.
OK	Click this button to add the action and exit out of the Pulse Open Door Group Properties window.
Cancel	Click this button to exit the Pulse Open Door Group Properties window without adding the action.
Help	Click this button to display online help for this window.

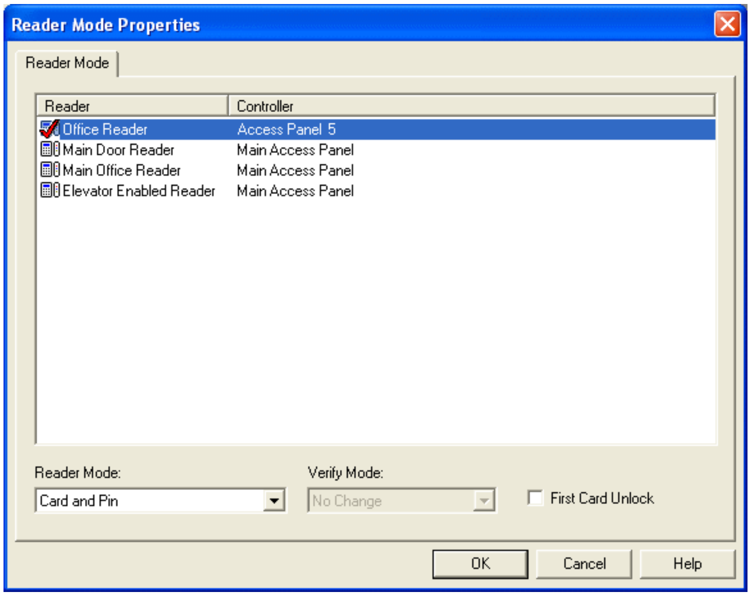
Pulse Open Door Group Properties Window Procedures

Add a Pulse Open Door Group Action

1. Open the Pulse Open Door Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) and entry in the Reader Group listing window.
3. Click [OK]. The pulse open door group action (the doors open and then close) is now configured for the selected reader.

Reader Mode Properties Window

You can display the Reader Mode Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Reader	Controller
✓ Office Reader	Access Panel 5
Main Door Reader	Main Access Panel
Main Office Reader	Main Access Panel
Elevator Enabled Reader	Main Access Panel

Reader Mode: Card and Pin

Verify Mode: No Change

□ First Card Unlock

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Reader Mode Form Properties Window Table

Form Element	Comment
Reader/Controller listing window	Displays a list of available readers which have been configured in the system and the controllers that are associated with each.
Reader Mode	When configuring a reader mode action, select a mode from this drop-down list. Choices include: • Card Only • Facility Code Only • Locked • Card and Pin • Pin or Card • Unlocked • Default Reader Mode - Used to return a reader to its default online access mode.
Verify Mode	When configuring a reader mode action for a reader on a Bosch controller that is a primary reader to an alternate biometric reader, you can select a verify mode. When verify mode is enabled, for alternate reader support, the primary reader will ask for verification from the alternate reader. When configuring a reader mode action for a reader that is not a primary reader to an alternate biometric reader, this field is disabled.
First Card Unlock	Select this check box if you want the reader mode action to be that first card unlock mode is enabled. Doors configured with first card unlock will not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., card only, card and pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will have to present their card. Once access is granted, the reader mode will change to unlocked. This feature is useful for days like “snow days” when employees can’t make it to work on time. **Note:** If the reader is in “Facility code only” mode, the first card unlock feature does not work.
OK	Click this button to add the action and exit out of the Reader Mode Properties window.
Cancel	Click this button to exit the Reader Mode Properties window without adding the action.
Help	Click this button to display online help for this window.

Reader Mode Properties Window Procedures

Add a Reader Mode Action

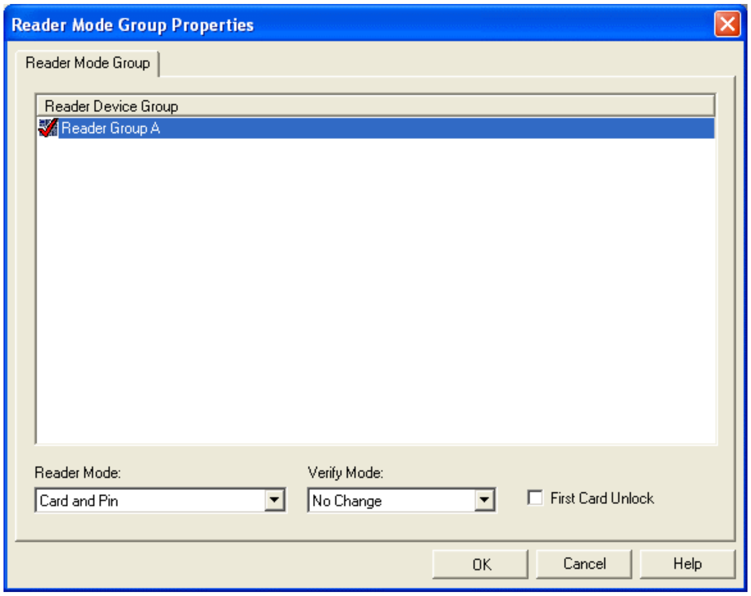
1. Open the Reader Mode Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more

information, refer to Open an Action Properties Window on page 331.

2. Select (place a checkmark beside) an entry in the Reader/Controller listing window.
3. From the **Reader Mode** drop-down list, select a reader mode for the selected reader/controller.
4. When configuring a reader mode action for a reader on a Bosch controller that is a primary reader to an alternate biometric reader, you can select a **Verify Mode**. When verify mode is enabled, for alternate reader support, the primary reader will ask for verification from the alternate reader.
5. Select the **First Card Unlock** check box if you want this reader mode action to enable first card unlock.
6. Click [OK].

Reader Mode Group Properties Window

You can display the Reader Mode Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



☑ Reader Group A

Reader Mode: Card and Pin

Verify Mode: No Change

□ First Card Unlock

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Reader Mode Group Properties Window Field Table

Form Element	Comment
Reader Device Group listing window	Displays a list of available reader groups which have been configured in the system.
Reader Mode	When configuring a reader mode action, select a mode from this drop-down list. Choices include: • Card Only • Facility Code Only • Locked • Card and Pin • Pin or Card • Unlocked • Default Reader Mode - Used to return a reader to its default online access mode.
Verify Mode	When configuring a reader mode group action for a group of readers on a Bosch controller that are primary readers to alternate biometric readers, you can select a verify mode. When verify mode is enabled, for alternate reader support, the primary reader will ask for verification from the alternate reader. When configuring a reader mode group action for readers that are not primary readers alternate biometric readers, this field is disabled.
First Card Unlock	Select this check box if you want the reader mode group action to be that first card unlock mode is enabled. Doors configured with first card unlock will not unlock until valid personnel arrives. For example, rather than setting a lobby door to unlock at 9:00 am, you can leave it in a secure mode (i.e., card only, card and pin, etc.) and set the first card unlock to 9:00 am. The first person that comes in the door after 9:00 am will have to present their card. Once access is granted, the reader mode will change to unlocked. This feature is useful for days like “snow days” when employees can’t make it to work on time. **Note:** If the reader is in “Facility code only” mode, the first card unlock feature does not work.
OK	Click this button to add the action and exit out of the Reader Mode Group Properties window.
Cancel	Click this button to exit the Reader Mode Group Properties window without adding the action.
Help	Click this button to display online help for this window.

Reader Mode Group Properties Window Procedures

Add a Reader Mode Group Action

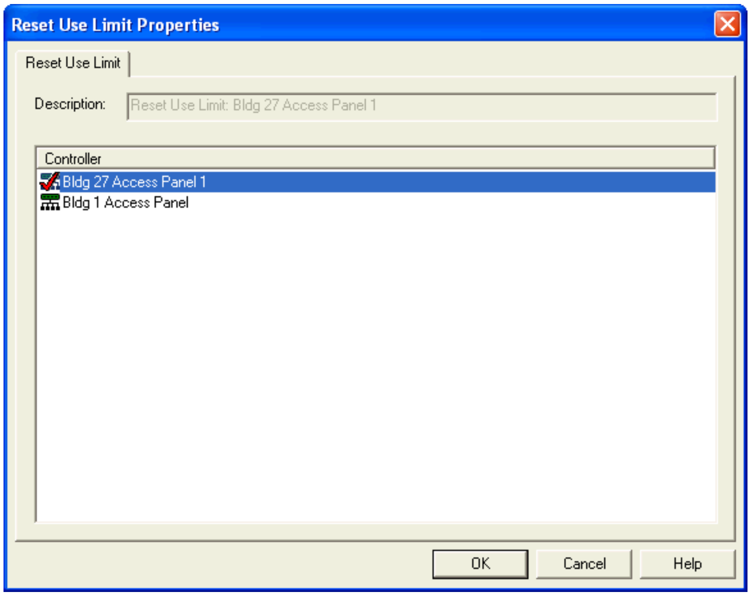
1. Open the Reader Mode Group Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on

page 331.

2. Select (place a checkmark beside) and entry in the Reader Device Group listing window.
3. From the **Reader Mode** drop-down list, select a reader mode for the selected reader group.
4. When configuring a reader mode group action for readers on a Bosch controller that are primary readers to alternate biometric readers, you can select a **Verify Mode**. When verify mode is enabled, for alternate reader support, the primary reader will ask for verification from the alternate reader.
5. Select the **First Card Unlock** check box if you want this reader mode group action to enable first card unlock.
6. Click [OK].

Reset Use Limit Properties Window

You can display the Reset Use Limit Properties window using the Action Group Library, Scheduler, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Description: Reset Use Limit: Bldg 27 Access Panel 1

Controller
✓ Bldg 27 Access Panel 1
Bldg 1 Access Panel

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Reset Use Limit Form Properties Window Table

Form Element	Comment
Description	When one controller is selected in the listing window, displays the text “Reset Use Limit:” followed by the controller name. For example, “Reset Use Limit: Front Door Bldg 1.” When more than one controller is selected in the listing window, this field is activated. Type in a descriptive name to identify the selected group of controllers.
Controller listing window	Displays a list of available controllers.
OK	Click this button to add the reset use limit action for the selected controller(s) and exit out of the Reset Use Limit Properties window. **Note:** Each time a use-limited badge is used at a reader, the badge’s use limit is decremented for the associated controller. A cardholder’s use limit is specified on the Badge form of the Cardholders folder. Whenever the cardholder swipes their badge at a reader where use limits are enforced, the cardholder’s use limit is reduced by one (1). When the use count reaches zero (0), the cardholder is unable to access use limit-enforced card readers on that controller.
Cancel	Click this button to exit the Reset Use Limit Properties window without adding the action.
Help	Click this button to display online help for this window.

Reset Use Limit Properties Window Procedures

Add a Reset Use Limit Action

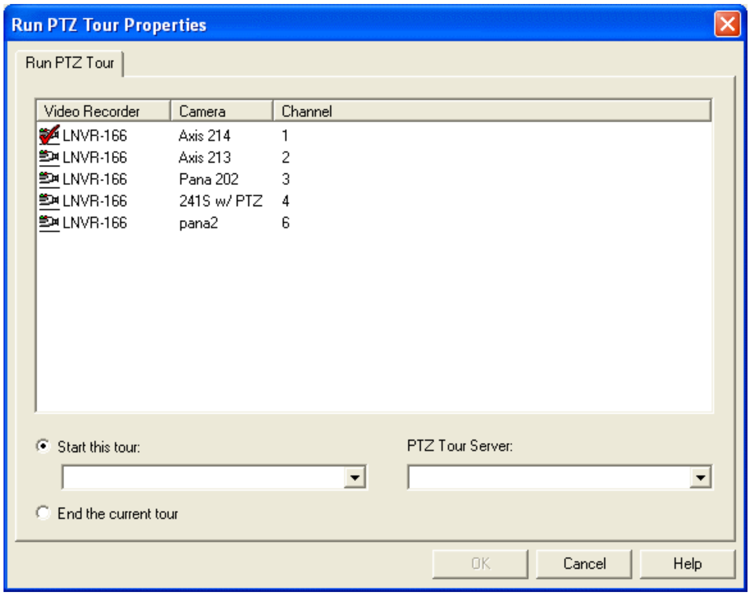
1. Open the Reset Use Limit Properties window using the Action Group Library, Scheduler, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) one or more controller from the listing window.
3. If you selected one controller from the listing window, skip this step. If you selected more than one controller from the listing window, type a descriptive name to identify the selected group of controllers in the **Description** field.
4. Click [OK].

Run PTZ Tour Properties Window

The Run PTZ Tour action type allows the user to start or end a continuous background PTZ tour. To use this action, a PTZ Tour Server must be configured in System Administration and a PTZ tour must be created in Alarm Monitoring.

Background PTZ tours can be interrupted by a user with a higher priority or by the user that started the tour. If a background PTZ tour is interrupted by the user that started it, the tour may fail to stop and control may not become available to the user. This issue will occur for any user of the same priority as the user who created the tour. In order for this not to occur, the user who creates the tour must have a priority lower than that of any user wishing to interrupt it.

You can open the Run PTZ Tour Action window using Scheduler or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Video Recorder	Camera	Channel
✓ LNVR-166	Axis 214	1
LNVR-166	Axis 213	2
LNVR-166	Pana 202	3
LNVR-166	241S w/ PTZ	4
LNVR-166	pana2	6

● Start this tour:

PTZ Tour Server:

○ End the current tour

Form Element	Comment
Listing window	To display only PTZ cameras, add the following line to the **ACS.INI** file in the `[DigitalVideo]` section: `TestForPTZOnStartUp=1`
Start this tour	To begin a tour, select the radio button and choose a tour from the drop-down list.
PTZ Tour Server	Select the PTZ tour server that should run this tour.
End the current tour	Select this radio button to stop a tour that is currently running on the selected camera.

Run PTZ Tour Properties Window Procedures

Add a Run PTZ Tour Action

1. Open the Run PTZ Tour Action window using the Scheduler or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) the camera from the listing window.
3. To start a tour:
   a. Select the **Start this tour** radio button and select the tour from the drop-down list.
   b. Select the server to run the tour from the **PTZ Tour Server** drop-down list.

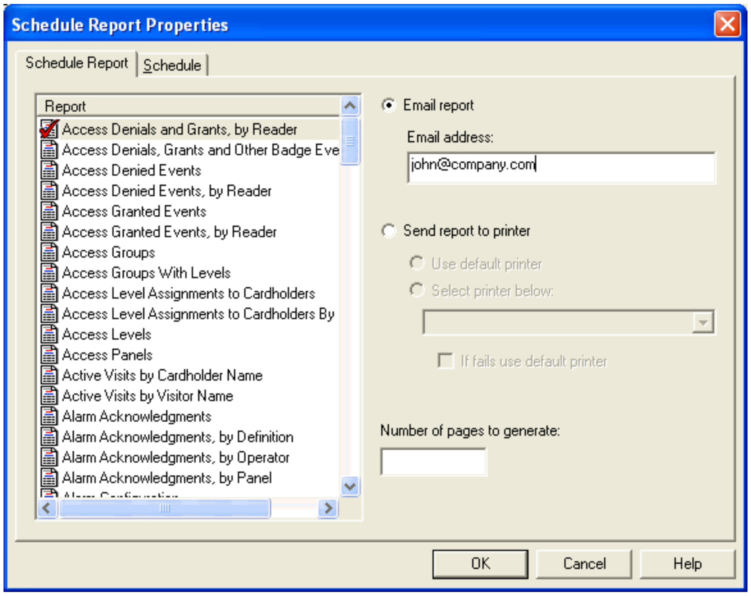
Note: Separate actions must be added to start and to end a PTZ tour. To end a tour, select the **End the current tour** radio button.

4. Click [OK].

Schedule Report Properties Window

The Schedule Report action type allows the user to either print a report or send a report in an email.

You can open the Schedule Report action window using Scheduler or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Access Denials and Grants, by Reader
Access Denials, Grants and Other Badge Eve
Access Denied Events
Access Denied Events, by Reader
Access Granted Events
Access Granted Events, by Reader
Access Groups
Access Groups With Levels
Access Level Assignments to Cardholders
Access Level Assignments to Cardholders By
Access Levels
Access Panels
Active Visits by Cardholder Name
Active Visits by Visitor Name
Alarm Acknowledgments
Alarm Acknowledgments, by Definition
Alarm Acknowledgments, by Operator
Alarm Acknowledgments, by Panel

● Email report

Email address: john@company.com

○ Send report to printer

○ Use default printer

○ Select printer below:

□ If fails use default printer

Number of pages to generate:

Form Element	Comment
Report listing window	Displays a list of available reports.
Email report	Select this radio button if you want the scheduled report to be sent in an email. E-mail notification requires the GOS module to be configured and running. For more information, refer to the Global Output Devices Folder chapter in the System Administration User Guide.
Email address	Enter the email address where the scheduled report is to be sent.
Send Report to printer	Select this radio button if you want the scheduled report to print.
Use default printer	Select this radio button if you want the scheduled report to print from the workstation’s default printer.
Select printer below	Select this radio button and choose a printer from the drop-down list if you want the scheduled report to print to a printer other than the workstation’s default printer. **Note:** The choices in the drop-down list are printers that are available for the computer running the linkage server and not for the workstation that the action is being configured on.

Form Element	Comment
If fails use default printer	If you selected the **Select printer below** radio button, select this check box if you want to print from the default printer if the selected printer does not exist. **Note:** Due to a limitation of Crystal Reports this setting is not enforced if the printer exists but is not accessible under the linkage server account. When this occurs the report will automatically be printed from the default printer regardless of this setting. For more information, refer to Request Print Action Flowchart on page 404.
Number or pages to generate	When configuring a scheduled report action, you can enter the number of pages that you want the report to have. This can be helpful when only a small section of a large report is needed.

Schedule Report Properties Window Procedures

Add a Schedule Report Action

1. Open the Schedule Report Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select the report from the listing window.
3. Select whether the report is to be printed or sent in an email.
   - If the report is being sent in an email, select the **Email report** radio button and add an email address to the **Email Address** field.

Important: E-mail notification requires the GOS module to be configured and running. For more information, refer to the Global Output Devices Folder chapter in the System Administration User Guide.

   - If the report is being printed, select the **Send report to printer** radio button and select the printer to be used.
4. Select how many pages will be sent in an email or printed by entering a number in the **Number of pages to generate** field.
5. Click [OK].

Important: The Scheduled Report Action will not run unless the user who creates the action has an internal account. This is because the user account that creates the action is used to generate the report, and might not be configured for Single Sign-on at every workstation.

Request Print Action Flowchart

This flowchart shows how a report may get printed from the default printer although the **If fails use default printer** check box is NOT selected in the Report Print Properties window.

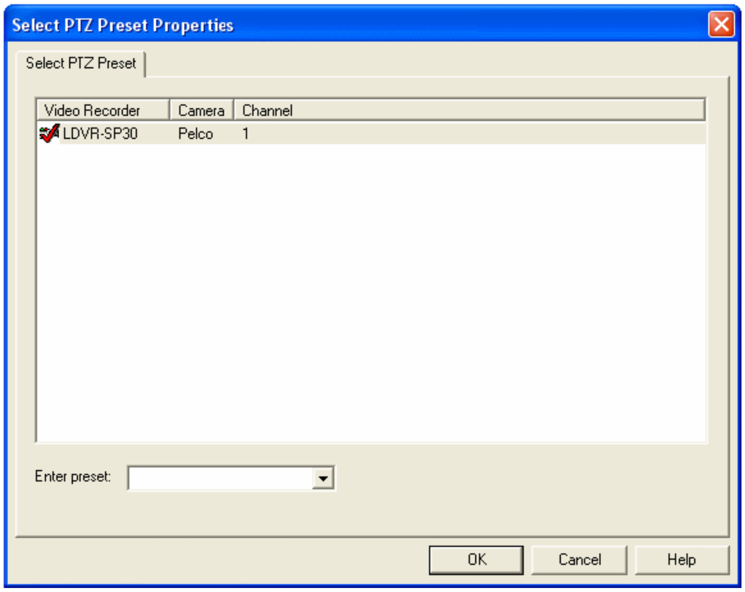
Select PTZ Preset Properties Window

The Select PTZ Preset action type allows users to select a preset for a PTZ camera to move to when the action is executed.

Notes: The camera must be online when you configure the action.

The camera must be online when the action executes.

You can display the Select PTZ Preset Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Video Recorder	Camera	Channel
LDVR-SP30	Pelco	1

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Form Element	Comment
Listing window	To display only PTZ cameras, add the following line to the **ACS.INI** file in the `[DigitalVideo]` section: `TestForPTZOnStartUp=1` **Note:** The camera must be online when you configure the action and the camera must be online when the action executes.
Enter preset	Enter the camera side preset number or select a client side preset from the drop-down list.

Select PTZ Preset Properties Window Procedures

Add a Select PTZ Preset Action

1. Open the Select PTZ Preset Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Select (place a checkmark beside) the video recorder/camera/channel option from the listing window.

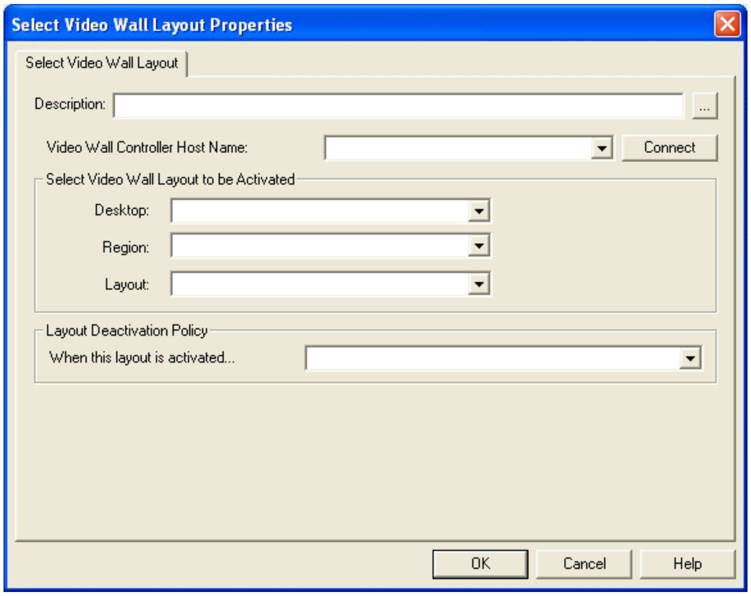
Note: The camera must be online when you configure the action and the camera must be online when the action executes.

3. Enter a camera side preset value or select a client side preset from the drop-down list.
4. Click [OK].

Select Video Wall Layout Properties Window

The Select Video Wall Layout action type allows users to activate and deactivate pre-configured layouts on the Barco video wall. Before this action is configured, video wall layouts must be defined using external software such as the Barco Apollo Explorer.

You can display the Select Video Wall Layout Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.


Select Video Wall Layout Properties
Select Video Wall Layout
Description:
...
Video Wall Controller Host Name:
Connect
Select Video Wall Layout to be Activated
Desktop:
Region:
Layout:
Layout Deactivation Policy
When this layout is activated...
OK
Cancel
Help

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Select Video Wall Layout Properties Window Field Table

Form Element	Comment
Description	A descriptive name for the action. After the Select Video Wall Layout to be Activate section of the dialog is configured, [...] can be used to automatically generate a name based on the controller, desktop, region, and layout names.
Video Wall Controller Host Name	Host name or IP address of the Barco Apollo server that controls the video wall. The drop-down list is populated by controller names that have been configured in other instances of the Select Video Wall Layout action.
Connect	Click to retrieve video wall layout information from the video wall controller to populate the drop-down lists in the Select Video Wall Layout to be Activated section.
Desktop	Identifies which physical video wall is being configured.
Region	If regions are enabled on the video wall, select one from the **Region** drop-down list. **Note:** Regions are used to logically separate content so that multiple users can work in parallel without affecting each other.
Layout	Identifies the layout to be activated by the action. Layouts are configured in the Barco Apollo Explorer.

Select Video Wall Layout Properties Window Field Table

Form Element	Comment
When this layout is activated...	Specifies the policy for deactivation of a layout that may be already active on the video wall. • Deactivate All Layouts - Deactivates all layouts that are active on the video wall regardless of region. • Deactivate Layouts in the Current Region - Deactivates layouts that are active in the region indicated in the **Region** drop-down list. • Do Not Deactivate Any Layouts - Adds the new layout without deactivating any currently active layouts.

Select Video Wall Layout Properties Window Procedures

Add a Select Video Wall Layout Action

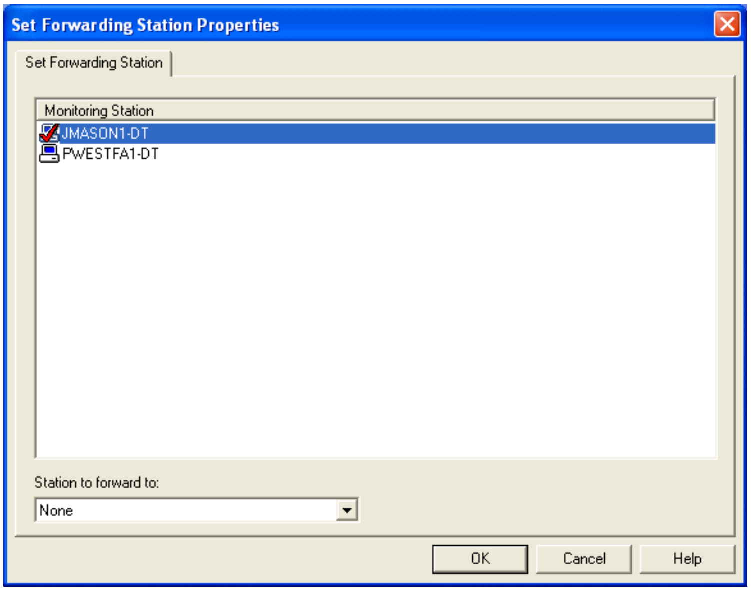
Before configuring this action, the video wall must be fully configured. For more information, refer to the Digital Video Hardware User Guide

1. Open the Select Video Wall Layout Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Enter the host name or IP address of the Barco Apollo server that controls the video wall in the **Video Wall Controller Host Name** field or select a controller from the drop-down list.
3. Select the **Desktop** name from the drop-down list.
4. If your Barco configuration utilizes regions, select the appropriate one from the **Region** drop-down list.
5. Select the **Layout** to activate from the drop-down list.
6. Specify the Layout Deactivation Policy by selecting an action for currently active layouts from the **When this layout is activated...** drop-down list.
   - Deactivate All Layouts - Deactivates all layouts that are active on the video wall regardless of region.
   - Deactivate Layouts in the Current Region - Deactivates layouts that are active in the region indicated in the **Region** drop-down list.
   - Do Not Deactivate Any Layouts - Adds the new layout without deactivating any currently active layouts.
7. Enter a descriptive name for the action or use [...] to generate a name for the **Description** field based on the selected desktop, region, and layout names.
8. Click [OK] to save the action.

Set Forwarding Station Properties Window

The Set Forwarding Station action allows you to change where a monitor station forwards its alarms. Using this action allows a monitor station to be configured to forward its alarms to a different monitoring station.

Note: The action is only valid for a scheduler invocation.



Monitoring Station

JMASON1-DT

PWESTFA1-DT

Station to forward to: None

Set Forwarding Station Properties Window Field Table

Form Element	Comment
Monitor Station listing window	Lists the monitoring stations available. Select the monitoring station that is having its alarms forwarded.
Station to forward to	Select the monitor station you would like the alarms forwarded to.
OK	Click this button to add the action and exit out of the Set Forwarding Station properties window.
Cancel	Click this button to exit the Set Forwarding Station properties window without adding the action.
Help	Click this button to display online help for this window.

Set Forwarding Station Properties Window Procedures

Add a Set Forwarding Station Action

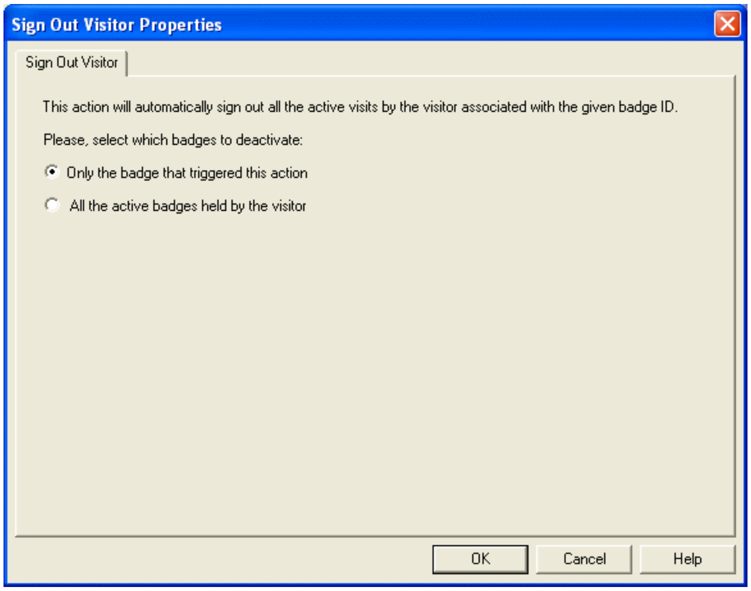
1. Open the Set Forwarding Station Properties window, using Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Choose the monitor station in the **Monitoring Station** list window. This will be the monitor station that has its alarms forwarded to another monitoring station.
3. In the **Station to forward to** drop-down box, choose the monitoring station that the alarms will be forwarded to.
4. Click [OK].

Sign Out Visitor Properties Window

The Sign Out Visitor action allows you to deactivate the badges of cardholders who have signed out of the system. You can further modify this action by choosing which of the cardholder's badges will be signed out, just the badge that triggered the action or all badges belonging to that cardholder.

You can display the Sign Out Visitor Properties window using Global I/O. For more information, refer to Open an Action Properties Window on page 331.

Note: In segmented systems, the Sign Out Visitor Properties action must be applied to all segments.



This action will automatically sign out all the active visits by the visitor associated with the given badge ID.

Please, select which badges to deactivate:

● Only the badge that triggered this action

○ All the active badges held by the visitor

Sign Out Visitor Properties Window Field Table

Form Element	Comment
Only the badge that triggered this action	Select if you want to deactivate only the badge that caused the visitor to sign out.
All the active badges held by the visitor	Select if you want all the badges belonging to the visitor to deactivate once the visitor is signed out.
OK	Click this button to add the action and exit out of the Sign Out Visitor properties window.
Cancel	Click this button to exit the Sign Out Visitor properties window without adding the action.
Help	Click this button to display online help for this window.

Sign Out Visitor Properties Window Procedures

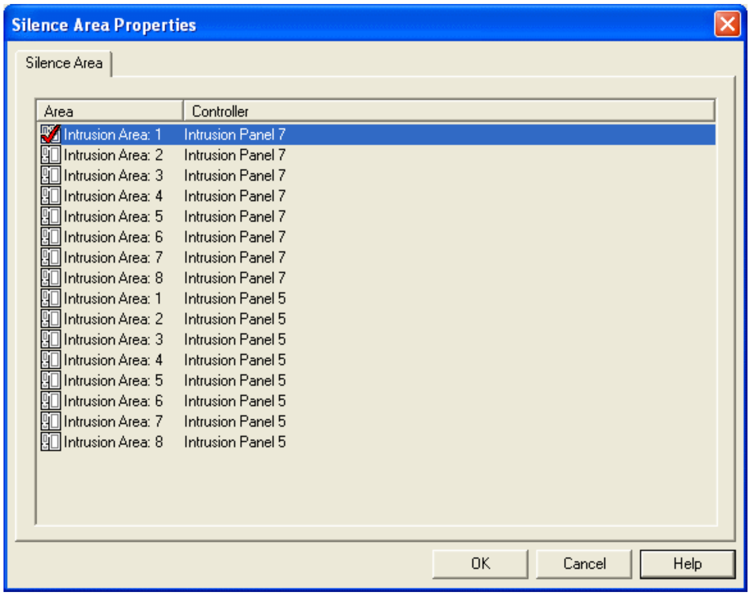
Add a Sign Out Visitor Action

1. Open the Sign Out Visitor Properties window, using Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. Choose the options that suit your needs.
3. Click [OK].

Silence Area Properties Window

The Silence Area action allows an area (that uses a Bosch intrusion panel) to be silenced during an alarm from that panel.

You can display the Silence Area Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.



Area	Controller
☑ Intrusion Area: 1	Intrusion Panel 7
Intrusion Area: 2	Intrusion Panel 7
Intrusion Area: 3	Intrusion Panel 7
Intrusion Area: 4	Intrusion Panel 7
Intrusion Area: 5	Intrusion Panel 7
Intrusion Area: 6	Intrusion Panel 7
Intrusion Area: 7	Intrusion Panel 7
Intrusion Area: 8	Intrusion Panel 7
Intrusion Area: 1	Intrusion Panel 5
Intrusion Area: 2	Intrusion Panel 5
Intrusion Area: 3	Intrusion Panel 5
Intrusion Area: 4	Intrusion Panel 5
Intrusion Area: 5	Intrusion Panel 5
Intrusion Area: 6	Intrusion Panel 5
Intrusion Area: 7	Intrusion Panel 5
Intrusion Area: 8	Intrusion Panel 5

Note: If you have accessed this window via the Scheduler folder, the window will also contain the Schedule tab. For more information, refer to Chapter 20: Scheduler Folder on page 317.

Silence Area Properties Window Field Table

Form Element	Comment
Listing window	Lists currently enabled intrusion areas. Intrusion areas are configured on the Areas form in the Intrusion Detection Configuration folder.
OK	Click this button to add the action and exit out of the Silence Area Properties window.
Cancel	Click this button to exit the Silence Area Properties window without adding the action.
Help	Click this button to display online help for this window.

Silence Area Properties Window Procedures

Add a Silence Area Action

1. Open the Silence Area Properties window using the Action Group Library, Scheduler, Guard Tour, Acknowledgment Actions, or Global I/O. For more information, refer to Open an Action Properties Window on page 331.
2. From the listing window, click on an entry to select it. The area you selected will now be silenced during an alarm from that panel.

Important: The silence area action can only be used with Bosch intrusion panels.

3. Click [OK].
4.

Appendix B: Alarm/Event Descriptions

Alarm	Event	Event Type	Description	Duress*
24 Hour Alarm	24 Hour Alarm	Trouble	A 24 hour alarm condition has been detected.	
24 Hour Alarm Restore	24 Hour Alarm Restore	Trouble	A 24 hour alarm condition has been restored.	
24 Hour Auto Test	24 Hour Auto Test	Trouble		
24 Hour Non-Burglary Alarm	24 Hour Non-Burglary Alarm	Trouble	A 24 hour non-burglary alarm condition has been detected.	
24 Hour Report Closed	24 Hour Report Closed	Trouble	A 24 Hour report on a closed zone	
24 Hour Report Open	24 Hour Report Open	Trouble	A 24 Hour report on an open zone	
24 Hour Zone Bypassed	24 Hour Zone Bypassed	Trouble	A 24 hour zone has been bypassed.	
24 Hour Zone Unbypassed	24 Hour Zone Unbypassed	Trouble	A 24 hour zone has been unbypassed.	
30 Minutes Since Fallback Command	30 Minutes Since Fallback Command	Trouble	30 minutes have passed since fallback command.	
32 Hour Event Log Marker	32 Hour Event Log Marker	System		
Abort	Abort	System	An event message was not sent due to User action	
AC Restore	AC Restore	System	AC power trouble has been restored.	
AC Trouble	AC Trouble	System	An AC power trouble condition has been detected.	
Accepted Biometric Score	Accepted Biometric Score	Biometric	This event returns the accepted biometric score. The actual access granted event is sent separately. This event is mainly used for diagnostic purposes.	
Access Closed	Access Closed	Denied	Access for all users prohibited.	
Access Code Used	Access Code Used	Denied	Access code was used.	
Access Denied	Access Denied	Denied	Access was denied.	

Alarm	Event	Event Type	Description	Duress*
Access Denied to Destination Floor	Access Denied to Destination Floor	Denied	Generated when a card was presented to a reader associated with an elevator terminal but the elevator assignment was not performed; used when elevator dispatching devices are present.	
Access Denied: Access Control Format Not Found	Access Denied: Access Control Format Not Found	Denied	Generated when there are no ACFs (Access Control Formats) stored at the lock.	
Access Denied: Area Empty	Access Denied	Denied	An event indicating that access was denied due to the room being empty.	Yes
Access Denied: Area Occupied	Access Denied	Denied	An event indicating that access was denied due to the room being empty.	Yes
Access Denied: Asset Required	Access Denied	Denied	An event indicating that access was denied since no asset was presented for the access attempt.	Yes
Access Denied: Biometric Reader Offline	Access Denied: Biometric Reader Offline	Denied	Generated when the alternate biometric reader could not be contacted for verification (was offline).	Yes
Access Denied: Card Expired	Access Denied: Card Expired	Denied	Card has expired.	
Access Denied: Escort Timeout Expired	Access Denied: Escort Timeout Expired	Denied	This event indicates that access was denied because a person requiring an escort attempted access but an escort did not present their credentials in the time period.	Yes
Access Denied: Door Secured	Access Denied: Door Secured	Denied	Access denied because door was secured.	
Access Denied: Interlock	Access Denied: Interlock	Denied	An access request was denied because the doors associated Interlock point is open.	
Access Denied: Invalid Access Control Data	Access Denied: Invalid Access Control Data	Denied	Failed to process Integra card data.	

Alarm	Event	Event Type	Description	Duress*
Access Denied: Invalid Access Control Data Length	Access Denied: Invalid Access Control Data Length	Denied	The length of the retrieved data did not match the length specified in selected ACF (Access Control Format).	
Access Denied: Invalid Access Control Data Parity	Access Denied: Invalid Access Control Data Parity	Denied	Parity calculations for retrieved data failed for selected ACF (Access Control Format).	
Access Denied: Invalid Access Control Data Type	Access Denied: Invalid Access Control Data Type	Denied	The type of retrieved data (Wiegand/Integra) did not match the ACF (Access Control Format) type.	
Access Denied: Invalid Smart Card Authentication	Access Denied: Invalid Smart Card Authentication	Denied	Failed to authenticate to the application specified by the selected SCF (Smart Card Format).	
Access Denied: Invalid Smart Card Data	Access Denied: Invalid Smart Card Data	Denied	Failed to retrieve HID application data; invalid header, invalid data length.	
Access Denied: Invalid Smart Card Location	Access Denied: Invalid Smart Card Location	Denied	Application data could not be located on the card based on the selected SCF (Smart Card Format).	
Access Denied: Invalid Smart Card Type	Access Denied: Invalid Smart Card Type	Denied	Either the card was not found in the field or the card failed to respond to the requested RF (Radio Frequency) protocol.	
Access Denied: No Biometric Template	Access Denied: No Biometric Template	Denied	Generated when the cardholder did not have a biometric template loaded in the database, so a verification could not be done.	Yes
Access Denied: No Occupant Approval	Access Denied: No Occupant Approval	Denied	An event indicating that access was denied due to no occupant approval.	Yes
Access Denied: Passback	Access Denied: Passback	Denied	Access was denied because the credential has not exited the area before attempting to re-enter same area.	
Access Denied: Reader Locked	Access Denied: Reader Locked	Denied	Generated when access was denied because the reader was locked.	Yes

Alarm	Event	Event Type	Description	Duress*
Access Denied: Secured Mode	Access Denied: Secured Mode	Denied	Lock is in secured mode; no users will be allowed access.	
Access Denied: Smart Card Format Not Found	Access Denied: Smart Card Format Not Found	Denied	No SCFs (Smart Card Formats) stored at the lock.	
Access Denied: Unauthorized Arming State	Access Denied: Unauthorized Arming State	Denied	An access request was denied because the user was not authorized in this area when the area was armed.	
Access Denied: Unauthorized Entry Level	Access Denied: Unauthorized Entry Level	Denied	An access request was denied because the user is not authorized in this area.	
Access Denied: Unauthorized Time	Access Denied: Unauthorized Time	Denied	An access request was denied because the request is occurring outside the user's authorized time window(s).	
Access Door Propped	Access Door Propped	System		
Access Door Status Monitor Shunt	Access Door Status Monitor Shunt	System		
Access Door Status Monitor Trouble	Access Door Status Monitor Trouble	System		
Access Granted	Access Granted	Granted	Access was granted.	Yes
Access Granted	Granted Access	Granted	Access was granted.	
Access Granted to Destination Floor	Access Granted to Destination Floor	Granted	Generated when a card was presented to a reader associated with an elevator terminal and the elevator cab assignment was performed; used when elevator dispatching devices are present.	
Access Granted - Entry Made	Access Granted - Entry Made	Granted	Access granted and door opened; used when latch or door sensor monitoring is present.	
Access Granted - No Entry Made	Granted No Entry	Granted	Access was granted but door not opened; used when latch or door sensor monitoring is present.	
Access Granted on Facility Code	Granted Facility Code	Granted	Access was granted based on a valid facility code.	Yes

Alarm	Event	Event Type	Description	Duress*
Access Granted on Facility Code, No Entry Made	Granted Facility Code, No Entry	Granted	Access was granted on facility code but no entry was made at the door.	Yes
Access Granted: Reader Unlocked	Access Granted: Reader Unlocked	Granted	Generated when access was granted because the reader was unlocked.	Yes
Access Granted Under Duress	Access Granted Under Duress	Duress	Indicates that the cardholder was granted access under duress.	Yes
Access Granted Under Duress - No Entry Made	Access Granted Under Duress - No Entry Made	Duress	Access Granted Under Duress - No Entry Made	Yes
Access Level Change	Access Level Change	System		
Access Lockout	Access Lockout	System	Access denied, known code	
Access Open	Access Open	System	Access for authorized users in now allowed	
Access Point Bypass	Access Point Bypass	System		
Access Program Exit	Access Program Exit	System		
Access Relay/Trigger Fail	Access Relay/ Trigger Fail	System		
Access Request to Exit Shunt	Access Request to Exit Shunt	System		
Access Schedule Change	Access Schedule Change	System	The access schedule has changed.	
Access Trouble	Access Trouble	System	An access system trouble condition has been detected.	
Access Zone Shunt	Access Zone Shunt	System	An access zone is put in the shunted state.	
Account Status Failure	Account Status Failure	System		
Account Status Restore	Account Status Restore	System		
Acknowledgment Action Executed	Acknowledgment Action Executed	System	Generated when an alarm is acknowledged and actions associated with the alarm are executed.	
Acknowledgment Action Failed	Acknowledgment Action Failed	System	Generated when there is a failure to execute actions associated with an alarm acknowledgment.	

Alarm	Event	Event Type	Description	Duress*
Activate Output	Activate Output	System		
Activity Resumed	Activity Resumed	System	A zone has detected activity after an alert.	
ACU Firmware Upgraded	ACU Firmware Upgraded	System	Lock firmware was updated.	
Air Flow Loss	Air Flow Loss	Trouble	An air flow loss condition has been detected.	
Air Flow Loss Restore	Air Flow Loss Restore	Trouble	An air flow loss condition has been restored.	
Alarm	Alarm	System		
Alarm Active	Alarm Active	System	Generated when an alarm has become active.	
Alarm Canceled	Alarm Restored	System	A device has come online or an alarm condition has been restored.	
Alarm Mask Group Armed			This event is generated when the alarm mask group is armed.	
Alarm Mask Group Disarmed			This event is generated when the alarm mask group is disarmed.	
Alarm Mask Group Force Armed			This event is generated when the alarm mask group is force armed.	
Alarm Mask Group Mask Count Incremented			This event is generated when a disarm command is issued and the alarm mask group is already disarmed, causing the alarm mask count to get incremented. The alarm mask group will still remain disarmed.	
Alarm Mask Group Mask Count Decremented			This event is generated when an arm or force arm command is issued and the alarm mask group has a mask count greater than 1, causing the mask count to be decremented. The alarm mask group will still remain disarmed.	

Alarm	Event	Event Type	Description	Duress*
Alarm Mask Group Arming Failure, Active Points			The following command is used to indicate an arming failure due to active points. This command should be hard to generate because currently the only way to issue the standard arm command is from the command keypad and this should only be available if there are no active points.	
Alarm Monitoring Action Group Executed	Alarm Monitoring Action Group Executed	System	Generated when the action group is executed.	
Alarm Monitoring Action Group Failed	Alarm Monitoring Action Group Failed	System	Generated when the action group execution fails.	
Alarm Relay Disable	Alarm Relay Disable	System		
Alarm Relay Disable Restored	Alarm Relay Disable Restored	System		
Alarm/Restore	Alarm/Restore	System	Generated when a device has come online or an alarm condition has been restored.	
Alarm Silenced	Alarm Silenced	System		
Alarm Tamper Loop	Alarm Tamper Loop	Trouble		
All Points Tested	All Points Tested	System	All points have been tested.	
All Systems Normal	All Systems Normal	Fire	Generated when the Notifier AM-2020 panel is booted up. This alarm may also be sent when all existing alarm conditions are resolved.	
Analog Restore	Analog Restore	Fire		
Analog Restored	Analog Restored	System		
Analog Service Requested	Analog Service Requested	System		
Analog Service Required	Analog Service Required	Fire	An analog fire sensor needs to be cleaned or calibrated.	
Anti-Passback Violation	Anti-Passback Violation	Area Control	Generated when the cardholder was denied access because the entry would have violated the anti-passback rules for the area.	Yes

Alarm	Event	Event Type	Description	Duress*
Archive Server Failure	Archive Server Failure	Video	Generic error indicating a failure on the archive server. This error indicates that the archive server could not move any more data from the video recorders to the archive server. The user will have to go to the physical archive server computer and review the remote storage application and logs, ReadykeyPRO log files in the ReadykeyPRO\logs directory, and also follow general trouble shooting techniques as outlined in the archive server manual to determine the specific cause of the alarm.	
Archive Server Failure Archive Location Full	Archive Server Failure	Video	This error indicates that the archive location is full and no further data can be moved from the video recorders to the archive server. If this issue is not resolved, it is possible events may be purged before they are archived.	
ARDIS Module Communication Loss	ARDIS Module Communication Loss	Trouble		
ARDIS Module Communication Restored	ARDIS Module Communication Restored	Trouble		
Area Closed	Area Closed	Area Control	Generated when access was denied because the area being entered is closed.	Yes
Area Limit Exceeded	Area Limit Exceeded	Area Control	Generated when access was denied because the area limit would have been exceeded.	Yes
Armed Perimeter Delay	Armed Perimeter Delay	System		
Armed Perimeter Instant	Armed Perimeter Instant	System		
Armed Stay	Armed Stay	System		

Alarm	Event	Event Type	Description	Duress*
Asset Denied - Invalid Access	Asset Denied - Invalid Access	Asset	Generated when the asset was denied because the cardholder had invalid access levels.	Yes
Asset Denied - Invalid Asset	Asset Denied - Invalid Asset	Asset	Generated when the asset was denied because of an invalid asset (the asset was not found in the controller).	Yes
Asset Denied - Invalid Cardholder	Asset Denied - Invalid Cardholder	Asset	Generated when the asset was denied because of an invalid cardholder.	Yes
Asset Denied - No Asset Privileges	Asset Denied - No Asset Privileges	Asset	Generated when the asset was denied because the cardholder had no asset privileges.	
Asset Granted - Asset Owner	Asset Granted - Asset Owner	Asset	Generated when the asset was granted because the cardholder was the asset owner.	Yes
Asset Granted - Asset Privileges Only	Asset Granted - Asset Privileges Only	Asset	Generated when the asset was granted because the cardholder had asset privileges.	Yes
Audible Alarm	Audible Alarm	Trouble	An audible alarm condition has been detected.	
Audible Alarm Restore	Audible Alarm Restore	Trouble	An audible alarm condition has been restored.	
Audibles Silenced	Audibles Silenced	Fire	Generated when all the alarm bells have been turned off on the controller.	
Audibles Unsilenced	Audibles Unsilenced	Fire	Generated when all the alarm bells have been turned back on for the controller.	
Audit Trail Cleared	Audit Trail Cleared	System	Generated when the audit (event) log is cleared.	
Audit Trail Limit Reached	Audit Trail Limit Reached	System	Informs ReadykeyPRO the audit (event) log is becoming full and will be overwritten.	
Auto Arming Time Changed	Auto Arming Time Changed	System		
Auto-Arm Failed	Auto-Arm Failed	Trouble	An automatic arm has failed.	

Alarm	Event	Event Type	Description	Duress*
Automatic Closing	Automatic Closing	Open/Close	The system was armed automatically.	
Automatic Opening	Automatic Opening	Open/Close	The system has disarmed automatically.	
Automatic Phone Test	Automatic Phone Test	System		
Automatic Test	Automatic Test	System	Automatic communication test report	
Auxiliary Power Fault	Auxiliary Power Fault	Trouble		
Auxiliary Power Supply AC Loss	Auxiliary Power Supply AC Loss	Trouble		
Auxiliary Power Supply AC Restored	Auxiliary Power Supply AC Restored	Trouble		
Auxiliary Power Supply Communication Loss	Auxiliary Power Supply Communication Loss	Trouble		
Auxiliary Power Supply Communication Restored	Auxiliary Power Supply Communication Restored	Trouble		
Auxiliary Power Supply Communication Restored	Auxiliary Power Supply Communication Restored	Trouble		
Auxiliary Power Supply Fault Restored	Auxiliary Power Supply Fault Restored	Trouble		
Auxiliary Power Supply Output Low	Auxiliary Power Supply Output Low	Trouble		
Auxiliary Power Supply Output Low Restored	Auxiliary Power Supply Output Low Restored	Trouble		
Background Map Found	Background Map Found	Video	Generated when background stickers are detected.	

Alarm	Event	Event Type	Description	Duress*
Background Map Not Found	Background Map Not Found	Video	Generated when the engine cannot detect the background stickers. This may be caused when there is poor contrast or the stickers are improperly shaped/separated.	
Background Scene Changed	Background Scene Changed	Video	Indicates that part of the background has changed. This can be from something added to the scene or something removed from the scene.	
Background Scene Change Restored	Background Scene Change Restored	Video	The alarm is restored.	
Bad 9112 Packet	Bad 9112 Packet	System		
Battery Test Fail	Battery Test Fail	System	A battery test fail condition has been detected.	
Battery Test Fail Restore	Battery Test Fail Restore	System	A battery test fail condition has been restored.	
Bell # Disable	Bell # Disable	Relay/ Sounder	Bell # has been disabled.	
Bell # Disable Restore	Bell # Disable Restore	Relay/ Sounder	Bell # has been restored.	
Bell Fault	Bell Fault	Relay/ Sounder	A trouble condition has been detected on a local bell, siren, or annunciator.	
Bell Restore	Bell Restore	Relay/ Sounder	A trouble condition has been restored on a local bell, siren, or annunciator.	
Biometric Mismatch	Biometric Mismatch	Denied	Generated when the cardholder has a biometric template and the alternate reader was utilized to capture a template to match, but the captured template did not match the stored template.	Yes
Biometric Verify Mode Disabled	Biometric Verify Mode Disabled	System	Generated when biometric verify mode is disabled.	
Biometric Verify Mode Enabled	Biometric Verify Mode Enabled	System	Generated when biometric verify mode is enabled.	

Alarm	Event	Event Type	Description	Duress*
Blind Camera (AI)	Blind Camera (AI)	Video	Indicates that level of camera blindness (covered by some sort of obstacle) exceeded configured threshold.	
Blind Camera (AI) Restored	Blind Camera (AI) Restored	Video	The alarm is restored.	
Block Acknowledge	Block Acknowledge	Fire	Generated when a block acknowledge command is sent. This command acknowledges any existing unacknowledged alarms in the system all at once.	
Brightness Change	Brightness Change	Video	Generated when a change in overall brightness level of the scene is detected.	
Brightness Change Restored	Brightness Change Restored	Video	Generated when changes in brightness level are no longer exceeding the user defined threshold.	
Burglary Alarm	Burglary Alarm	Burglary	A burglary alarm condition has been detected.	
Burglary Alarm Cross Point	Burglary Alarm Cross Point	Burglary		
Burglary Alarm Restore	Burglary Alarm Restore	Burglary	A burglary alarm condition has been restored.	
Burglary Bypass	Burglary Bypass	Burglary	A burglary zone has been bypassed.	
Burglary Cancel	Burglary Cancel	Burglary	A burglary zone has been cancelled by an authorized user.	
Burglary Close	Burglary Close	Open/Close		
Burglary Inactive	Burglary Inactive	Burglary		
Burglary Open	Burglary Open	Open/Close		
Burglary Restore	Burglary Restore	Burglary	A burglary alarm/trouble condition has been eliminated.	
Burglary Supervisory	Burglary Supervisory	Burglary	An unsafe intrusion detection system condition has been detected.	
Burglary Test	Burglary Test	Burglary	A burglary zone has been activated during testing.	
Burglary Trouble	Burglary Trouble	Burglary	A burglary trouble condition has been detected.	

Alarm	Event	Event Type	Description	Duress*
Burglary Trouble Restore	Burglary Trouble Restore	Burglary	A burglary trouble condition has been restored.	
Burglary Unbypass	Burglary Unbypass	Burglary	Burglary zone bypass has been removed.	
Burglary Verified	Burglary Verified	Burglary	A burglary alarm has occurred and been verified within programmed conditions.	
Busy Seconds	Busy Seconds	System	The percent of time the receiver's line card is online.	
Bypass - Closed	Bypass - Closed	Open/Close		
Bypass Restore	Bypass Restore	System		
C900 Battery Low	C900 Battery Low	C900		
C900 Battery Restore	C900 Battery Restore	C900		
C900 Input Open	C900 Input Open	C900		
C900 Input Restored	C900 Input Restored	C900		
C900 Input Shorted	C900 Input Shorted	C900		
C900 Intercepted Disabled	C900 Intercepted Disabled	C900		
C900 Intercepted Enabled	C900 Intercepted Enabled	C900		
C900 Output Activated	C900 Output Activated	C900		
C900 Output Deactivated	C900 Output Deactivated	C900		
C900 Reboot	C900 Reboot	C900		
C900 Switched to Fallback	C900 Switched to Fallback	C900		
C900 Switched to Intercept	C900 Switched to Intercept	C900		
Cabinet Tamper Active	Cabinet Tamper	System	Generated when a cabinet tamper condition has been detected.	
Cabinet Tamper Restored	Cancelled Cabinet Tamper	System	Generated when a cabinet tamper condition has been restored.	
Callback Request	Callback Request	System		

Alarm	Event	Event Type	Description	Duress*
Callback Request	Call Conferenced	Intercom		
Call Disconnected	Call Disconnected	Intercom	Generated when an intercom call has been disconnected.	
Call Ended	Call Ended	Intercom	Generated when a call has ended.	
Call Established	Call Established	Intercom	Generated when an intercom call is answered.	
Call Failed	Call Failed	Intercom	Generated when an intercom call fails.	
Call to a busy subscriber	Call to a busy subscriber	Intercom	Generated when an intercom call has been placed to a busy subscriber.	
Call to an open subscriber	Call to an open subscriber	Intercom	Generated when an intercom call has been placed to an open subscriber.	
Call to a private subscriber	Call to a private subscriber	Intercom	Generated when a call has been placed to a private subscriber.	
Call Transferred	Call Transferred	Intercom	Generated when a call was transferred.	
Camera Enabled	Camera Enabled	NetDVMS	The camera is enabled in the NetDVMS Administrator.	
Camera Disabled	Camera Disabled	NetDVMS	The camera is disabled in the NetDVMS Administrator.	
Camera Motion	Camera Motion	NetDVMS	Generated when motion has been detected on a given input channel (camera). Motion is considered any change in the environment within the field of view of the camera. Sensitivity is determined by the motion detection settings in the NetDVMS Administrator.	

Alarm	Event	Event Type	Description	Duress*
Camera Tamper Active	Camera Tamper Active	Video	Indicates that IP Camera configuration was changed bypassing the ReadykeyPRO software. (It is possible if the user knows password to access the IP Camera and connect to it directly using IP Camera provided Web-interface.)	
Camera Tamper Restored	Camera Tamper Restored	Video	The alarm is restored.	
Cancel Alarm	Cancel Alarm	System		
Cancel Entire Sale	Cancel Entire Sale	POS	Generated when a transaction is used to indicate that an entire sale was cancelled.	
Cancel Report	Cancel Report	System	Untyped zone cancel.	
Cannot Open Door: Interlock Area Busy	Cannot Open Door: Interlock Area Busy	Area Control	An attempt to open the door in Alarm Monitoring was denied because a door is open or the door strike is active within an interlocked area.	
Capture Source Mismatch	Capture Source Mismatch	Video	Indicates that user-specified IP Camera type in ReadykeyPRO does not match actual IP Camera type.	
Carbon Monoxide Detected	Carbon Monoxide Detected	Gas	Generated when carbon monoxide has been detected by an alarm.	
Card Added	Card Added	System	Generated when a card has been added.	
Card Assigned	Card Assigned	System	An access ID has been added to the controller.	
Card Deleted	Card Deleted	System	An access ID has been deleted from the controller.	
Card Only Mode Denied: Blocked Mode	Card Only Mode Denied: Blocked Mode	System	Automatic scheduled change to card only mode was denied because lock is in blocked mode.	
Card Only Mode Denied: Secured Mode	Card Only Mode Denied: Secured Mode	System	Automatic scheduled change to card only mode was denied because lock is in secured mode.	

Alarm	Event	Event Type	Description	Duress*
Cash Amount Tendered	Cash Amount Tendered	POS	Generated when an event is used to indicate that a cash amount has been tendered	
Cash or Safe Drop	Cash or Safe Drop	POS	Generated when a transaction indicating a cash or safe drop has occurred.	
Change Due	Change Due	POS	Generated when a transaction indicating the change due has occurred.	
Change of State	Change of State	System	An expansion/peripheral device is reporting a new condition or state change.	
Charge Account Tender	Charge Account Tender	POS	Generated when a charge account was used as tender.	
Check Tender	Check Tender	POS	Generated when a check was used as tender.	
Checksum Fail	Checksum Fail	System	A checksum failure has been detected.	
Cipher Mode Disabled	Cipher Mode Disabled	System	Generated when Cipher mode is disabled for a reader.	
Cipher Mode Enabled	Cipher Mode Enabled	System	Generated when cipher mode is enabled for a reader. When this occurs card data can be entered via the keypad.	
Clerk Name or Number	Clerk Name or Number	POS	A transaction that reports the clerk’s name or number.	
Close Area	Close Area	Open/Close	The system has been partially armed	
Close by User	Close by User	Open/Close	The area has been armed by a user.	
Close Exception	Close Exception	Open/Close		
Close Out of Window	Close Out of Window	Open/Close		
Closing	Closing	Open/Close		
Closing Delinquent	Closing Delinquent	Open/Close		
Closing Extend	Closing Extend	Open/Close	The closing time has been extended.	
Closing Out of Window by User	Closing Out of Window by User	Open/Close		

Alarm	Event	Event Type	Description	Duress*
Closing Report	Closing Report	Open/Close	The system is armed and normal	
Closing Switch	Closing Switch	Open/Close		
Closing Time Changed	Closing Time Changed	Open/Close		
Combustion Alarm	Combustion Alarm	Open/Close	A combustion alarm condition has been detected.	
Combustion Alarm Restore	Combustion Alarm Restore	Open/Close	A combustion alarm condition has been restored.	
Command (#) Set From Reader	Command (#) Set From Reader	System	Generated when the reader keypad command “(#)” was executed.	
Command Pin +10 Set From Reader	Command Pin +10 Set From Reader	System	Indicates the reader command “Pin +10” was executed.	
Command Pin +20 Set From Reader	Command Pin +20 Set From Reader	System	Indicates the reader command “Pin +20” was executed.	
Command Sent	Command Sent	System	A command has been sent to an expansion/peripheral device.	
Communication Access Denied	Communication Access Denied	System	Indicates that a wrong password has been entered while logging on to a communication device.	
Communication Initialization Failed	Communication Initialization Failed	System	Generated when the Communication Server fails to initialize communications. For example if you are using RS-232 and have hyperterminal running and using COM1 and then you start up the Communication Server and it needs to use COM1 to communicate to a panel, it will fail to open up the serial port and this event will be logged.	
Communication Trouble Restore	Communication Trouble Restore	System	A communication trouble has been restored.	
Communications Fail	Communications Fail	System	A communication has failed.	
Communications Lost	Communications Lost	System	Generated when communications to the device have been lost.	

Alarm	Event	Event Type	Description	Duress*
Communications Lost - Primary Path	Primary Communication Path Lost	System	Generated when the primary path lost communication with the host.	
Communications Lost - Secondary Path	Secondary Communication Path Lost	System	Generated when the secondary path loses communication with the host.	
Communications Path Switched - Primary to Secondary	Communications Path Switched - Primary to Secondary	System	Generated when the communication path has been switched from the primary path to the secondary path.	
Communications Path Switched Secondary to Primary	Communications Path Switched Secondary to Primary	System	Generated when the communication path has switched from the secondary path to the primary path.	
Communications Restore	Communications Restore	System	Generated when communications have been restored.	
Communications Restored	Communications Restored	System	Generated when communications to the device have been restored.	
Communications Restored - Primary Path	Primary Communication Path Restored	System	Generated when the primary path restored communication with the host.	
Communications Restored - Secondary Path	Secondary Communication Path Restored	System	Generated when the secondary path restored communication with the host.	
Communications Trouble	Communications Trouble	System	A communications trouble has been detected.	
Communications With Host Lost	Communications With Host Lost	System	An event was generated by the hardware when communications with the host was lost.	
Communications With Host Restored	Communications With Host Restored	System	An event was generated by the hardware when communications with the host was restored.	
Complimentary Tender	Complimentary Tender	POS	Generated when the tender was complimentary.	
Computer Trouble	Computer Trouble	System		

Alarm	Event	Event Type	Description	Duress*
Conferenced Call		Intercom	Generated if a call is conferenced together with another call.	
Congestion	Congestion	Video	Generated when the user-specified level and pattern of congestion is detected within a region of interest.	
Congestion Restored	Congestion Restored	Video	Generated 8 seconds after last detection of a Congestion event.	
Controller Connection Mismatch	Controller Connection Mismatch	System	Generated when the ReadykeyPRO attempts to make a connection to a controller by upgrading or degrading the connection while the controller is online.	
Controller Encryption Error	Controller Encryption Error	System	Generated in several instances, including when: • A controller is configured for a plain connection when it requires encryption. • An encrypted controller is online, but its configuration is changed to a plain connection. • A controller is configured for a plain connection, but then a physical controller swap is made where the new controller requires encryption. • A controller that supports encryption is currently online with a plan connection, and then the DIR switch 8 is turned on.	
CPU Data Error	CPU Data Error	System	A CPU data error was detected.	
Credit Card Tendered	Credit Card Tendered	POS	Generated when a credit card was used as tender.	
Cross Zone Trouble	Cross Zone Trouble	Trouble		

Alarm	Event	Event Type	Description	Duress*
Current Time	Current Time	POS	An event that reports the current time.	
Database Error Event Polling Stopped	Database Error Event Polling Stopped	System	Generated by the communication server when there is a problem writing events to the database. This event is not written to the database but is sent to Alarm Monitoring clients. Polling of the events from the various hardware devices is stopped until the events can be written to the database.	
Database Error in Panel Download	Database Error in Panel Download	System	Generated by the communication server when the database cannot be opened at the start of a database download to a controller.	
Data Lost	Data Lost	System	The dialer data has been lost and there is a transmission error.	
Date Changed	Date Changed	System	The date was changed.	
Day Trouble	Day Trouble	Trouble	A day trouble condition has been detected.	
Day Trouble Restore	Day Trouble Restore	Trouble	A day trouble condition has been restored.	
Day/Night Alarm	Day/Night Alarm	Trouble	A day/night alarm condition has been detected.	
Day/Night Alarm Restore	Day/Night Alarm Restore	Trouble	A day/night alarm condition has been restored.	
Daylight Saving Time Audit	Daylight Saving Time Audit	System	Start of DST (Daylight Saving Time) or end of DST has occurred.	
Deactivate Output	Deactivate Output	System		
Dealer ID	Dealer ID	System		
Debit, ATM, Check Card Tender	Debit, ATM, Check Card Tender	POS	Transaction that indicated that a debit, ATM, or check card was used as tender.	
Deferred Close	Deferred Close	Open/Close		
Deferred Open/Close	Deferred Open/ Close	Open/Close		

Alarm	Event	Event Type	Description	Duress*
Denied, Badge Not in Panel	Denied, Badge Not in Panel	Denied	Generated when a badge is denied at a reader because it is not in the system.	Yes
Denied Count Exceeded	Denied Count Exceeded	Denied		Yes
Denied Low Battery	Denied Low Battery	Denied	Generated when access is denied because the battery on the device is low.	
Denied, No Command Authority	Denied, No Command Authority	Denied	Generated when a reader command function was denied because the user did not have the command authority to execute the function.	
Denied - No Host Approval	Denied - No Host Approval	Denied	Generated when access was denied because the host did not grant approval. This can happen because the host response did not come back in a timely fashion or the controller is offline with the host.	Yes
Denied, Not Authorized	Denied, Not Authorized	Denied	Generated when access was denied because user authorization did not match authorization assigned to the reader (lock).	
Denied, PIN Only Request	Denied, PIN Only Request	Denied	Generated when access was denied for a pin only request (either an invalid pin code or pin support is not enabled for the panel).	Yes
Denied - Unauthorized Assets	Denied - Unauthorized Assets	Denied	Generated when access was denied because of unauthorized assets.	Yes
Denied Under Duress	Access Denied Under Duress	Duress	Generated when the cardholder was denied access under duress.	Yes
Denied Unmask, Active Zones in Group	Denied Unmask - Active Zones in Group	Denied	Generated when the unmask command failed because there are still active zones in the group.	
Deny Count Exceeded	Deny Count Exceeded	Denied	Generated when a specified number of invalid attempts are made in a row at a reader.	

Alarm	Event	Event Type	Description	Duress*
Deposit Amount Paid Pending Purchase	Deposit Amount Paid Pending Purchase	POS	Event indicating that a deposit amount paid pending purchase has occurred.	
Deposit Return	Deposit Return	POS	Transaction for a deposit return.	
Detector High Sensitivity	Detector High Sensitivity	Trouble	A detector high sensitivity condition has been detected.	
Detector High Sensitivity Restore	Detector High Sensitivity Restore	Trouble	A detector high sensitivity condition has been restored.	
Detector Low Sensitivity	Detector Low Sensitivity	Trouble	A detector low sensitivity condition has been detected.	
Detector Low Sensitivity Restore	Detector Low Sensitivity Restore	Trouble	A detector low sensitivity condition has been restored.	
Detector Test	Detector Test	Fire	Generated when the fire detection test is initiated.	
Detector Test Fail	Detector Test Fail	Fire	Generated when the fire detection test fails.	
Detector Test OK	Detector Test OK	Fire	Generated when the fire detection test is successfully completed.	
Device Turned Off	Device Turned Off	Trouble	A device turned off.	
Device Turned On	Device Turned On	Trouble	A device turned on.	
Device Type Mismatch	Device Type Mismatch	System	Generated when the device is of a different type than what it has been configured for.	
Diagnostic	Diagnostic	System	A diagnostic report was requested.	
Diagnostic Error	Diagnostic Error	System	A device is reporting a diagnostic error.	
Dial Out Method	Dial Out Method	System		
Dialer Disabled	Dialer Disabled	Trouble	The dialer has become disabled.	
Dialer Disabled Restore	Dialer Disabled Restore	Trouble	The dialer has been restored from being disabled.	
Dialer Shutdown	Dialer Shutdown	Trouble	The dialer has shutdown.	

Alarm	Event	Event Type	Description	Duress*
Dialing Error	Dialing Error	Trouble	An error has been detected when dialing.	
Dialup Last Connection Time Expired	Dialup Last Connection Time Expired	System	Generated by the communication server for dialup panels that have exceeded the set number of hours since their last connection. When this event is generated, the communication server will attempt to connect to the panel. If the dialup panel repeatedly receives this event, the panel should be investigated to see why it is not calling back.	
Dialup Stored Command Limit Exceeded	Dialup Stored Command Limit Exceeded	System	Generated by the communication server for dialup panels that have exceeded their stored command limit. When this event is generated, the communication server will attempt to connect to the panel. If the dialup panel repeatedly receives this event, the panel should be investigated to see why it is not calling back.	
Digital Dialer Daily Test Fail	Digital Dialer Daily Test Fail	System	Digital dialer failed to report its daily test.	
Disable Intercept Mode	Disable Intercept Mode	System		
Directional Motion	Directional Motion	Video	Generated when an object moving in a pre-specified direction is detected.	
Directional Motion Restored	Directional Motion Restored	Video	Generated 8 seconds after last detection of a Directional Motion event.	
Disarm From Alarm	Disarm From Alarm	System	An account in alarm was reset/disarmed.	
Discount Entered as Absolute Amount	Discount Entered as Absolute Amount	POS	Generated when a discount was entered as an absolute amount.	
Discount Entered as Percentage	Discount Entered as Percentage	POS	Generated when a discount was entered as a percentage.	
Door Close	Door Close	System	Generated when a door closes.	

Alarm	Event	Event Type	Description	Duress*
Door Contact Tamper Active	Door Contact Tamper	System	Generated when the door contact tamper has gone active.	
Door Contact Tamper Restored	Door Contact Tamper Cancelled	System	Generated when the door contact tamper has been restored.	
Door Cycled	Door Cycled	System	Generated when momentary access is granted to a door. This is a temporary door state in which the door initiates the door sequence as if a valid card was read. Door cycled cannot be scheduled.	
Door Forced	Door Forced	Trouble	The door was forced open without an access request.	
Door Forced Open	Door Forced Open	System	Generated when a “Door Forced Open” condition has been detected.	
Door Forced Open Masked	Door Forced Open Masked	System	Generated when the “Door Forced Open” event has become masked for the device.	
Door Forced Open Restored	Door Forced Open Cancelled	System	Generated when a “Door Forced Open” condition has been restored.	
Door Forced Open Unmasked	Door Forced Open Unmasked	System	Generated when the “Door Forced Open” event has become unmasked for the device.	
Door Forced Trouble	Door Forced Trouble	Trouble	An access point has been forced open in an unarmed area.	
Door Held Open	Door Held Open	System	Generated when a “Door Held Open” condition has been detected.	
Door Held Open Masked	Door Held Open Masked	System	Generated when the “Door Held Open” event has become masked for the device.	
Door Held Open Restored	Door Held Open Cancelled	System	Generated when a “Door Held Open” condition was restored.	

Alarm	Event	Event Type	Description	Duress*
Door Held Open Unmasked	Door Held Open Unmasked	System	Generated when the “Door Held Open” event has become unmasked for the device.	
Door Left Open	Door Left Open	Trouble	An access point was open when the door cycle time expired.	
Door Left Open Alarm	Door Left Open Alarm	Trouble	An open access point was open when the open time expired in an armed area.	
Door Left Open Restore	Door Left Open Restore	Trouble	An access point in a door left open state has restored.	
Door Left Open Trouble	Door Left Open Trouble	Trouble	An open access point was open when the open time expired in an unarmed area.	
Door Locked	Door Locked	Trouble	Generated when a door returns to its normal door state (locked). When a door is in the lock door state, you can initiate the door sequence using schedules, command center functions, door requests, or valid card requests. Door locked is similar to a reader being in card and pin mode.	
Door Open	Door Open	System	An event indicating that the door has opened.	
Door Open From Inside	Door Open From Inside		Door opened from inside, only when not in unlocked mode.	
Door Request	Door Request	System	This event is generated from Bosch intrusion panels when a door is manually activated to open without the presentation of an ID.	
Door Restore	Door Restore	Trouble	An access alarm/trouble condition has been eliminated.	

Alarm	Event	Event Type	Description	Duress*
Door Secured	Door Secured	System	Generated when no access is allowed to a door. When a door is in a secure state, no access is allowed through the door until it is returned to the locked state. Door secured is similar to a reader being in locked mode.	
Door Shunt Command Executed From Reader	Door Shunt Command Executed From Reader	System	Generated when the door shunt command was executed from the reader.	
Door Shunt Command Results - Cancelled	Door Shunt Command Results - Cancelled	System	Generated when the door is closed while the door shunt command is executing.	
Door Station	Door Station	Trouble	Identified door for next report.	
Door Unlocked	Door Unlocked	System	Generated when there is free access to a door. When a door is unlocked, the door is shunted and the strike does not prevent the door from opening. In this state, you do not need to activate a door request or present a valid card to gain access. Door unlocked is similar to a reader being in unlocked mode.	
Drift Compensation Error	Drift Compensation Error	Trouble		
Driver Error in Panel Download	Driver Error in Panel Download	System	Generated by the communication server when an error occurs during a database download to a controller.	
Duct Alarm	Duct Alarm	Trouble	A duct alarm condition has been detected.	
Duct Alarm Restore	Duct Alarm Restore	Trouble	A duct alarm condition has been restored.	
Duress Access Grant	Duress Access Grant	Duress		
Duress Egress Grant	Duress Egress Grant	Duress		
DURESS - Interlock Area Busy	DURESS - Interlock Area Busy	Duress	Access was requested to an interlocked area while under duress.	Yes

Alarm	Event	Event Type	Description	Duress*
Egress Denied	Egress	Egress	A user presented a badge to an out reader (reader leaving the area) and was denied access.	
Egress Granted	Egress	Egress	A user presented a badge to an out reader (reader leaving the area), was granted access and opened the door after the grant.	
Elevator Terminal Mode Access to Authorized Floors	Elevator Terminal Mode Access to Authorized Floors	System	Generated when the elevator terminal mode has changed to “Access to Authorized Floors.”	
Elevator Terminal Mode Default Floor	Elevator Terminal Mode Default Floor	System	Generated when the elevator terminal mode has changed to “Default Floor Only.”	
Elevator Terminal Mode Default Floor or User Entry of Destination Floor	Elevator Terminal Mode Default Floor or User Entry of Destination Floor	System	Generated when the elevator terminal mode has changed to “Default Floor or User Entry of Destination Floor.”	
Elevator Terminal Mode User Entry of Destination Floor	Elevator Terminal Mode User Entry of Destination Floor	System	Generated when the elevator terminal mode has changed to “User Entry of Destination Floor.”	
Embedded Analytics Failure	Embedded Analytics Failure	System	Generated when embedded analytics fail to initialize.	
Embedded Analytics Restored	Embedded Analytics Restored	System	Generated when embedded analytics initialize successfully following a failure.	
Employee Sign Off	Employee Sign Off	POS	Generated when an employee signs off.	
Employee Sign On	Employee Sign On	POS	Generated when an employee signs on.	
Exit Request Denied: Interlock Area Busy	Exit Request Denied: Interlock Area Busy	Area Control	A request to exit made via REX button was denied because a door is open or the door strike is active within an interlocked area.	
Extended Held Command Denied	Extended Held Command Denied	System	Generated when an extended held command is denied.	

Alarm	Event	Event Type	Description	Duress*
Extended Held Command Set From Reader	Extended Held Command Set From Reader	System	Generated when an extended held command is entered at the reader.	
Extended Held Open Mode Disabled	Extended Held Open Mode Disabled	System	Generated when extended held open mode is disabled.	
Extended Held Open Mode Enabled	Extended Held Open Mode Enabled	System	Generated when extended held open mode is enabled.	
Facial Detection	Facial Detection	Video	Generated when one or several faces are detected.	
Facial Detection Restored	Facial Detection Restored	Video	Generated 8 seconds after last detection of a face.	
Facility Code Only Mode Denied: Blocked Mode	Facility Code Only Mode Denied: Blocked Mode	System	Automatic scheduled change to facility code only mode was denied because lock is in blocked mode.	
Facility Code Only Mode Denied: Secured Mode	Facility Code Only Mode Denied: Secured Mode	System	Automatic scheduled change to facility code only mode was denied because lock is in secured mode.	
Facility Occupancy Too Low	Facility Occupancy Too Low	Video	Generated when the occupancy falls below the user-specified limit.	
Facility Occupancy Too Low Restored	Facility Occupancy Too Low Restored	Video	Generated when the occupancy returns to a value above the lower limit.	
Facility Occupancy Too High	Facility Occupancy Too High	Video	Generated when the occupancy rises above the user-specified limit.	
Facility Occupancy Too High Restored	Facility Occupancy Too High Restored	Video	Generated when the occupancy returns to a value below the upper limit.	
Failed to Report Expected Event	Failed to Report Expected Event	System	Generated when a device that is supposed to report an event within a certain period of time fails to report an event during this time period.	
Fire Alarm	Fire Alarm	Fire	Generated when a fire device is in alarm.	
Fire Alarm Acknowledge	Fire Alarm Acknowledge	Fire	Generated when a fire alarm has been acknowledged.	
Fire Alarm Acknowledged Clear	Fire Alarm Acknowledged Clear	Fire	Generated when a fire alarm has been acknowledged and cleared.	

Alarm	Event	Event Type	Description	Duress*
Fire Alarm Block Acknowledge	Fire Alarm Block Acknowledge	Fire	Generated when all fire alarms have been acknowledged at the fire panel.	
Fire Alarm In	Fire Alarm In	Fire	Generated when a new fire alarm has been detected for the device.	
Fire Alarm Out	Fire Alarm Out	Fire	Generated when a device with a previous fire alarm has returned to its normal state.	
Fire Button Set	Fire Button Set	Fire	The reported fire button has been set.	
Fire Missing	Fire Missing	Fire		
Fire Walk Test Ended	Fire Walk Test Ended	Fire	A fire walk test has ended.	
Fire Walk Test Started	Fire Walk Test Started	Fire	A fire walk test has started.	
Fire Zone Walk Tested	Fire Zone Walk Tested	Fire	A fire zone has been tested.	
Firmware Download Started	Firmware Download Started	System	Generated when the firmware download has started.	
Firmware Download Completed	Firmware Download Completed	System	Generated when the firmware download has completed.	
Firmware Download Failed	Firmware Download Failed	System	Generated when the firmware download has failed.	
First Card Unlock Mode Denied: Blocked Mode	First Card Unlock Mode Denied: Blocked Mode	System	Automatic scheduled change to first card unlock mode was denied because lock is in blocked mode.	
First Card Unlock Mode Denied: Secured Mode	First Card Unlock Mode Denied: Secured Mode	System	Automatic scheduled change to first card unlock mode was denied because lock is in secured mode.	
First Card Unlock Mode Disabled	First Card Unlock Mode Disabled	System	Generated when first card unlock mode is disabled for a door.	
First Card Unlock Mode Enabled	First Card Unlock Mode Enabled	System	Generated when first card unlock mode is enabled for a door.	

Alarm	Event	Event Type	Description	Duress*
Foil Break Alarm	Foil Break Alarm	Trouble	Generated when a break in a foil circuit occurs. This is most commonly used to trigger an alarm when glass being protected with the foil circuit is broken.	
Foil Break Restore	Foil Break Restore	Trouble	Generated when a foil break alarm condition has been restored.	
Foodstamps Tender	Foodstamps Tender	POS	Indicates that food stamps were used as tender.	
Gasoline Prepayment	Gasoline Prepayment	POS	Transaction for a gasoline prepayment	
Gasoline Prepayment Refund	Gasoline Prepayment Refund	POS	Transaction for a gasoline prepayment	
Generic Event	Generic Event	Generic	A generic event exists with more specific information in the event text.	
Global Linkage Action Executed	Global Linkage Action Executed	System	Generated when a global I/O linkage has executed.	
Global Linkage Action Failed	Global Linkage Action Failed	System	Generated when a global I/O linkage has failed.	
Granted Access	Access Granted	Granted	Generated when access was granted.	
Granted APB Violation, Entry Made	Access Granted Anti-Passback Used	Area Control	Generated when an anti-passback violation occurred but access was granted and entry was made. This can happen when using soft anti-passback.	
Granted APB Violation, No Entry Made	Access Granted Anti-Passback Not Used	Area Control	Generated when an anti-passback violation occurred and access was granted but no entry was made. This can happen when using soft anti-passback.	
Granted Facility Code	Access Granted On Facility Code	Granted	Generated when access was granted based on a valid facility code.	
Granted Facility Code, No Entry	Access Granted On Facility Code No Entry Made	Granted	Generated when access was granted on facility code but no entry was made at the door.	
Granted No Entry	Access Granted No Entry Made	Granted	Generated when access was granted but no entry was made at the door.	Yes

Alarm	Event	Event Type	Description	Duress*
Granted Under Duress	Access Granted Under Duress	Emergency	Generated when the cardholder was granted access under duress.	
Granted Under Duress, No Entry	Access Granted Under Duress - No Entry Made	Emergency	Generated when the cardholder was granted access under duress but no entry was made.	
Grounded Loop Active	Grounded Loop Alarm Active	System	Generated when a grounded loop fault condition has been detected.	
Grounded Loop Restored	Cancelled Grounded Loop	System	Generated when the grounded loop fault condition was restored.	
Guard Tour Action Executed	Guard Tour Action Executed	System	Generated when a guard tour action has executed.	
Guard Tour Action Failed	Guard Tour Action Failed	System	Generated when a guard tour action has failed.	
History Report End	History Report End	System		
History Report Start	History Report Start	System		
Hold	Hold	Intercom	Generated when a phone call is placed on hold.	
Holdup Alarm Restore	Holdup Alarm Restore	Emergency	Holdup alarm was restored.	
Host Executed Function List	Host Executed Function List	System	Generated when a function list has been executed from the host.	
Host Open Door - Door Used	Host Open Door - Door Not Used	System	When the host issued an open door command and the door was opened.	
Host Open Door - Door Not Used	Host Open Door - Door Not Used	System	When the host issued an open door command and the door was not opened.	
In-Camera-Memory Download Completed	In-Camera-Memory Download Completed	System	Generated when the process of retrieving the files from the camera memory is completed.	
In-Camera-Memory Download Failed	In-Camera-Memory Download Failed	System	Generated when the process of retrieving the files from the camera memory is failed.	
In-Camera-Memory Download Restored	In-Camera-Memory Download Restored	System	Generated when the process of retrieving the files from the camera memory is restored.	

Alarm	Event	Event Type	Description	Duress*
In-Camera-Memory Download Started	In-Camera-Memory Download Started	System	Generated when the process of retrieving the files from the camera memory is started.	
Inactive Badge	Inactive Badge	Denied	Generated when access was denied because the badge was inactive.	Yes
Incoming Call	Incoming Call	Intercom	Generated when there is an incoming call.	
Information Message	Information Message	POS	Used to report information messages	
Initiated	Initiated	Intercom	Generated when a phone call is initiated.	
Input Bypassed	Input Bypassed	System	Generated when an input has been temporarily bypassed from detecting changes in state and reporting alarms. Typically, you would specify to bypass the input in order to troubleshoot an input issue without reporting the alarms for it. This is often done during an armed state. After the system enters the disarmed state, the input normally leaves the bypassed state.	
Input Disabled	Input Disabled	System	This is similar to Input Bypassed except the input has been permanently disabled from detecting and reporting activity until the operator specifically enables it.	
Input Masked	Input Masked	System	Generated when an input has become masked.	
Input Restored	Input Restored	System	An input has been returned to the normal mode of operation after being in either a bypassed or disabled state.	
Input Unmasked	Input Unmasked	System	Generated when an input has become unmasked.	
Intercom Function	Intercom Function	Intercom	Generated when an intercom function has been executed.	

Alarm	Event	Event Type	Description	Duress*
Interlock Area Busy	Interlock Area Busy	Area Control	Access requested by presenting a badge was denied because a door is open or the door strike is active within an interlocked area.	
Insufficient Frame Rate Detected	N/A	N/A	This warning appears when the analytics are not receiving the required minimum frame rate for the events configured on the video channel.	
Insufficient Frame Rate Restored	N/A	N/A	Generated when the frame rate reaches a value sufficient for the events configured on the video channel.	
Intrusion Command Accepted	Intrusion Command Accepted	Generic	An intrusion command was successfully executed.	
Intrusion Command Denied	Intrusion Command Denied	Denied	An attempt to execute an intrusion command was denied, either the command is not allowed at the reader, the user is not authorized for this command, or invalid command arguments were supplied.	
Invalid Access Level	Invalid Access Level	Denied	Generated when access was denied because of an invalid access level.	Yes
Invalid Badge	Invalid Badge	Denied	Generated when access was denied because the badge ID was unknown to the controller.	Yes
Invalid Camera	Invalid Camera	Video	Generated when the camera is tampered with (covered, moved, or out-of-focus).	
Invalid Camera Restored	Invalid Camera Restored	Video	Generated 8 seconds after the camera becomes valid again or in the case of camera covered or moved, when the background is relearned.	
Invalid Card Format	Invalid Card Format	Denied	Generated when the badge contained a card format that was not recognized by the reader.	

Alarm	Event	Event Type	Description	Duress*
Invalid Device Serial Number	Invalid Device Serial Number	System	Generated when the device does not have a valid serial number.	
Invalid Facility Code	Invalid Facility Code	Denied	Generated when access was denied because the badge had an invalid facility code.	Yes
Invalid Issue Code	Invalid Issue Code	Denied	Generated when access was denied because the issue code read from the badge did not match the current issue code stored in the database for the badge.	Yes
Invalid OEM Code	Invalid OEM Code	System	Indicates that the hardware did not contain the expected OEM (Original Equipment Manufacturer) code.	
Invalid PIN Number	Invalid PIN Number	Denied	Generated when access was denied because an invalid PIN was entered.	Yes
Item Correct of Previously entered Item	Item Correct of Previously entered Item	POS	Generated to indicate that an item was corrected.	
Item Sold	Item Sold	POS	Indicates an item was sold.	
IVS Channel Processing Failed	IVS Channel Processing Failed	Video	Generated by the IntelligentVideo Server when video processing is terminated due to an error or lost connection.	
IVS Channel Processing Restarted	IVS Channel Processing Restarted	Video	Generated when the IntelligentVideo Server re-establishes a connection to a channel that previously reported failure.	
IVS Connection Lost	IVS Connection Lost	Video	Generated when the camera is configured to analyze video on a remote IntelligentVideo Server and connection to the IntelligentVideo Server is lost.	
IVS Connection Restored	IVS Connection Restored	Video	Generated when the connection to the IntelligentVideo Server was lost and has been restored.	

Alarm	Event	Event Type	Description	Duress*
IVS Engine Connection Lost	IVS Engine Connection Lost	Video	Generated when the IntelligentVideo Server looses connection to the LpsSearchSvc service and video processing of all channels fails.	
IVS Engine Connection Restored	IVS Engine Connection Restored	Video	Generated when the IntelligentVideo Server reconnects to the LpsSearchSvc service after the connection has been lost.	
Key Override	Key Override	System	Generated when the key override is used in a Mortise lockset. Not supported in Cylindrical lockset.	
Keypad Fire	Keypad Fire	Fire	A fire alarm has been generated from a keypad.	
Lamp Test Activated	Lamp Test Activated	Fire	Generated when the lamp test is activated. When a lamp test is activated the AM-2020 will send out a command sequence to display a set of solid blocks on the hardware’s LCD.	
Lamp Test Completed	Lamp Test Completed	Fire	Generated when the lamp test successfully completes.	

Alarm	Event	Event Type	Description	Duress*
License Will Soon Expire - X Days Left	License Will Soon Expire - X Days Left	System	Generated when the system license is reaching its expiration date. This alarm is dependent on linkage server being configured and running on a host workstation. It is advised that this alarm be configured to be e-mailed to the system administrator. For more information, refer to Send an E-mail on page 113. **Note:** In order for the alarm to be reported to monitoring stations there must be at least one panel configured and marked online. The panel does not need to exist or actually be online in Alarm Monitoring, it simply needs to exist in the System Status view. **Note:** This event must be available as an input event to use the Global I/O output action. Make sure it is available to be sent out via DataConduIT.	
Line Error Active	Line Error Active	System	Generated when a line error fault condition has been detected.	
Line Error Restored	Cancelled Line Error	System	Generated when the line error fault condition was restored.	
Local I/O Executed Function List	Local I/O Executed Function List	System	Generated when a local I/O function list has been activated.	
Loitering	Loitering	Video	Generated when a loiterer is detected.	

Alarm	Event	Event Type	Description	Duress*
Loitering Restored	Loitering Restored	Video	Generated 8 seconds after the last detection of a Loitering event.	
Lock Initialized	Lock Initialized	System	Lock was initialized using the PP (Portable Programmer) application.	
Lock Updated	Lock Updated	System	Lock was updated.	
Lock Powered Up by Portable Programmer	Lock Powered Up by Portable Programmer	System	Generated after a power up by the portable programmer.	
Locked Under AFC	Locked Under AFC	System	End of AFC state.	
Locked Under First Card Unlock	Locked Under First Card Unlock	System	First card unlock mode; door is relocked.	
Lottery Pay Out	Lottery Pay Out	POS	Generated when a lottery pay out has occurred.	
Low Battery	Low Battery	System	Low battery alarm.	
Low Battery Restored	Low Battery Restored	System	Generated when a low battery is restored.	
Lottery Sale	Lottery Sale	POS	Generated when an event for a lottery sale has occurred.	
Low Voltage	Low Voltage	System	Generated when a low voltage condition has been detected at the device.	
Low Voltage Restored	Low Voltage Restored	System	Generated when a device resumes its proper voltage.	
Manufacturer Coupon	Manufacturer Coupon	POS	Indicates a manufacturer coupons.	
Manufacturer Coupon Redemption	Manufacturer Coupon Redemption	POS	Transaction generated for a manufacturer coupon redemption.	
Max Assets Reached	Max Assets Reached	System	Generated during a download when the number of assets exceeds the maximum value configured for the controller. Only the maximum number of assets will be downloaded (all others will be ignored).	

Alarm	Event	Event Type	Description	Duress*
Max Biometric Templates Reached	Max Biometric Templates Reached	System	Generated during a download when the number of biometric templates exceeds the maximum value configured for the controller. Only the maximum number of templates will be downloaded (all others will be ignored).	
Max Cardholders Reached	Max Cardholders Reached	System	Generated during a download when the number of cardholders exceeds the maximum value configured for the controller. Only the maximum number of cardholders will be downloaded (all others will be ignored).	
Merchandise Returned	Merchandise Returned	POS	Generated when merchandise is returned.	
Miscellaneous Tender	Miscellaneous Tender	POS	Generated when miscellaneous tender is used.	
Module Active	Module Active	Fire	Generated when a monitor or control module connected to the system becomes active. The device label assigned to this device and the zone label assigned to the first zone programmed for this device will be included with the event.	
Module Clear	Module Clear	Fire	Generated when a monitor or control module connected to the system is no longer active. The device label assigned to this device and the zone label assigned to the first zone programmed for this device will be included with the event.	
Motion Detected (AI)	Motion Detected (AI)	Video	Generated when motion has been detected on a given input channel (camera). Motion is considered any change in the environment within the field of view of the camera.	

Alarm	Event	Event Type	Description	Duress*
Motion Detected (AI) Restored	Motion Detected (AI) Restored	Video	Generated when motion has been restored (is no longer detected) on a given input channel (camera). Motion is considered any change in the environment within the field of view of the camera.	
Muster Mode Reset	Muster Mode Reset	Mustering	Generated when muster mode is reset.	
Muster Mode Start	Muster Mode Start	Mustering	Generated when muster mode is started.	
Negative Tax	Negative Tax	POS	Generated when negative tax is used.	
Negative Total	Negative Total	POS	Generated when there is a negative total.	
No Biometric Template Data	No Biometric Template Data	Biometric	Generated when no biometric template data was available from the biometric reader at the end of a verification sequence.	
No Blocking Override	No Blocking Override		User does not have Blocked override privilege.	
Non-Fire Active	Non-Fire Active	System	An event indicating a non fire related alarm condition is active.	
Non-Fire Active Cleared	Non-Fire Active Cleared	System	An event indicating a non fire related alarm condition is no longer active.	
Not Configured	Not Configured	System	Generated when a device has not been configured or defined by the host.	
No Sale	No Sale	POS	Transaction generated for a no sale.	
Object Crosses a Region	Object Crosses a Region	Video	Generated when an object is detected in the process of crossing a user-specified region.	
Object Crosses a Region Restored	Object Crosses a Region Restored	Video	Generated 8 seconds after the last detection of an Object Crosses a Region event.	
Object Detection	Object Detection	Video	Generated when an object complying with user-specifications is detected.	

Alarm	Event	Event Type	Description	Duress*
Object Detection Restored	Object Detection Restored	Video	Generated 8 seconds after the last detection of an Object Detection event.	
Object Left Behind	Object Left Behind	Video	Generated when a foreground object is left for more than a pre-specified duration.	
Object Left Behind Restored	Object Left Behind Restored	Video	Generated when the left object was taken or the background (after a certain time interval) is relearned.	
Object Lurking	Object Lurking	Video	Generated when a moving object stops or slows down for at least 7 seconds.	
Object Lurking Restored	Object Lurking Restored	Video	Generated 8 seconds after the last detection of an Object Lurking event.	
Object Moves Too Fast	Object Moves Too Fast	Video	Generated when a moving object is detected in a scene with a speed that exceeds the user-specified rate.	
Object Moves Too Fast Restored	Object Moves Too Fast Restored	Video	Generated 8 seconds after the last detection of an Object Moves Too Fast event.	
Object Starts to Move	Object Starts to Move	Video	Generated when a monitored object begins moving.	
Object Starts to Move Restored	Object Starts to Move Restored	Video	Generated 8 seconds after last detection of an Object Starts to Move event.	
Object Removed	Object Removed	Video	Generated when a background object is removed.	
Object Removed Restored	Object Removed Restored	Video	Generated when the object is returned to its original location or the background (after a certain time interval) is relearned.	
Object Stops	Object Stops	Video	Generated when a foreground object stops.	
Object Stops Restored	Object Stops Restored	Video	Generated 8 seconds after the last detection of an Object Stops event.	

Alarm	Event	Event Type	Description	Duress*
Open Door Command Issued - Door Used	Open Door Command Issued - Door Used	System	Indicates that a command was issued to open the door and the door was used. This can be for a locally generated open door command or one from the host.	
Open Door Command Issued - Door Not Used	Open Door Command Issued - Door Not Used	System	Indicates that a command was issued to open up the door and the door was not used. This can be for a locally generated open door command or one from the host.	
Open Line Active	Open Line Active	System	Generated when an open line fault condition has been detected.	
Open Line Restored	Cancelled Open Line	System	Generated when the open line fault condition was restored.	
Override Preprogrammed Price	Override Preprogrammed Price	POS	Generated when the preprogrammed price is overridden.	
Panel Download Completed	Full Panel Download Completed	System	Generated when a database download to the controller has completed.	
Panel Download Started	Full Panel Download Started	System	Generated when a database download to the controller has started.	
Panel Event Capacity Exceeded - Events Overwritten	Panel Event Capacity Exceeded - Events Overwritten	System	Generated when the event log in the panel fills up and starts overwriting old events.	
Panel Free Memory Low	Panel Free Memory Low	System	Generated when the free memory in the panel (controller) is below what is determined to be a safe value.	
Panel ID Mismatch	Panel ID Mismatch	System	Generated when the panel (controller) has a different ID than what is in the database. This can happen if a new panel or replacement panel is placed out in the field. A download to the panel should correct the problem.	

Alarm	Event	Event Type	Description	Duress*
Panel Marked Offline After Timeout	Panel Marked Offline After Timeout	System	Generated when the video recorder is automatically placed offline because a connection cannot be made after the user specified amount of time.	
Panel Options Mismatch	Panel Options Mismatch	System	Generated when the options inside of the panel differ from what the panel is currently configured for in the database. This can happen if the panel options change and a download is not issued to the panel. To correct this situation, a download should be issued to the panel.	
Panel Power Up Complete	Panel Power Up Complete	System	Generated when the panel power up is complete.	
Panic Abort	Panic Abort	Trouble	Generated when a panic alarm has been manually aborted/canceled.	
Panic Alarm	Panic Alarm	Trouble	Generated when emergency assistance has been manually requested.	
Panic Alarm Restore	Panic Alarm Restore	Trouble	Generated when the panic alarm has been restored.	
Pay Out	Pay Out	POS	Generated when a payout takes place.	
Payment of Refund to Customer	Payment of Refund to Customer	POS	Generated when a payment or refund is given to a customer.	
Payment Toward Charge Account Balance	Payment Toward Charge Account Balance	POS	Generated when a payment toward an account balance.	
People Counting	People Counting	Video	Generated when the count was updated (usually within a short delay after an individual passes).	
People Entry Rate Too High	People Entry Rate Too High	Video	Generated when the number of entering people rises above the limit during the specified time interval.	

Alarm	Event	Event Type	Description	Duress*
People Entry Rate Too High Restored	People Entry Rate Too High Restored	Video	Generated when the number of entering people returns to a value below the limit during the specified time interval.	
People Entry Rate Too Low	People Entry Rate Too Low	Video	Generated when the number of entering people falls below the limit during the specified time interval.	
People Entry Rate Too Low Restored	People Entry Rate Too Low Restored	Video	Generated when the number of entering people returns to a value above the limit during the specified time interval.	
People Exit Rate Too High	People Exit Rate Too High	Video	Generated when the number of exiting people rises above the limit during the specified time interval.	
People Exit Rate Too High Restored	People Exit Rate Too High Restored	Video	Generated when the number of exiting people returns to a value below the limit during the specified time interval.	
People Exit Rate Too Low	People Exit Rate Too Low	Video	Generated when the number of exiting people falls below the limit during the specified time interval.	
People Exit Rate Too Low Restored	People Exit Rate Too Low Restored	Video	Generated when the number of exiting people returns to a value above the limit during the specified time interval.	
Pick Up	Pick Up	POS	Transaction indicating a pick up has occurred.	
Point Enabled	Point Enabled	System		
Point Disabled	Point Disabled	System		
Poor Video Visibility Restored	N/A	N/A	Generated when the video quality returns to an acceptable level.	
Power Failure Active	Power Failure	System	Generated when a power failure condition has been detected.	
Power Failure Restored	Cancelled Power Failure	System	Generated when the power failure condition was restored.	

Alarm	Event	Event Type	Description	Duress*
Pre-Alarm	Pre-Alarm	System	An event indicating a pre-alarm condition is active.	
Pre-Alarm Clear	Pre-Alarm Clear	System	An event indicating a pre-alarm condition is no longer active.	
Price Lookup	Price Lookup	POS	Generated when a price lookup has taken place.	
Quantity or Weight	Quantity or Weight	POS	An event indicating a quantity or weight.	
Reader Input Tamper Active	Reader Input Tamper	System	Generated when the reader input tamper has gone active.	
Reader Low Battery	Reader Low Battery	System	Reader low battery alarm.	
Reader Low Battery Restored	Reader Low Battery Restored	System	Generated when a reader low battery is restored.	
Reader Input Tamper Restored	Reader Input Tamper Cancelled	System	Generated when the reader input tamper was restored.	
Reader Mode Blocked	Reader Mode Blocked	System	Lock has entered blocked mode.	
Reader Mode Secured	Reader Mode Secured	System	Lock has entered secured mode.	
Reader Mode Unsecured	Reader Mode Unsecured	System	Lock has entered unsecured mode.	
Reader Mode Card and Pin	Reader Mode Card and Pin	System	Generated when the reader mode has changed to “Pin and Card” for the device.	
Reader Mode Card Only	Reader Mode Card Only	System	Generated when the reader mode has changed to “Card Only.”	
Reader Mode Facility Code	Reader Mode Facility Code	System	Generated when the reader mode has changed to “Facility Code Only.”	
Reader Mode First Card Unlock	Reader Mode First Card Unlock	System	Generated when the reader mode has changed to “First Card Unlock.”	
Reader Mode Locked	Reader Mode Locked	System	Generated when the reader mode has changed to “Locked.”	
Reader Mode Pin or Card	Reader Mode Pin or Card	System	Generated when the reader mode has changed to “Pin or Card” for the device.	

Alarm	Event	Event Type	Description	Duress*
Reader Mode Unlocked	Reader Mode Unlocked	System	Generated when the reader mode has changed to “Unlocked.”	
Reader Module Firmware Upgraded	Reader Module Firmware Upgraded	System	Reader firmware has been updated.	
Reader Motor Stalled	Reader Motor Stalled	System	Generated when the motor stalls on a reader.	
Reader Motor Stalled Restored	Reader Motor Stalled Restored	System	Generated when a motor stalled condition has been restored.	
Reader Reset	Reader Reset	System	Generated when the firmware resets the reader. This can happen if the reader is brand new or in the case of a failed/ incomplete download. Internal conditions, such as a possible corrupt memory, can also cause the firmware to reset. In these cases, the firmware will rewrite its entire storage with default values, overwriting the downloaded values. When this happens, the user must reprogram the lockset.	
Realtime Clock Updated	Realtime Clock Updated	System	The Real Time Clock (RTC) was updated.	
Register X Report	Register X Report	POS	Indicates a X report was generated. X reports are financial, end of day, clerk, etc. reports.	
Register Z Report	Register Z Report	POS	Indicates a Z report was generated. Z reports are the same as X reports, but resets totals to zero.	
Rejected Biometric Score	Rejected Biometric Score	Biometric	This event returns the rejected biometric score (the actual denied event is sent separately).	
Relay Contact Activated	Relay Contact Activated	System	Generated when a relay contact was activated.	
Relay Contact Deactivated	Relay Contact Deactivated	System	Generated when a relay contact was deactivated.	

Alarm	Event	Event Type	Description	Duress*
Removed Object	Removed Object	Video	Generated when an object which was part of the background is detected as missing.	
Removed Object Restored	Removed Object Restored	Video	Generated when the object is returned to its original location or the background (after a certain time interval) is relearned.	
Request to Exit - Door Used	Request to Exit - Door Used	System	Generated when the request to exit is granted and the door is used. **Note:** If the **Assumed Door Used** checkbox is selected on the Readers form, then the door is assumed to be used. This might interfere with this event.	
Request to Exit - Door Not Used	Request to Exit - Door Not Used	System	Generated when the request to exit is granted and the door is not used. **Note:** If the **Assumed Door Used** checkbox is selected on the Readers form, then the door is assumed to be used. This might interfere with this event.	
Retrieved	Retrieved	Intercom	Generated when a phone call is retrieved/answered.	
Ringing	Ringing	Intercom	Generated when an intercom station/phone is ringing.	
Runaway Device	Runaway Device	System	Generated when the conditions specified for a runaway state are met. These conditions are configured on the System Options > Runaway Detection tab in System Administration.	

Alarm	Event	Event Type	Description	Duress*
Runaway Device Restored	Runaway Device Restored	System	Generated when the conditions configured for runaway detection are no longer true.	
Running Out of Disk Space	Running Out of Disk Space	NetDVMS	Generated when the live recording drive for the camera is running low on disk space. The criteria for generating this alarm is determined by the size of the drive and where the archive drive is located. For more information, refer to the NetDVMS documentation.	
Sales Subtotal	Sales Subtotal	POS	A transaction that reports the sale subtotal	
Schedule Change	Schedule Change	System	Generated when a schedule, added in the Scheduler, is changed.	
Schedule Executed	Schedule Executed	System	Generated when a schedule, added in the Scheduler, is executed.	
Scheduler Action Executed	Scheduler Action Executed	System	Generated when a scheduler action has executed.	
Scheduler Action Failed	Scheduler Action Failed	System	Generated when a scheduler action has failed.	
Security Alarm Acknowledge	Security Alarm Acknowledge	Fire	Generated when a security alarm has been acknowledged.	
Security Alarm Block Acknowledge	Security Alarm Block Acknowledge	Fire	Generated when all security alarms have been acknowledged at the fire panel.	
Security Alarm In	Security Alarm In	Fire	Generated when a new security alarm has been detected for the device.	
Security Alarm Out	Security Alarm Out	Fire	Generated when a device with a previous security alarm has returned to its normal state.	
Shorted Line Active	Shorted Line Alarm Active	System	Generated when a shorted line fault condition has been detected.	

Alarm	Event	Event Type	Description	Duress*
Shorted Line Restored	Canceled Shorted Line	System	Generated when a device with a shorted line fault condition has returned to its normal state.	
Signal Silence	Signal Silence	Fire	Generated when the alarm signal on the hardware has been silenced.	
Smart Card Authentication Failed	Smart Card Authentication Failed	System	Generated when a smart card authentication failed.	Yes
Smart VMD	Smart VMD	Video	Generated when a change is detected.	
Smart VMD Restored	Smart VMD Restored	Video	Generated 8 seconds after the last detection of a Smart VMD event.	
Status In	Status In	Fire	Generated when a status reporting device is active.	
Status - Missing Fire Supervision	Status - Missing Fire Supervision	Fire	Fire supervision is missing.	
Status Out	Status Out	Fire	Generated when a status reporting device has returned to the inactive state.	
Storage Failure	Storage Failure	Video	Indicates that something is wrong related to recording/ retrieving video to/from hard drives.	
Store Coupon	Store Coupon	POS	Indicates a store coupon.	
Supervisory Acknowledge	Supervisory Acknowledge	Fire	Generated when a supervisory condition has been acknowledged.	
Supervisory Block Acknowledge	Supervisory Block Acknowledge	Fire	Generated when all supervisory conditions have been acknowledged at the fire panel.	
Supervisory In	Supervisory In	Fire	Generated when a new supervisory condition has been detected for the device.	
Supervisory Out	Supervisory Out	Fire	Generated when a device with a previous supervisory condition has returned to its normal state.	
System Reset	System Reset	Fire	Generated when the fire panel has been reset.	

Alarm	Event	Event Type	Description	Duress*
Tax Amount	Tax Amount	POS	Event that indicates the tax amount.	
Taxable Subtotal	Taxable Subtotal	POS	Transaction that reports the taxable subtotal	
Timeout Exceeded - No Second Card	Timeout Exceeded - No Second Card	Area Control	Generated when no second card was presented within the time limit for the area/ reader using two-man control.	Yes
Time Out-Of-Sync	Time Out-Of-Sync	Video	Generated when the time stamp feature is enabled and the time on the camera has a difference of 20 seconds or more from the video recorder time.	
Time Out-Of-Sync Restored	Time Out-Of-Sync Restored	Video	Generated when the time difference between the camera and video recorder returns to less than 20 seconds.	
Total Amount Due	Total Amount Due	POS	Transaction indicating the total amount due.	
Transaction Number	Transaction Number	POS	Event Generated that indicates the transaction number of the sales transaction.	
Transfer, Diagnostics	Transfer, Diagnostics	System	Generated when a user is connected to the device for diagnostic purposes.	
Transfer, History	Transfer, History	System	Generated when a history data was transferred from the device to the parent device.	
Transfer, PDA To Lock	Transfer, PDA To Lock	System	Generated when the device (lockset) is programmed/ reprogrammed through a download from a Mobile Configurator.	
Transferred Call		Intercom	Generated if an intercom call is transferred.	
Transmitter Alarm	Transmitter Alarm	Transmitter	Generated when the button or input on a transmitter has been activated.	
Transmitter Alarm Restored	Transmitter Alarm Restored	Transmitter	Generated when the transmitter alarm has been restored.	

Alarm	Event	Event Type	Description	Duress*
Transmitter Inactivity	Transmitter Inactivity	Transmitter	Transmitter has been inactive longer than the supervision interval	
Transmitter Low Battery	Transmitter Low Battery	Transmitter	Transmitter low battery alarm	
Transmitter Low Battery Restored	Transmitter Low Battery Restored	Transmitter	Generated when a transmitter low battery has been restored.	
Transmitter Pre-Tilt	Transmitter Pre-Tilt	Transmitter	Generated when the transmitter is in the pre-tilt state.	
Transmitter Pre-Tilt Restored	Transmitter Pre-Tilt Restored	Transmitter	Generated when the transmitter has returned to normal from the pre-tilt state.	
Transmitter Pull Cord Alarm	Transmitter Pull Cord Alarm	Transmitter	Generated when the pull cord on a transmitter has been pulled and is in alarm.	
Transmitter Pull Cord Restored	Transmitter Pull Cord Restored	Transmitter	Generated when the transmitter pull cord alarm has been restored.	
Transmitter Tamper	Transmitter Tamper	Transmitter	Transmitter tamper alarm.	
Transmitter Tamper Restored	Transmitter Tamper Restored	Transmitter	Generated when a transmitter tamper has been restored.	
Transmitter Temporary Tilt Disable	Transmitter Temporary Tilt Disable	Transmitter	Generated when the transmitter temporary tilt has been disabled.	
Transmitter Tilt	Transmitter Tilt	Transmitter	Generated when a tilt condition on the transmitter has been detected.	
Transmitter Tilt Disabled	Transmitter Tilt Disabled	Transmitter	Generated when the transmitter tilt function has been disabled.	
Transmitter Tilt Enabled	Transmitter Tilt Enabled	Transmitter	Generated when the transmitter tilt function has been enabled.	
Transmitter Tilt Restored	Transmitter Tilt Restored	Transmitter	Generated when the tilt condition on the transmitter has been restored.	
Transmitter Acknowledge	Transmitter Acknowledge	Transmitter	This event is reported when an alarm generated by a transmitter has been acknowledged.	

Alarm	Event	Event Type	Description	Duress*
Transmitter No Response	Transmitter No Response	Transmitter	This event is reported when an alarm generated by a transmitter has not been acknowledged.	
Transmitter Touch Alarm	Transmitter Touch Alarm	Transmitter	Alarm generated by a transmitter when the item it is protecting is touched.	
Transmitter Removal Alarm	Transmitter Removal Alarm	Transmitter	Alarm generated by a transmitter when an item it is protecting is removed.	
Trouble Acknowledge	Trouble Acknowledge	Fire	Generated when the trouble condition has been acknowledged.	
Trouble Acknowledge Clear	Trouble Acknowledge Clear	Fire	Generated when a trouble condition that has been cleared from the system has been acknowledged by a user.	
Trouble Bell #	Trouble Bell 1 or 2	Relay/ Sounder	Generated when Trouble bell 1 or 2 is in alarm.	
Trouble Bell # Restore	Trouble Bell 1 or 2 Restore	Relay/ Sounder	Generated when Trouble bell 1 or 2 is restored.	
Trouble Block Acknowledge	Trouble Block Acknowledge	Fire	Generated when all trouble conditions have been acknowledged at the fire panel.	
Trouble In	Trouble In	Fire	Generated when a new trouble condition has been detected for the device.	
Trouble Out	Trouble Out	Fire	Generated when a device with a previous trouble condition has returned to its normal state.	
Unanswered Call	Unanswered Call	Intercom	Generated if a ringing intercom call goes unanswered.	
Unexpected Access	Unexpected Access	System	Generated when a user successfully exits using an unexpected exit reader, after gaining access to a specific entry reader, and the “must proceed to exit readers” option is enabled.	

Alarm	Event	Event Type	Description	Duress*
Unexpected Access Attempt	Unexpected Access Attempt	System	Generated when a user attempts to exit using an unexpected exit reader, after gaining access to a specific entry reader, and the “must proceed to exit readers” option is enabled.	
Unknown Elevator Terminal	Unknown Elevator Terminal	System	Generated when an elevator terminal is detected that has not been configured in the system.	
Unknown User Command	Unknown User Command	System	Generated when an unknown user command is entered through a reader. For example, if a cardholder enters the command *1234# (where that command means nothing) an unknown user command alarm is sent to Alarm Monitoring. The numbers entered as the command are used as the event text for the alarm.	
Unlocked Under AFC	Unlocked Under AFC	System	Lock has entered AFC state.	
Unlocked Mode Change Denied: Blocked Mode	Unlocked Mode Change Denied: Blocked Mode	System	Automatic scheduled change to unlocked mode was denied because lock is in blocked mode.	
Unlocked Mode Change Denied: Low Battery	Unlocked Mode Change Denied: Low Battery	System	Automatic scheduled change to unlocked mode was denied due to low battery condition.	
Unlocked Mode Change Denied: Secured Mode	Unlocked Mode Change Denied: Secured Mode	System	Automatic scheduled change to unlocked mode was denied because lock is in secured mode.	
Unlocked Under First Card Unlock	Unlocked Under First Card Unlock	System	First card unlock mode; door is unlocked.	
Unsupported Hardware	Unsupported Hardware	System	Generated when hardware that is not supported is added to the system.	
Untyped Abort	Untyped Abort	Trouble	Generated when an alarm for a device of an unknown type has been aborted/ canceled.	

Alarm	Event	Event Type	Description	Duress*
Untyped Alarm	Untyped Alarm	Trouble	Generated when an alarm for a device of unknown type occurs.	
Untyped Alarm Restore	Untyped Alarm Restore	Trouble	Generated when the device of an unknown type is restored.	
Untyped Bypass	Untyped Bypass	Trouble	Generated when a device of an unknown type has been bypassed.	
Use Limit Exceeded	Use Limit Exceeded	Denied	Access was denied because the use limit for the badge has been exceeded.	Yes
User Failed to Reach Destination	User Failed to Reach Destination	System	Generated when a user fails to exit at a specific exit reader, after gaining access to a specific entry reader, before the timeout value expires.	
User Generated Video Event	User Generated Video Event	Video	Video events are typically created automatically by the system based on an event from an external device. This allows the user to generate an event that is not tied to any device. It can be created from any camera with any user defined time limit from within the video player window in Alarm Monitoring. This event can then be included in reports, or have a trace performed like any other event in the system.	
Value Added	Value Added	POS	Event that indicates value added.	
Video Event Threshold Reached	Video Event Threshold Reached	Video	Generated when the user-defined event threshold has been reached and exceeded. (The percent of disk space used by video events has been reached, typically signaling the archive server to start archiving or purging.)	
Video Failover Failed	Video Failover Failed	Video	Generated when the camera is configured for failover and failover cannot be activated on this camera.	

Alarm	Event	Event Type	Description	Duress*
Video Failover Restored	Video Failover Restored	Video	Generated when the camera is configured for failover and secondary recorder is currently recording video from the camera and secondary recorder determined that the primary recorder came back online and started recording video from the camera. Secondary recorder will stop recording video from the camera. Alarm Monitoring users should log off of the application and back on when the primary recorder comes back online.	
Video Failover Started	Video Failover Started	Video	Generated when the camera is configured for failover and secondary recorder determined that the primary recorder is not recording video from the camera, so secondary recorder starts recording from this camera. Alarm Monitoring users should log off of the application and back on when failover occurs.	
Video Graininess Restored	N/A	N/A	Displayed after noise (graininess) in the video has been reduced.	
Video Overflow Restored	Video Overflow Restored	Video	Generated when the recorder is no longer having troubles handling incoming video.	
Video Overflow Started	Video Overflow Started	Video	Generated when the recorder determined that it cannot handle incoming video. Usually it happens when hard drive or CPU utilization is close to 100%, so recorder cannot keep up with amount of video.	

Alarm	Event	Event Type	Description	Duress*
Video Server Disk Full	Video Server Disk Full	Video	Generated when the user-defined event threshold has been exceeded by 5% or more. (The percent of disk space used by video events has been exceeded by at least 5%, typically signaling the archive server to start archiving or purging.) If a user-defined event threshold has not been defined, this alarm/event will be generated when the video server disk space is 75% full of video events.	
Video Server is Not Recording	Video Server is Not Recording	Video	Generated when it has been detected that the video recorder is no longer recording. A check is done periodically (default is every 10 minutes) to check to make sure that video is still being recorded. This event is generated when the check fails.	
Video Source Signal Lost	Video Source Signal Lost	Video	Generated when the video signal from a channel is lost from the video server. This alarm may be accompanied by a Communications Lost alarm.	
Video Source Signal Restored	Video Source Signal Restored	Video	Generated when the video signal from a channel is restored to the video server. This alarm maybe accompanied by a Communications Restored alarm.	
Video Storage Unavailable	Video Storage Unavailable	Video	Generated when the recorder cannot record video to a drive.	
Void or Error Correction	Void or Error Correction	POS	Transaction that indicates a void or error correction	

Alarm	Event	Event Type	Description	Duress*
Walk Test ##	Walk Test ##	Fire	Generated when walk test ## is initiated. A walk test is used to test devices in the system and report devices addressed incorrectly. The device and the first zone programmed for this device are reported with each message.	
Walk Test Uninstalled	Walk Test Uninstalled	Fire	Generated when the reported device was part of a walk test and has been physically disconnected from the system.	
Walk Test Unprogrammed	Walk Test Unprogrammed	Fire	Generated when the reported device was part of a walk test and has been removed from the system (it is not longer configured in the system).	
Walk Test Untest	Walk Test Untest	Fire	Generated when the reported device is no longer being tested (part of a walk test).	
Warning: Poor Visibility	N/A	N/A	This warning appears when the camera's view of a scene is impaired by glare, fog, etc. The sensitivity of the Poor Visibility warning can be adjusted in the Channel Configuration dialog.	
Warning: Video Graininess	N/A	N/A	This warning appears when the video is noisy (grainy.) The alarm may also be generated in scenes with very fine detail, such as heavy vegetation.	
Wireless Smoke Detector	Wireless Smoke Detector	Fire	A wireless smoke detector has generated an alarm.	
WLM Firmware Upgraded	WLM Firmware Upgraded	System	Radio module firmware was updated	

* The duress column marks which alarm events can be used as duress events if your system is configured for duress.

Appendix B: Reports

Reports are installed when Database Setup is run. All reports are installed on the database server under the ReportTemplates subdirectory in the ReadykeyPRO installation path. By default, this location is **C:\Program Files\ReadykeyPRO\ReportTemplates**.

Note: For custom reports you must use the actual data field and not the internal database ID.

Note: Refer to the release notes for the versions of Seagate Crystal Reports that are supported. The release notes are located on the root of the ReadykeyPRO installation disc.

Report name	Description
Access Denials and Grants, by Reader	Badge-related events, grouped by reader.
Access Denials, Grants and Other Badge Events	All badge-related events, including time, reader, badge and cardholder name. All badge events will be shown.
Access Denied Events	All Access Denied events, including time, reader, badge, and cardholder name.
Access Denied Events, by Reader	Access Denied Events, grouped by reader.
Access Granted Events	All Access Granted events, including time, reader, badge, and cardholder name.
Access Granted Events, by Reader	Access Granted events, grouped by reader.
Access Groups	Lists all Access Groups and the Access Levels contained in each group.
Access Groups With Levels	Access Group definitions including access level details.
Access Level Assignments to Cardholders	Listing of each Access Level, with each cardholder that has that access level assigned to them. Also summarizes the total number of badges that need to be downloaded.
Access Level Assignments to Cardholders, by Segment	Listing of each Access Level by Segment, with each cardholder that has that access level assigned to them. Also summarizes the total number of badges that need to be downloaded to each segment. This report is valid only for systems using Segmentation.
Access Levels	Access Level definitions.
Access Panels	Access Panel definitions.
Active Visits, by Host Name	Lists all visits that are currently active (not signed out), grouped by host name.

Report name	Description
Active Visits, by Visitor Name	Lists all visits that are currently active (not signed out), grouped by visitor name.
Alarm Acknowledgments	All alarm acknowledgments, including the alarm information and acknowledgment notes.
Alarm Acknowledgments, by Definition	All alarm acknowledgments, grouped by alarm definition.
Alarm Acknowledgments, by Operator	All alarm acknowledgments, grouped by system operator.
Alarm Acknowledgments, by Panel	All alarm acknowledgments, grouped by panel.
Alarm Configuration	Alarm configuration summary.
Alarm Input Events	All alarm input events by date.
Alarm Panel Inputs	Lists all alarm panel inputs, grouped by main panel and alarm panel.
Alarm Panel Local Linkage	Lists alarm input/output local links on alarm panels.
Alarm Panel Outputs	Lists all alarm panel outputs, grouped by access panel and alarm panel.
Alarm Panels	Lists all alarm panels, grouped by parent panel.
All Cardholders With Logical Access	Lists all cardholders that have linked logical access accounts.
All Events Over Time	A listing of all event types over time.
All Events Over Time With Local Panel Time	Lists all event types over time. This report also shows the time an event occurred in the panel’s time. **Note:** This report might generate slowly.
All Events Over Time With Unique Alarm ID	A listing of all event types over time with unique alarm IDs.
Anti-Passback Events	All anti-passback events over time.
Area Configuration	Lists all areas, including the reader entrances and exits.
Area Entrance History	History of all cardholders entering areas, sorted by area and date.
Asset Classes	Lists all asset classes and the asset groups to which they belong.
Asset Events	All events having to do with assets.
Asset Groups	Lists all asset groups and the classes they contain.
Asset Types	Lists all defined asset types and their subtypes.

Report name	Description
Assets, by Scan ID	Lists all assets, sorted by Scan ID.
Assets, by Type	Lists all assets, sorted by type and subtype.
Assigned Assets by Type, Scan ID	Lists all currently assigned assets, sorted by type and Scan ID.
Assigned Assets, by Cardholder	Lists all currently assigned assets, sorted by cardholder.
Assigned Assets, by Scan ID	Lists all currently assigned assets, sorted by Scan ID.
Audio Notifications and Instructions	Lists all audio notifications and instructions in the database.
Badge Type Configuration	Lists all badge types that have been configured in the system.
Badges Without Access Levels	Lists all badges with no assigned access levels.
Badges, by Deactivate Date	Listing of all badges by deactivate date. Can be used to determine which badges are about to expire.
Card Formats	Definitions of all Magnetic and Wiegand card formats in the system. This combined report replaces the Magnetic Card Formats and Wiegand Card Formats reports that were available with previous software releases.
Cardholder Access to Readers	Listing of each reader, and which cardholders have access to that reader. Includes the associated access level and timezone.
Cardholder Exit/ Entry	Displays user-defined Exit/Entry on a per-cardholder basis. To run this report, readers must be designated as ‘Time and Attendance’ Entrance or Exit readers on the Readers/Controls page. This is not an Area report.
Cardholder Photo Gallery	All cardholder photos, sorted by name.
Cardholder Precision Access to Readers	Listing of each reader, and which cardholders have precision access to that reader. Includes the associated precision access and time zone.
Cardholder Time and Attendance	Pairs each in-time with an out-time for cardholders gaining entry to time and attendance readers.
Cardholders Located in Each Area, by Date	List of the cardholders located in each area, sorted by area and date.
Cardholders Located in Each Area, by Name	List of the cardholders located in each area, sorted by area and cardholder name.
Cardholders With Access, by Badge Type	All cardholders with active badges that have access, sorted by badge type. Includes access level assignments.
Cardholders With Access, by Last Name	All cardholders with active badges that have access, sorted by last name. Includes access level assignments.

Report name	Description
Cardholders With Precision Access, by Badge Type	All cardholders with active badges that have access, sorted by badge type. Includes precision access level assignments.
Cardholders With Precision Access, by Last Name	All cardholders with active badges that have access, sorted by last name. Includes precision access level assignments.
Cardholders, by Badge Type	All cardholders sorted by badge type, no access levels shown. **Note:** Only personnel with badges assigned will be included in this report.
Cardholders, by Last Name	All cardholders sorted by last name, with badges but no access levels. **Note:** Only personnel with badges assigned will be included in this report.
CCTV Instructions	Summary of all CCTV instructions in the database.
Continuous Video	Lists all of the times that there has been continuous video archived.
Current Visits	Lists all currently signed in visits.
Destination Assurance Configuration	Lists all entrance readers, their settings, and the associated exit readers.
Destination Assurance Exempt Cardholders	Lists all cardholders who have a badge that is exempt from destination assurance.
Device Status Events	Status events for all devices.
Dialup Events, by Panel	Lists all dialup events, grouped by panel.
Dialup Last Connect Time	Lists online dialup panels, and the last time they were connected.
Elevator Access Denied and Granted Events	All Access Denied and Granted events for elevator readers with the Track Floors option enabled. Includes time, reader, badge, cardholder name, and the floor to which access was attempted. All access denials and grants are shown.
Elevator Dispatching Devices and Terminals	Lists all elevator dispatching devices with the configured terminals.
Elevator Floor Assignments to Cardholders	Lists all cardholders that have access to a particular elevator floor list.
Emergency Events	All emergency events over time.
Event Codes	Event code templates and event code mapping configuration.
Event Count, by Panel	A count of all events, grouped by panel. Includes a pie chart graphic of the event counts.
Fire Device Input/ Outputs	Lists all fire input/outputs, grouped by panel and fire device.

Report name	Description
Global Area/ Occupancy, by Date	Shows the last known area accessed by each cardholder, sorted by date and time.
Global Area/ Occupancy, by Name	Shows the last known area accessed by each cardholder, sorted by name.
Global I/O Linkages	Lists all of the global I/O linkages, including the input events and output actions.
Guard Tour Configuration	Lists all of the configured guard tours including checkpoints, actions, and messages.
Guard Tour History	Lists all of the events, associated with checkpoints, that happened for each guard tour.
Hardware Panels	Lists all top-level hardware panels by category, including access, fire, intercom, and personal safety.
Holidays	Lists all system holiday definitions.
ILS Lock Authorizations, by Cardholder	Lists ILS lock authorization levels assigned to the cardholder/badge, sorted by cardholder.
ILS Authorizations, by Level	Lists ILS lock authorization levels assigned to the cardholder/badge, sorted by level.
ILS Lock Battery Status, by Status	Lists ILS lock battery status, grouped by battery status (Low to High), wireless gateway, and battery percent.
ILS Lock Characteristics	Lists ILS lock configuration details, sorted by lock name.
ILS Lock Communications	Lists ILS wireless lock diagnostics, sorted by lock name.
ILS Lock Ownership	Lists the ILS locks owned by a cardholder.
Intercom Functions	Lists all defined intercom functions.
Intercom Stations	Lists all intercom stations, grouped by intercom exchange.
Intrusion Command Authority - Advanced	Lists all cardholders that have access level assignments configured to use advanced intrusion command authority.
Intrusion Command Authority - Global	Lists all cardholders who are assigned access levels with global intrusion command authority.
Intrusion Command Events	Lists all events associated with intrusion commands, including device, cardholder name, and badge.
Intrusion Detection Areas	Lists all intrusion areas grouped by panel.
Intrusion Detection Devices	Lists all of the intrusion detection devices grouped by panel.
Intrusion Panel User Groups	Lists all panel users grouped by panel user groups.

Report name	Description
Last Location of Cardholders	Shows the last reader accessed by each cardholder, sorted by cardholder name.
Locked Video Events	Lists all system events with associated locked video events.
Maps	List of available maps in the database.
Mobile Verify User Transaction Log	Chronological log of all transactions performed.
Mobile Verify User Transaction Log, by Operation	Chronological log of all transactions performed, grouped by operation.
Mobile Verify User Transaction Log, by User ID	Chronological log of all transactions performed, grouped by User ID.
Module Details	Lists all module definitions, grouped by parent panel.
Module Summary	Lists all modules, grouped by parent panel.
Monitor Stations	Lists all alarm monitoring stations defined in the system, including which monitor zones and access panels they are monitoring.
Monitor Zones	Lists all Monitoring Zone definitions.
Overdue Visits	Lists all scheduled visits that have not signed in.
Overstayed Visits	Lists all visitors logged into the facility, but whose badge or visit has expired.
Permission Profiles	Lists all permission profile definitions.
Personal Safety Transmitter Assignments	Lists all assignments of personal safety transmitters to cardholders, assets, and so on.
Personal Safety Transmitters	Lists all personal safety transmitters.
Personnel Without an Active Badge	Lists all personnel in the database who do not have an active badge assigned to them.
Personnel, by Last Name	Lists all personnel in the database, with basic information only.
Personnel, Organization Details	Lists all personnel in the database, with organization details. This report is designed for the standard cardholder layout. It might not work with user-customized cardholder layouts.
Personnel, Personal Details	Lists all personnel in the database, with personal details. This report is designed for the standard cardholder and visitor layout. It might not work with user-customized cardholder and visitor layouts.
Point of Sale Registers	Lists all point of sale registers by point of sale device.
Precision Access Groups	Precision Access Group definitions.
Reader Assignments to Cardholders	Lists all cardholders that have access to a particular reader.

Report name	Description
Reader Command Programming Configuration	Lists all command programming readers along with the associated user and instant commands.
Reader Precision Access Assignments to Cardholders	Lists all cardholders that have precision access to a particular reader.
Reader Status Events	All reader status events, grouped by reader.
Reader Timezone Schedules	Reader timezone scheduling for reader modes.
Readers	Reader definitions, grouped by access panel.
Receiver Account Alarm Activity	Lists all alarm activity for receiver accounts including notes and elapsed times.
Receiver Account Areas	Lists all receiver account areas, grouped by receiver account.
Receiver Account Groups	Lists all receiver account groups and the receiver accounts contained in each group.
Receiver Account Zones	Lists all receiver account zones, grouped by receiver account.
Receiver Accounts	Lists all receiver accounts.
Receiver Accounts That Failed to Report	Lists all of the receiver accounts that failed to report during their duration.
Receiver and Receiver Account Events	Lists all the events that occurred on a receiver or receiver account.
Segment Badge Download Summary	For each segment, lists the count of badges that must be downloaded to the access panels in that segment. This report is valid only for systems that use the Segmentation feature.
Segments	Lists all segments defined on the system and their options. This report is valid only for systems that use the Segmentation feature.
SNMP Agents	Lists all SNMP agents sorted by segment and name.
SNMP Management Information Base Configuration	Lists all MIB data, grouped by enterprise.
System Servers	Lists all servers defined on the system.
Text Instructions and Acknowledgment Notes	Lists all text instructions and acknowledgment notes.
Timezones	Lists all timezone definitions.
User Permissions	Lists all system users and their permissions.
User Transaction Log	Chronological log of all transactions performed on the system by users.
User Transaction Log, by User ID	Chronological log of all transactions performed on the system, grouped by User ID.

Report name	Description
Users With Area Access Levels to Manage	Lists all Area Access Manager users and the access levels they manage.
Video Camera Device Links	Lists the device links for each camera.
Video Cameras	Lists all video cameras, grouped by video server.
Video Servers	Lists all video servers.
Visit History	History of all visits in the system.
Visit History With Host	History of all visitors that visited the facility with their host.
Visitors	Lists all visitors in the system. **Note:** This report might not run properly if you have deleted the default visitor fields using FormDesigner.

Appendix D: IntelligentAudio

IntelligentAudio performs audio analysis on forensic (live or recorded) video in Alarm Monitoring or VideoViewer. The Video Search can be used to monitor live or scan recorded video for audio events. Searches can be performed based on the type and volume of sound detected.

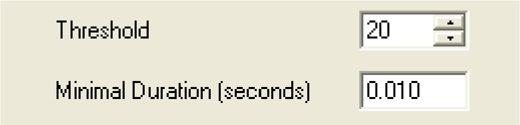
The Audio Level event can be configured in System Administration to trigger alarms in Alarm Monitoring. For more information, refer to the Digital Video Software User Guide.

Once Video Search is launched, select an IntelligentAudio event from the **Event** > **Select Event** > **IntelligentAudio** menu.

Audio Level

The Audio Level event identifies sound events crossing a volume threshold.

Event Properties



Threshold: 20

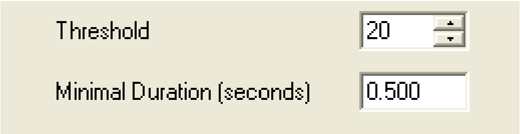
Minimal Duration (seconds): 0.010

Property	Description
Threshold	Volume threshold for detection. Use the level displayed on the Event Feedback pane to determine a value appropriate to the scene.
Minimal Duration (seconds)	Length of time that sound should continue before an event is detected. The range of values is 0.010 to 10.000 seconds.

High Pitch Sounds

Typical high pitch sounds include: screams, sirens, squealing tires, etc.

Event Properties



Threshold: 20

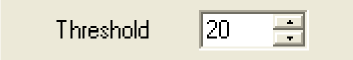
Minimal Duration (seconds): 0.500

Property	Description
Threshold	Volume threshold for detection. Use the level displayed on the Event Feedback pane to determine a value appropriate to the scene.
Minimal Duration (seconds)	Length of time that sound should continue before an event is detected. The range of values is 0.060 to 10.000 seconds.

Impact Sounds

Typical impact sounds include: fallen object, crash, gunshot, etc.

Event Properties



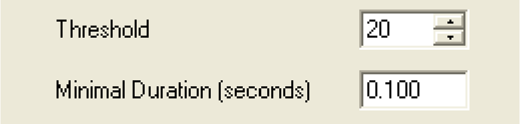
Threshold 20

Property	Description
Threshold	Volume threshold for detection. Use the level displayed on the Event Feedback pane to determine a value appropriate to the scene.

Unclassified Sounds

The Unclassified Sounds event can be used to detect sounds not classified as impact or high pitch. For example, undefined noise, speech, car starting, etc.

Event Properties



Threshold 20

Minimal Duration (seconds) 0.100

Property	Description
Threshold	Volume threshold for detection. Use the level displayed on the Event Feedback pane to determine a value appropriate to the scene.
Minimal Duration (seconds)	Length of time that sound should continue before an event is detected. The range of values is 0.060 to 10.000 seconds.

Appendix E: Bosch ILS (Integrated Locking Solutions)

This section contains information about using ILS locking solutions in Alarm Monitoring, in particular, the ILS wireless locking solution. For instructions on configuring the ILS locking solutions in ReadykeyPRO, refer to the System Administration User Guide.

Offline Locks

Offline locks include the following types:

- **ILS Offline Locks .** The lock operator reads the audits (events) from the ILS offline lock using the portable programmer (Mobile Configurator).
- **ILS Integra Locks .** These are also offline locks. The lock operator reads the audits (events) from the ILS Integra lock using the portable programmer (XPP).

For more information on using ILS offline and ILS Integra locks in Alarm Monitoring, refer to the following:

- Retrieve Events from an ILS Offline Lock on page 484
- View ILS Offline Lock Events on page 484
- Show the Operator Column on page 484
- Retrieve Events from an ILS Integra Lock on page 484

Wireless Locks

ILS wireless lock events are transmitted directly to Alarm Monitoring via the Wireless Gateway. You can also request wireless lock events on demand. For more information, refer to Retrieve Events from Wireless Locks on page 485.

For more information on using ILS wireless locks in Alarm Monitoring, refer to:

- Download ILS Wireless Locks on page 485
- Monitor ILS Wireless Lock Events on page 485
- View Wireless Lock Status on page 486
- Change Reader Access Modes on page 487
- Secure/Unsecure All Locks from a Reader Device Group on page 488
- View Wireless Diagnostics Information on page 489

For information on downloading ILS wireless firmware, refer to:

- Download Wireless Gateway Firmware on page 490
- Download ILS Wireless Lock Firmware on page 490

ILS Offline and ILS Integra Locks

Retrieve Events from an ILS Offline Lock

Complete the following steps to see the offline lock events in Alarm Monitoring:

1. Read the audits (events) at the ILS offline lock using the Mobile Configurator.
2. Disconnect the Mobile Configurator from the lock, and then connect it to a workstation where Communication Server and Alarm Monitoring are running. The lock events will automatically display in the Main Alarm Monitor window.

Important: If you are using a Mobile Configurator with ReadykeyPRO on a Windows XP or Windows 2003 system, Communication Server must be run as an application.

View ILS Offline Lock Events

When ILS offline lock events are uploaded from the Mobile Configurator to ReadykeyPRO:

- All other Mobile Configurators (ILS Offline panels) will show an online status in Alarm Monitoring.
- Events that have a lock operator associated with them will display with the operator name in the Operator column. By default, the Operator column is not shown.

Show the Operator Column

In order to enable this feature, complete the following steps:

1. Log into Alarm Monitoring.
2. Select **Columns** from the **Configure** menu.
3. Move “Operator” to the viewable columns list, and then click [OK].

Retrieve Events from an ILS Integra Lock

1. Read the audits (events) at the ILS Integra lock using the XPP portable programmer.
2. Disconnect the XPP from the lock, and then connect it to the workstation where it was configured. The lock events will automatically display in the Main Alarm Monitor window.

ILS Wireless Locks

Retrieve Events from Wireless Locks

From Alarm Monitoring, complete the following steps:

1. Open the system status tree. From the **View** menu, select **System Status**, and then select a new or existing window. Expand the ILS wireless panel icon to show the locks assigned to it.
2. In the system status tree, complete either of the following steps:
   a. Right-click on an ILS wireless panel and then select **Read Audits** to upload the events of all locks assigned to that panel.
   b. (Optional) Right-click on an individual ILS wireless lock and then select **Read Audits** to upload the events of that lock, exclusively.

   When the Read Audits command is successfully issued, the Wireless Gateway adds the request to the queue to send at the next lock heartbeat at which time the latest lock events will display in Alarm Monitoring.

Download ILS Wireless Locks

ILS wireless locks can be downloaded from the Alarm Monitoring system status tree.

From Alarm Monitoring, complete the following steps:

1. Open the system status tree. From the **View** menu, select **System Status**, and then select an existing window or open a new one. Expand the segment node.
2. Right-click on the ILS wireless panel icon, and then select **Download Database** to directly download the data from the locks assigned to the Wireless Gateway.
3. (Optional) You can download the ILS wireless panels from the System Administration system tree, the Readers and Doors folder, or the Access Panels folder. For more information, refer to the System Administration User Guide.

Monitor ILS Wireless Lock Events

ILS wireless lock events are reported in Alarm Monitoring by way of four (4) different mechanisms:

- Priority one events are sent immediately as soon as these events occur at the lock. For more information, refer to ILS Priority One Events in the System Administration User Guide.
- Non-priority events are retrieved at configurable intervals, and then sent at the next heartbeat. For more information, refer to the **Request audits** option in the System Administration User Guide.
- From Alarm Monitoring, you can request to have non-priority events sent at the next heartbeat by issuing the Read Audits command. For more information, refer to Retrieve Events from Wireless Locks on page 485.

- The Mobile Configurator read events (audits) at the lock and uploads them to ReadykeyPRO.

View Wireless Lock Status

The Alarm Monitoring system status tree provides information about the ILS wireless lock including firmware version, battery level, (reader) access mode, deadbolt, door forced, and door held status, and the maximum number of cardholders that can be stored in the lock.

Status Updates When the Lock is Online

Status	Updated Hardware Status	Events
Firmware version	Yes	Not applicable.
Battery level	Yes	Not applicable.
Access mode	Yes	Reader mode changes such as Reader Mode Blocked, Reader Mode Card Only, Reader Mode Facility Code Only, Reader Mode First Card Unlock, and Reader Mode Unlocked.
Deadbolt	Yes	Internal Deadbolt On Internal Deadbolt Off
Door forced	Not applicable	Door Forced Open Door Forced Open Restored
Door held	Not applicable	Door Held Open Door Held Open Restored

Some of the lock status information depends on proper event handling. It is recommended that you configure lock events the affect lock status as priority one to ensure you are viewing live information. Otherwise, the corresponding events will not be updated until they are received. For more information, refer to Monitor ILS Wireless Lock Events on page 485.

Recommendations:

- Configure the deadbolt, door forced, and door held events as priority one, and make sure to include both members of the event set such as Door Held Open and Door Held Open Restored. For more information, refer to “Configure ILS Priority One Events” in the System Administration User Guide.
- Configure the reader mode change events as priority one.

Note: The maximum number of cardholders supported by the lock is calculated from the current cardholder (badge) data. For more information, refer to “Calculate Maximum Cardholders” in the System Administration User Guide.

Note: Battery level shows the percent of battery power remaining. This information is intended to provide an estimate but, if the battery level drops off significantly over a short period of time, it is recommended that you replace the batteries. For instructions on replacing the batteries, refer to the ILS Lock Operation User Guide.

From Alarm Monitoring, complete the following steps:

1. Open the system status tree. From the **View** menu, select **System Status**, and then select a new or existing window.
2. Expand the ILS wireless panel icon, and then view the status of each wireless lock assigned to that device.

Change Reader Access Modes

You can issue a command to change the reader access mode of ILS wireless locks. For more information, refer to Lock Operation Mode Changes in the ILS Lock Operation User Guide.

Choices include:

- **Card Only**: Sets the lock to card only mode.
- **Unlocked**: Sets the lock to unlocked mode.
- **Facility Code Only**: Sets the lock to facility code only mode.
- **First Card Unlock**: Sets the lock to first card unlock mode. The first card unlock mode is a qualifier for online Reader Mode. When updated, the online Reader Mode is in effect until the first (qualified) access granted with entry occurs. When the first access granted with entry occurs, the online Reader Mode changes to unlocked.
- **Blocked**: Sets the reader (lock) to blocked mode. When a lock is placed into blocked mode it remains locked for all cardholders except those with blocking override privileges. A lock can only be placed into blocked mode when the lock is in card only or unlocked mode. After exiting the blocked mode the lock returns to the mode it was in previous to entering the blocked mode unless there is an automatic scheduled change.
- **Secure**: Sets the lock to secure mode and locks the door.
- **Unsecure**: Sets the lock to unsecure mode and unlocks the door following a secured lock.

Note: The lock can also be put into or taken out of Blocked, Secure, or Unsecure mode by presenting a Blocking, Emergency Lock, or Emergency Unlock card. For more information, refer to Special Purpose Cards in the System Administration User Guide.

From Alarm Monitoring, complete the following steps:

1. Open the system status tree. From the **View** menu, select **System Status**, and then select a new or existing window. Expand the ILS wireless panel icon to show the locks assigned to it.
2. In the system status tree, complete either of the following steps:
   a. Right-click on an ILS Wireless panel icon, select **Reader Access Modes**, and then the access mode for all locks assigned to that panel.
   b. (Optional) Right-click on an individual ILS wireless lock icon, select **Reader Access Modes**, and then the access mode for that lock, exclusively. When the Reader Access Modes command is successfully issued, the request is queued up at the Wireless Gateway waiting for the next heartbeat.
   c. (Optional) You can also change the reader access mode of all locks from a reader device group. For more information, refer to Reader Group Right-click Options on page 95. For adding an ILS wireless lock to a reader device group, refer to the System Administration User Guide.
      - Select **Device Groups** from the **View** menu. The Device Groups window displays the currently configured device groups within a monitoring zone. The Device Groups window allows you to view and change the status of reader devices.
      - Expand the Device Groups icon.
      - Right-click on the reader device group icon, and then select **Reader Access Modes**, and then the access mode for all locks in the group.

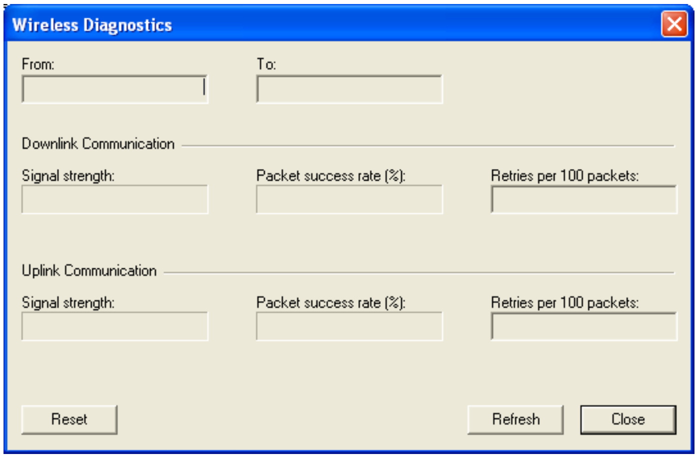
Secure/Unsecure All Locks from a Reader Device Group

In emergency situations, use the Secure All or Unsecure All command to lock or unlock all ILS wireless locks assigned to a reader device group. For more information, refer to Adding a Device Group in the System Administration User Guide and Access Control Procedures Checklist on page 58.

From Alarm Monitoring, complete the following steps:

1. Select **Device Groups** from the **View** menu. The Device Groups window displays the currently configured device groups within a monitoring zone. The Device Groups window allows you to view and change the status of reader devices.
2. Expand the Device Groups icon.
3. Right-click on the reader device group icon, and then select **Secure All**. All ILS wireless locks in the reader device group are locked and set to the secured mode.
4. (Optional) Right-click on the device group icon, and then select **Unsecure All**. All ILS wireless locks in the reader device group are unlocked and set to the unsecured mode.

Wireless Diagnostics Dialog



Wireless Diagnostics Dialog

Form Element	Comment
From/To	The time range for which the wireless diagnostics data is available for the lock. • **From:** mm/dd/yyyy hh:mm:ss AM/PM • **To:** mm/dd/yyyy hh:mm:ss AM/PM
Signal Strength	This is the relative signal strength being received by the antenna for unlink/downlink communication. Signal strength values range from 0 - 3 with the higher values indicating a stronger signal.
Packet success rate (%)	This is the average success rate of transferred packets for unlink/downlink communication. 100% indicates that all packets were transferred successfully (no loss).
Retries per 100 packets	This the average number of retry attempts per 100 packets for unlink/downlink communication. A value of zero (0) indicates no packets were retried. Values greater than zero (0) indicate that retries were attempted. Less retries is desirable.
Reset	Clears all diagnostic data stored for the lock.
Refresh	Updates the diagnostic information for the lock.
Close	Closes the Wireless Diagnostics dialog.

View Wireless Diagnostics Information

During each heartbeat, uplink/downlink communication data is stored for the ILS wireless lock. Uplink refers to the signal sent from the Wireless Gateway whereas downlink is the signal received by the lock. This information is used to calculate the wireless diagnostics from Alarm Monitoring to check the health of the wireless network.

The data is stored for a specified number of days. When the data is older than the specified days, the system automatically purges the lock's diagnostic information. For more information, refer to ILS System Options in the System Administration User Guide.

From Alarm Monitoring, complete the following steps:

1. Open the System Status Tree:
   a. From the **View** menu, select **System Status**, and then select a new or existing window.
   b. Expand the ILS wireless panel icon to show the locks assigned to it.
2. Right-click on the ILS wireless lock, and then select **View Wireless Diagnostics**. The Wireless Diagnostics dialog is displayed for the lock.

ILS Wireless Firmware

Important: It is recommended to use the most current version of the firmware.

The Wireless Gateway contains two (2) micro-controllers:

- Wireless WAP Module (WWM)
- WAP Main Controller (WMC)

ILS wireless locks have a reader unit and two (2) micro-controllers:

- Access Control Unit (ACU)
- Wireless Lock Module (WLM) - This is the radio unit.

The firmware for all of these controllers and the reader can be downloaded from Alarm Monitoring.

Note: Reader firmware is not available for magnetic type locks.

Download Wireless Gateway Firmware

From Alarm Monitoring, complete the following steps:

1. Open the System Status Tree. From the **View** menu, select **System Status**, and then select a new or existing window.
2. Right-click on the Wireless Gateway panel you want to upgrade, and then select **Download Firmware** > **Wireless Gateway**. The panel status shows the updated firmware version for the WWM and WMC when the download is completed successfully.

Download ILS Wireless Lock Firmware

In Alarm Monitoring, complete the following steps:

1. Open the System Status Tree.

a. From the **View** menu, select **System Status**, and then select a new or existing window.

b. Expand the Wireless Gateway panel icon to show the locks assigned to it.

2. Upgrade the firmware of all locks assigned to a Wireless Gateway. Right-click on the Wireless Gateway, and then select **Download Firmware** > **ACU**, **WLM**, or **Reader**.
3. (Optionally) Upgrade the firmware of individual wireless locks. Right-click on the lock you want to upgrade, and then select **Download Firmware** > **ACU**, **WLM**, or **Reader**.

   During the lock firmware download operation, the device status reports the progress:

   - "Firmware download pending" is displayed when the request is queued up at the Wireless Gateway while the system waits for the next lock heartbeat.
   - "Downloading firmware" is displayed when the locks receive the Download Firmware command from the Wireless Gateway and the download operation is started.
   - When the firmware download is complete, the displayed firmware versions are updated and the Main Alarm Monitor window shows the firmware upgraded events.

Index

Bosch Security Systems
130 Perinton Parkway
Fairport, NY 14450-9199
Customer Service: (800) 289-0096
Technical Support: (888) 886-6189