



S Y S T E M



ACCESS CONTROL MANAGEMENT SOFTWARE

Table Of Contents

TABLE OF CONTENTS	1
KEYSCAN SYSTEM VII	11
INTRODUCTION	12
What is Access Control.....	13
Access Control Features and Components	13
System VII Requirements	14
System VII Registration	15
System VII Client Main Screen	16
1-Software Menus	16
2 Quick Buttons	16
Software Version and License Agreement	17
System VII Function Keys.....	17
F1 - On-line Help	17
F4 - Panel Updates	18
F5 - Refresh.....	18
F8 - Alarm Monitoring Window	18
Esc Key	18
About the System VII Help.....	18
Contents/Index/Search.....	18
Important Information	18
Procedures	18
Related Topic Links.....	19
SETUP THE SYSTEM	20
Setting up the System.....	21
Related Topic.....	21
Site Setup Wizard	21
Procedure	21
Log On	22
Procedures.....	22
Related Topics	22
Site Setup	23
Site Setup.....	24
Print Site Setup	24
Site Information Search.....	24
Procedures.....	24

Site Information Form.....	24
Cardholder Folder Location.....	25
Procedures.....	25
Site Unit Setup Form.....	27
Procedures.....	27
Site Contacts Information Form.....	28
Procedures.....	28
Schedule a Remote Modem Connection.....	29
Procedures.....	29
SMTP Email Settings.....	30
Procedures.....	30
Door Time Zones.....	32
Set Door Time Zones.....	33
Schedules.....	33
Holiday 1, Holiday 2, Holiday 3.....	33
Security Levels.....	37
First Person In.....	37
Procedures.....	37
Related Topics.....	39
Door Time Zone Examples.....	39
Time Zone - Stays within 24 Hour Clock.....	39
Time Zone - Overlaps Midnight - 7 Days.....	39
Time Zone - Overlaps Midnight - 5 Days.....	39
Time Zone - Continues Across Multiple Days.....	39
Door Setup.....	41
Setting Up Doors.....	42
Door Group Names.....	42
Copy Group Descriptions to Other Sites.....	42
Security Levels.....	42
Procedures.....	42
Related Topic.....	43
Set Door and Reader Parameters.....	43
Reader Information Form.....	43
Door Output Form.....	43
Anti-Passback.....	44
Types of Anti-passback.....	44
Door Operation Modes.....	45
Procedures.....	45
Assign Time Zones to Doors.....	48
Procedures.....	49
Related Topics.....	50
First Person In.....	50
Procedures.....	50
Related Topics.....	51
First Person In - Example.....	51
Related Topic.....	51

Set Auxiliary Output Names & Auxiliary Output Status	52
Procedures	53
Set Auxiliary/Supervised Input Names-Output Assignment	53
Procedures	53
Set IOCB1616 Parameters	54
Assign Time Zones to Auxiliary Outputs	54
Procedures	54
Related Topic	54
Assign Time Zones to Auxiliary Inputs	55
Input Type	55
Procedures	55
Assign Time Zones to Supervised Inputs	56
Procedure	56
Assign Time Zones to Readers/Keypads	56
Procedures	57
Set Alarm Response Instructions/Alarm Graphic Locations	58
Procedures	59
Door Group Access Levels	60
Assign Door Group Access Levels	61
Procedures	61
Related Topic	62
Assign Door Group Access Levels - Example	62
Elevator Setup	63
Setting Up Elevators	64
Elevator Group Names	64
Procedures	64
Set Elevator Bank Names	65
Procedures	65
Set Elevator Names and Floor Hold Times	65
Procedures	65
Assign Elevators to Elevator Banks	66
Procedures	66
Set Elevator Floor Names	66
Procedures	67
Set Elevator Banks to Time Zones	67
Elevator Time Zones	67
Elevator Schedules	67
Procedures	68
Set Elevator Time Zones to Automatically Lock/Unlock Floor Buttons	69
Procedures	70
Elevator Group Access Levels	71
Assign Elevator Floors to Group Access Levels	72
Procedures	72
Related Topic	73
Elevator Group Access Levels - Example	73

Setup Holidays.....	74
Assign Dates to Holiday 1, Holiday 2, or Holiday 3.....	75
Procedures.....	75
Related Topic.....	76
Setup Daylight Savings.....	77
Daylight Savings.....	78
Procedures.....	78
Setup Cardholder Records	80
Create Cardholder Records	81
Related Topics	81
Complete Card Information and Access Levels	81
Door Group Access Levels/Elevator Group Access Levels.....	81
Display Access Level Summary	82
Accessibility Feature	82
Previous/Next Buttons.....	82
Procedures.....	82
Temporary Card Options.....	83
Procedures.....	84
Optional (Cardholder) Fields	84
Procedures.....	85
Photo Capture	85
Procedures.....	85
Signature Capture	86
Procedure	86
Create System Users.....	88
About System Users.....	89
Procedure	89
Related Topics	91
System User Account Types	91
System User Account Types & Privileges	91
User Authority Levels	92
Security Levels	92
Example of Single Site with Multiple Users.....	93
Example of System Users - Multiple Sites	94
Email Alarm Notification.....	96
Setup Email for Alarm Notification	97
SMTP Email Setup.....	97
Command Line Option	97
Load Active Map on Alarm Event.....	97
Procedures.....	97
Related Topic.....	99
Setup Database Backup	100
Schedule Automatic Database Backups	101
Default Database Backup Folder	101
Single PC Installation.....	101

Multiple PC Installation.....	101
Email Notification	101
Procedures.....	101
Database Location	102
Setup Communication Service	104
Communication Service Setup.....	105
Preliminary.....	105
Procedures - Local / Workgroup	105
Procedures - Network/Domain	106
Communication Service Verification.....	107
Upload Access Control Units	109
Uploading the Access Control Panels.....	110
Procedures.....	110
OPERATE THE SYSTEM.....	111
Alarms.....	112
Alarm Monitoring	113
Procedures.....	113
Related Topics	113
Alarm Response Instructions	113
Procedures.....	114
Related Topic.....	115
Alarm Listings.....	115
Procedures.....	116
Alarm Warning.....	117
Related Topics	117
Alarm Types	117
Cardholders	119
Add a Cardholder	120
Related Topic.....	120
Add a Block of Cards.....	120
Procedures.....	120
Card Enrollment Feature	121
Procedure	121
Searching for Cardholders	122
Wild Cards	122
Procedures.....	123
Menus	123
Import and Export Cardholder Information	123
Reports	123
Utilities	123
Search for Records	123
General Cardholder Information Fields	123
Additional Cardholder Information Tab.....	124
Optional Cardholder Information Tab.....	124
Not Used Since	124

Sort By Field	124
Find Cards	124
Find All Cards	124
Clear Find	124
New Card	124
Add a Block of Cards	124
Delete Cards	124
Archive Cards	124
Print Listing	125
Print Photo Badge	125
Copy Card to Another Site	125
Edit/Delete Cardholders	126
Procedures	126
Archiving Cardholder Records	127
Procedures	128
Copy Card Records to Other Sites	129
Procedure	129
Related Topic	130
Replace Lost or Stolen Card	130
Procedure	130
Create a Temporary Card	130
Procedures	131
Related Topics	131
Find Cards with "Not Used Since" Feature	132
Procedure	132
Print Cardholder Records	132
Procedures	133
Print Photo Badges	133
Printing Multiple Photo Badges	133
Procedures	133
Export Records in PDF Format	134
Procedure	134
Import/Export Cardholder Information	135
Conventions for Importing CSV Files	135
Procedures	136
Related Topic	137
Import CSV Files - Conventions	137
Mandatory Cardholder Database Fields	138
Non-mandatory Cardholder Database Fields	139
Non-mandatory Additional Cardholder Fields	139
Non-mandatory Optional Cardholder Fields	140
Schedule CSV Imports	140
Procedures	141
Related Topic	142
Reports - Access Levels	142
Related Topic	144

Last Card Transactions	144
To Display Transactions.....	144
Communication Requests.....	145
Processing Communications Request	146
Door Status/Manually Lock/Unlock Doors	147
Door Lock/Unlock Status.....	148
Procedures.....	148
Keyscan Admin User Account	150
Keyscan Admin User Account.....	151
Procedures.....	151
Log On/Passwords	153
Log On to a Site	154
Procedures.....	154
Passwords.....	154
Log On Password.....	154
Password Confirmation	154
Procedures.....	154
Database Options	156
Database Maintenance Options	157
Related Topics	157
Restore the Database	157
Networks	158
Procedures.....	158
Preliminary	158
Steps to Stop the Keyscan System VII Communication Service	158
Steps to Restore the Database	159
Re-Start the Keyscan System VII Communication Service	159
Related Topic.....	160
Purging Transactions	160
Procedure	160
Related Topic.....	162
Compress and Re-index the Database	162
Procedure	162
Site Contacts	163
Find Site Contacts	164
Procedures.....	164
System Users	166
Add System Users.....	167
Find System Users	167
Procedures.....	167
Delete or Archive System Users	169
Procedures.....	169
Transaction Reports	171
Transaction Reports	172

Overview	172
Additional Cardholder Information.....	173
Optional Cardholder Information	174
Procedures.....	175
Related Topics	177
Schedule/Email a Report.....	177
Procedure	177
Keyscan Report Previewer.....	178
Overview	178
Related Topics	178
Utilities	180
System Log.....	181
Procedures.....	181
To Search for System Log Entries	181
To Save System Log Entries.....	182
To Open a CSV file (System Log File)	182
To Clear All System Log Entries	183
Cardholder Optional Fields.....	183
Procedures.....	183
To delete a single caption	184
To delete all captions	184
Photo Shape Setup	184
Procedure	185
Default Panel Outputs & Protocols.....	185
Procedures.....	185
To assign an output for a power failure	185
To assign an output for an invalid code.....	186
To assign an output for keypad duress	186
Set Power Failure Delay	186
Set Manufacturer Codes WSSKP-1 Keypads	187
Default Code	187
Reader Access Level Reports.....	187
Procedures.....	187
Cumulative Hours Reports	189
Example of Cumulative Hours Setup	189
Procedures	190
Door and Input Status	190
Door & Auxiliary Input Status Legend	191
Supervised Input – Shunt Status.....	191
Supervised Input – Input Status	191
Time Zone Status	191
Procedure	191
Manual AI Shunt and SI Control.....	192
Procedures.....	192
Set Individual Inputs – Normal or Disarmed	192
Set All Inputs – Normal or Disarmed	193
IOCB1616 Shunt Control Status	193

Shunt Status	193
Auto Status	193
Input Status	193
IOCB1616 Output Control Status	194
Automatic/Manual	194
IOCB Current Status	194
IOCB Automatic Status	194
Manual Output Control	194
Procedure	194
To Toggle Individual Outputs	194
To Toggle All Outputs	195
Elevator Floor Control Status	195
Procedures	195
Reset Anti-Passback	196
Procedure	196
Related Topic	197
Card In/Out Status	197
Procedures	197
Alarm Notification	199
Displaying Online Transactions	199
Procedures	199
Related Topics	200
Show Photos	200
Procedures	200
Related Topics	200
Display Software Connections	201
Procedures	201
CCTV	202
Setting Up CCTV	203
Setup a CCTV System	204
DVR Pre-configuration	204
System VII CCTV Forms	204
Related CCTV Topics	204
CCTV Type Setup	205
Switcher/Matrix	205
DVR	205
Procedure	205
CCTV Command Setup Form	207
Procedures	207
Show Live Video	207
Procedures	208
Potential DVR Connection Problems	208
Related Topic	209
CCTV Action Setup and Email Notification Form	209
Procedures	209

Operate the CCTV Module	212
Operate the Video Control Panel	213
Video Stream	213
PTZ Camera Control	213
View Control	213
Video Resolution	213
Playback Control	214
Camera Selection Control	214
Find Video from a Report	214
Procedure	214
Related Topic	215
PRESENT3	216
Present3	217
Related Topics	217
Present3 Modes	217
Door Toggle	218
Time Zone Toggle with Cardholder Lockout	218
Time Zone Toggle with Cardholder Lockout and Exit Delay	220
Time Zone Toggle without Cardholder Lockout	222
Not Used	224
Using Present3	225
Setup Present3	225
Procedures	225
I/O MANAGEMENT	230
I/O Management	231
GLOSSARY	232
Glossary of Terms	233
TROUBLESHOOT DATABASE CONNECTION ERROR	235

Keyscan System VII

Keyscan's System VII is the multi-dimensional software application that operates your access control system. It has been designed to give you complete and precise control over which individuals are permitted to enter specific doors or elevators at specific times on specific days. System VII keeps you informed of all site activity and alarm conditions. And, with its self-contained, internal database, System VII lets you keep detailed cardholder records and allows you to produce extensive, management reports and audits.'

If you're unfamiliar with access control and what's involved in setting up and operating the system, System VII includes comprehensive, context-sensitive, on-line help. No matter where you are in the System VII software, pressing the F1 key opens the help for the interface screen that you're currently viewing. It explains the purpose of the screen and the steps to complete it so that you always have assistance when you're not sure how to do something.

For a new installation, we suggest that first you review the topics under Introduction. When you're ready to start inputting data, follow the topics listed in  Set Up the System which takes you through the necessary procedures to create a site and make it operational.

System VII with Multiple Monitoring Capability



Introduction

What is Access Control

Electronic access control is based primarily on three Ws – WHO, WHERE, and WHEN. Bearing this in mind, an electronic access control system regulates who may access specific doors or other types of entry points, such as parking gates, or elevators at specified times.

Authorized individuals are recognized by a "credential", which could be a card, token, fingerprint, or personal identification number. Acting as a sort of passport, each credential has a unique marker for individual identity. To gain access at a controlled door or entry point, the credential is presented at a reader. Like an invisible sentry, the access control system grants access or denies access based on programmed settings for the credential. Called a "transaction", each instance of attempted access, whether access is granted or denied, is recorded to a dedicated access control database. This database provides a source of records for auditing site activity and security information.

Access Control Features and Components

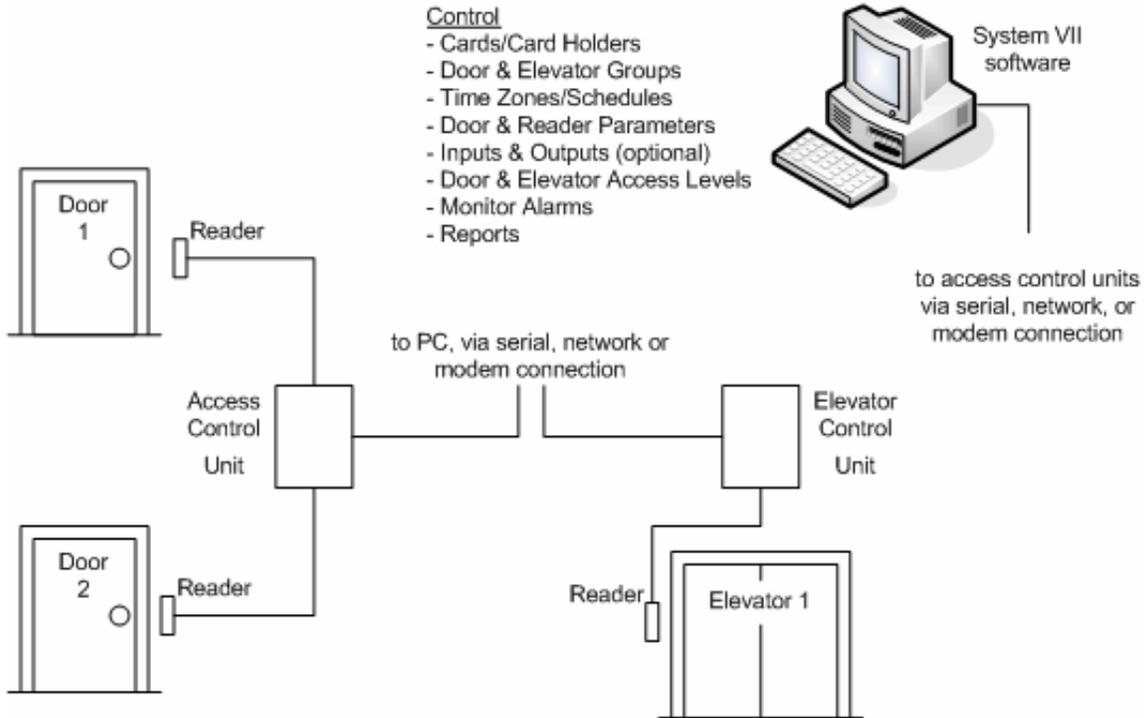
An access control system provides complete control and management of a building or site.

- controls door, elevator, parking lot, or garage access
- operates 24 hours a day, 7 days a week, 12 months of the year
- specifies access conditions for each individual at every door
- monitors access points for alarms
- integrates with other building systems
- connects to modems or networks for multiple building control
- reports site activity for complete security management auditing

The access control system consists of the following components that work together giving you complete security and access control management:

- System VII software
- personal computer
- proximity cards or other forms of credentials
- card readers and/or keypads
- door locking hardware
- access control units (ACU)
- alarm monitoring

System VII System Overview



System VII Requirements

The following list outlines minimum PC requirements to operate the System VII software:

- Recommended Central Processing Unit (CPU): Pentium D or later
- Recommended minimum RAM: 1 gigabyte or greater
- Hard Disk: Recommended 20 gigabytes of available space
- USB Port for Photo Badging or Signature Capture
- COM Port - 1 required if using direct serial connection to access control units; 2 required if using CCTV control as well
- CD-ROM or DVD drive
- Mouse or compatible pointing device
- Removable Media Storage Device such as CD or DVD Writer for database backup
- Network Interface Card (NIC) with TCP/IP protocol, a valid, active IP address (PC with System VII database - SQL Server 2005 Express - must be assigned a static IP address) and file & printer sharing for Microsoft networks
- Graphic Card supporting 1024 x 768 or higher screen resolution
- Operating System - Windows 2000 with Service Pack 4 or later, XP

Professional with Service Pack 2 or later, Vista Business, or Windows 2003 Server

- Microsoft Internet Explorer 6.0 SP1 or later
- Microsoft .NET 2.0 Framework

System VII Registration

You must register your System VII software application to be an authorized user. Only registered users are eligible for Keyscan technical support. After completing the on-screen registration form, call the one of the numbers listed below. When you call, a Keyscan representative will request the Machine Key Serial Number posted at the top of the System VII Registration form, the registration software serial numbers listed on the card that accompanied the Installation CD, and your company and dealer information. You will be given an Unlock Serial Number to complete your software registration.

If you choose not to register your product now, Keyscan offers a trial period of 30 days to review the software application. During the 30 days you are free to try the product, however, you are not eligible for any technical support. When the 30 days have ended, the application will no longer function.

Registration Information

Telephone Numbers	Hours	Days
Canada/USA -Toll Free 1-888-539-7226 Outside Canada/USA 905-430-7226	9:00 A.M. – 5:00 P.M. Eastern Time	Monday – Friday

Complete the Company Information and the Dealer Information on the Software Registration form. The top 4 captions under the Company Information and the Dealer Information are required fields.

Your software package includes a card with a registration serial number for each software module that you purchased which could be any of the following applications:

- System VII Software (2 Concurrent Client Licenses)
- System VII Additional Client License - VAC (Optional)
- System VII CCTV Integration - VTVM (Optional)
- System VII Photo Badging - VIDM (Optional)
- System VII SDK (Optional)
- System VII Visitor Module -VVM (Optional)

Enter the serial numbers in the applicable Serial Number text boxes on the Keyscan System VII Registration form.

Have your Machine Key Serial Number, the registration software serial numbers, and your company and dealer information available and call one of the Keyscan numbers listed above. A Keyscan representative will provide you with a corresponding Unlock Serial Number for each purchased module to complete your registration.

After you have entered the Unlock Serial Number, click on the Register Software button. You are now an authorized user.

If you wish to register later, click on the Register Software Later button to retain your information. Each time you log on, the Registration form will open to remind you about registering.

System VII Client Main Screen

1-Software Menus

Use the pull down menus to access all the forms in the Client software application to create, edit, and delete site information.



The red text in the upper left corner on the main screen appears until System VII has been registered.

2 Quick Buttons

Quick buttons are convenient shortcuts to commonly used functions. To access a Quick Button, click on the caption directly below the icon. All Quick Buttons displayed on the main screen can also be accessed from the Quick Buttons menu.

- Cardholder Database - Provides quick access to perform all tasks associated with cardholders.
- Time Zones/Schedules - Provides quick access to add, edit, or delete time zones, schedules or holiday schedules for doors or elevator banks.
- Door Lock Unlock Status - Provides direct access to manually lock or unlock doors.
- Group Access Levels - Provides quick access to edit either door or elevator group access levels. Each door or elevator group is assigned an access level – no access, 24 hour access, or an access period based on a time zone.
- Display On-line Transactions - Provides direct access to view and sort site transactions.
- Transaction Reports - Provides direct access to run user-specified transaction reports on site activity.
- Alarm Listings - Provides direct access to view new or pending alarms or find alarms by a date range.

- Update Changes - Accesses the Panel Updates form to upload data to the access control units.

System VII Client Main Screen



Software Version and License Agreement

The System VII Client version and current license agreement are specified on the About form, which is accessed from the Help menu. System Information can be displayed by clicking on the System Info... button. To close the window, click on the OK button.

If you call for technical support, you will be requested to give the System VII software version number.

System VII Function Keys

When the System VII software is open, press the following function keys along the top of the keyboard to access information or open windows as listed:

F1 - On-line Help

Press the F1 key to open the System VII on-line help. The help is context sensitive and opens on the topic relevant to the interface screen you are viewing.

F4 - Panel Updates

When a panel is selected in the Panel Updates form, pressing F4 opens a dialog box listing the panel serial number and the model type.

F5 - Refresh

When the main screen, alarm, or transaction windows are open, pressing F5 updates the screen.

F8 - Alarm Monitoring Window

When the System VII Client is the active window, pressing F8 restores the Alarm Monitoring window if it was closed.

Esc Key

During a panel upload, pressing the Esc key aborts the upload. The upload continues until all data from the current field has been sent to the panel before it aborts.

About the System VII Help

The System VII on-line help can be accessed in two ways:

- from the Help menu on the main screen
- pressing the F1 key from anywhere in the System VII software

The help has two window panes:

- Left Pane - Contents/Index/Search for navigating the help
- Right Pane - Topic information, procedures, and related topic links

Contents/Index/Search

-  Double click on a closed book or click the + to the left to open a book and view related topics.
-  Click on a topic to view the contents.
- Click on the Index tab and type a word or phrase in the text box and select the topic from the list.

Important Information

-  Indicates important information

Procedures

- A green arrow  indicates instructions, diagrams, or explanations. Click on the italicised green text to the right of the green arrow to open. To close, click on the italicised green text again.

Related Topic Links

- A blue arrow indicates [▶](#) a link to related topics. Click on the italicized & underlined blue text to go to a related topic.

Setup the System

Setting up the System

After installing the System VII software, the next task is to set up your site. This involves entering data on the forms that are accessed from the menus or the quick buttons on the Client's main screen. The configuration of your site will determine which steps and forms you complete. As an example, if your site does not have elevators, by-pass the section on completing the forms within the Elevator Controllers menu. In some cases, you may require the assistance of your dealer/installer to set access control unit and input and output data.

The System VII software includes a Setup Wizard which walks you through the basic steps to get your system up and running.



Until the PC you are using to setup the System VII software has a communication link with the access control panels, you will have a Communication Status FAILED message on the main screen. This is normal as the software has been designed to advise you whenever it can't "talk" to the access control units. You will not be able to open some of the Door Maintenance forms nor Upload the Panels however until the access control units are operating and communicating with the PC.

Related Topic

▶ *Site Setup Wizard*

Site Setup Wizard

The Site Setup Wizard is an on-line aid that guides you through the steps to setup your site. When you start the Site Setup Wizard, it automatically opens the forms for each step in successive order. Just enter the required information and save your data as you progress through each form.



The Site Setup Wizard does not allow you to deviate from the order of the forms as they are presented. Do not open other forms from within the form you are completing, otherwise the Site Setup Wizard closes.

Additionally, if you use the Site Setup Wizard, be sure to review the Setup Communications Service instructions in order that the software and the panels can "talk" to each other.

Procedure

To Open the Site Setup Wizard, select the System Settings menu > Site Wizard > Start Wizard button.

Log On

When you open the Client application or switch to another site, you are prompted to specify the following information in the Log On dialog box.:

- Specify the name of the site you are logging on (if other than the site listed in the Site Name box)
- Select a language (N/A)
- Enter your user name
- Enter your password

You will note that any time a system user account has been assigned with the Master Login designation, it is listed in the Site Name field. For more information on Master Login, see Setup System Users under Setting Up the System in the Contents window.

Procedures

►Steps To Log On

1. If you are logging on for the first time or you have not created a specific user account, type the following in the corresponding text boxes :
 - User Name: Keyscan
 - Password: KEYSKAN (Must be entered in upper case.)
2. Click on the OK button

Each subsequent time you open the Client application, you must log on by specifying the site name, and enter your User Name and Password, which will be based on what was entered in your user account in the System User Information form. Until you create user accounts for system administrators, the above applies to logging on to the Client and the optional Photo Badge Template Editor.

Related Topics

►*Log On to Another Site*

►*Passwords*

Site Setup

Site Setup

The Site Setup forms identify the site, specify the types of access control units installed, set communication criteria, and list the names of persons to be notified in an emergency. Site Setup consists of the following forms:

- Site Information
- Site Unit Setup
- Contact Information
- Schedule Remote Modem Connection (optional if using a dial-up modem)
- SMTP Email Settings (required if using email alarm notification)



Before beginning to create your new site, you need to know the Access Control Unit serial numbers, unit types, and unit passwords. The ACU serial number and unit type are listed on the packing slip or they can be found on the main control board inside the ACU panel. The default password for all Keyscan ACUs is KEYSKAN. This information has to be entered in the Site Unit Setup form.

Print Site Setup

As a safeguard to protect your system data, after you have completed the site setup forms, it is strongly recommended that you print a hard copy of the site information by selecting the Print Site Setup button on the Site Information Search form and storing the site records in a safe place. You should always print a new copy whenever site information is added or changed.

Site Information Search

When you access Site Setup from the System Settings menu, the first form to open is the Site Information Search form. Whether you wish to add a new site or amend information on an existing site, the Site Information Search form acts as the hub to perform any site setup tasks.

Procedures

To create a new site, select the Add Site button to open the Site Setup forms..

To locate, verify, or update information about an existing site, click on the Find Sites button to list all sites or specify specific criteria in the field search text boxes at the top to narrow your search, then click on the Find Sites button.

To open an existing site, double click on the site name in the table.

Site Information Form

The purpose of the Site Information form is to identify the location of the site. This includes a site ID descriptor, the site name, address and telephone number. You must also specify whether you are creating a host or remote site and in the case of a remote site, specify the data collection format that is employed to transfer data from the access control units back to the host site database.

Cardholder Folder Location

The Site Information form has a Cardholder Folder Location field. If you have the optional Keyscan System VII Photo Badging module, you can use this field to specify an alternate folder location for your cardholder images.

- If you leave this field blank, cardholder images are saved in the Keyscan database.
- If you specify a Cardholder Photo location, cardholder images are saved in the Keyscan database as well as the specified folder location.

Procedures

►Steps to Complete the Site Information Form

1. From the main screen, select System Settings > Site Setup > Site Information Search. Click on the Add New button.
 - If you previously started to setup a site, saved it, and you are now returning to complete setting up the site, do not click on the Add New button. Click on the Find Sites button. Your site will be listed in the body of the Site Information Search form. Double click on the site name in the body of the Site Information Search form to open the site.
2. Click in the Site ID text box and enter an ID name. The maximum is 8 characters. The purpose of a Site ID is to identify the location so that other individuals operating or monitoring the system can determine the source of where an alarm occurs. This is especially important where multiple sites are going to exist.
3. Click in the Site Name text box and enter the name of the site.
4. Complete the remaining site information from Site Location to Fax Number, whichever fields are applicable.
5. If applicable, click on the down arrow to the right of System Logging Level and select a level. The default is Full Logging Level which lists all the user's activity in the System Log. To retain less details in the System Log, select a level between Level 1 and Level 4.
 - Level 4 retains the least System Log details
6. If applicable, enter any special comments in the Site Comments text box.
7. Specify a Card Holder Folder Location if you have the optional System VII Photo Badging module and you want your cardholder images to reside in an

- alternative folder. All cardholder photos are saved in the Keyscan System VII database as well.
8. If the site has any modem connections and you do not want the Host site to automatically dial out to the remote site/panels and perform an upload whenever cardholder, time zone, holidays, daylight savings, or access level data has been added or revised, select Disable Auto Updates by clicking in the box to the left.
 9. To assign the site you are creating as the default site, select the Default Site check box to activate the field. When you log on, the Default Site is automatically listed in the Site ID field on the Client Log On dialog box.
 10. If there are no modem connections go to step 15. If you have modem connections but are creating a host site, leave the default setting at No Collection and go to step 13. If you are creating a remote site/panel with a modem connection go to step 10.
 11. Specify one of the following Activity Collection options:
 - Capacity Only – the host site is contacted when the remote site’s ACU memory reaches the specified percentage of its total capacity. Specify the percentage in the % of Capacity field.
 - Time/Capacity – the host site is contacted when the remote site’s ACU memory reaches the specified % of its total capacity or at the specified time whichever event is first. Specify the percentage in the % of Capacity field and the time in the Time HH:MM fields.
 - If there is a time period when you do not want the remote site/panel modem connecting with the host site, select a time zone from the drop down list by clicking on the arrow to the right of Time Zone – Disable Dialing Period. The time zone selection is based on the remote panel's type – door or elevator. You may wish to create a specific door or elevator time zone for this function. For a new site, you will have to first create a time zone and return later to assign a disable dialing period.
 12. To set the number of dial attempts in case the modem fails to make a connection on the first call, click on the down arrow to the right of Dial Attempts and select a number from the list. The range is 1 to 99.
 13. To set the Delay Attempt Time, the period in minutes between dial out attempts, click on the down arrow to the right and select a number from the list. The range is 1 minute to 99 minutes.
 14. In the Host Telephone Number enter the telephone number that the remote site/panel calls.
 15. In the Access Control Unit Modem Initialization String, right click to open a drop down list and select the correct initialization string. If you are unsure of which string to select, consult your modem manufacturer’s literature.

16. Complete the other forms by clicking on the respective buttons, Site Unit Setup (required) and Site Contacts (optional), SMTP Email Setup (optional) and Schedule Remote Connections (optional). When you have completed the other forms, be sure to click on the Save & Exit button.

Site Unit Setup Form

The Site Unit Setup form is used to specify the types of access control units installed and set communication criteria. You may require the manufacturer's literature that accompanied your modem or network card for communication settings. The baud rate specified on the Site Unit Setup form for a serial connection must match the baud rate jumper setting on the access control unit circuit board. You may have to consult with your dealer/installer.



Before beginning to complete the Site Unit Setup form, you need to know the access control unit serial number, unit type, and unit password. The ACU serial number and unit type are listed on the packing slip or they can be found on the main control board inside the ACU panel. The default password for all Keyscan ACUs is KEYSKAN.

Procedures

► Steps to Complete the Site Unit Setup Form

1. From the Site Information form, select the Panel Setup button.
2. Enter the corresponding information into the following five fields:
 - Unit ID – Enter a unique Unit ID that distinguishes the ACU/ECU from other panels at the site. The maximum is 6 alpha-numeric characters.
 - Serial # - Enter the access control unit serial number which starts with an alpha character, followed by 4 numeric characters. The serial # is on the packing slip and the ACU circuit board.
 - Unit Password – For a remote site setup, it is recommended to change the password from KEYSKAN; for a host site setup, it is recommended to retain the default password KEYSKAN.
 - Unit Type – Use the down arrow to select the corresponding unit type.
 - Status - Select Active from the drop down list.
3. Click the down arrow to the right side of Communication Setup and select the appropriate mode - Serial, Network or Dial Up. Enter the necessary settings based on your selection:
 - For a Serial Connection – Specify the Baud Rate and Communication Port.
 - For a Network – Specify the IP Address and Subnet Mask.

- For a Dial Up Connection – Specify the Auto Dial Telephone Number, this is the phone number that the host site modem dials to connect with the remote site/panel modem – Baud Rate – Communication Port, the port number assigned to the modem at the host PC – Initializing String, the initializing string of the host modem. Refer to the manufacturer's literature.
4. If the remote site/panel is connecting with a host number that is different than the number specified on the Site Information form, enter the number in the Host Telephone Number. Generally this applies to panel to panel modem communication.
 5. In the Unit Location Description, enter a brief caption to indicate the ACU's physical location.
 6. Click the down arrow on the right side of the Geographical Time Zone Setting field and select the time zone from the drop down list where the panel/site is located.
 7. In the Communications Server Processing field, enter the name of the PC. This is the PC that has the Communications Service tagged to the ACU you are currently entering. The PC name is listed opposite the Full Computer Name field in Window's System Properties \ Computer Name dialog box.
 8. Leave Communications Server Processing set on Main Communication unless you have installed multiple Communication Managers.
 9. Select the Add Unit button.
 10. If you are entering more than one access control unit, repeat steps 2 - 9, or if you have finished adding ACUs, select the Save & Exit button to return to the Site Information form.

Site Contacts Information Form

The names of contacts entered in the Site Contacts form are made available on the Set Alarm Response Instructions – Alarm Graphic Locations form, which outlines who to contact in the event of an emergency alarm.

Procedures

►Steps to Complete the Site Contacts Information

1. From the Site Information form, select the Site Contacts button.
2. From the Search Site Contacts form, click on the Add New button.
3. Leave the Site Contact ID blank. This is a system assigned entry.
4. Click in the First Name text box and enter the person's first name.

5. Complete the remaining fields from Last Name to Email Address, whichever information is applicable.
 - In the Telephone Number field, enter the number without using hyphens or brackets.
6. Select the Save & Exit button.
7. To confirm your contact entry, click on the Find Contacts button. The contact name is listed in the table.
8. To add another contact, click on the Add New button and complete the Site Contact Information form, or select the Exit button to return to the Site Information form.
9. To complete the SMTP Email Settings or Schedule a Remote Connection select the appropriate button or select the Save & Exit button > Exit button to return to the main screen.

Schedule a Remote Modem Connection

To access the Schedule Remote Connections form, you must be in the Site Information form and your site must have at least one ACU with modem communication specified in the Communication Setup field on the Site Unit Setup form. Otherwise, the Schedule Remote Connections button is dimmed and unavailable. Scheduling a remote connection instructs the host PC modem to establish contact with a remote access control unit modem.



In the Schedule Remote Connections form, the Start Time and End Time represent a 1 day window that the host modem will attempt to make contact with the remote panel modem. As an example, if the Start Time is set to 9:00 and the End Time is set to 17:00, the host modem will attempt to dial out to the remote panel modem between 9:00 A.M. and 5:00 P.M. This could be every day, every other day, every third day etc., depending on the day interval specified in the Every field. If the host PC is not running during the schedule, it will not dial out on that day. However, it will re-schedule the remote connection based on the next day interval.

Procedures

►Steps to Schedule Remote Connections

1. From the Site Information form, select the Schedule Remote Connections button.
2. Click on the down arrow to the right of Unit ID, and select the access control unit from the drop down list.
3. Leave the Type field set on 1-PC to ACU.

4. Click on the down arrow to the right of Connection Attempts. Select the maximum number of times the calling modem will attempt dialing out in the event it is unsuccessful establishing a connection the on the first try.
5. The Start Time is the beginning time that the host PC modem will attempt to contact the remote access control unit modem. By default, the current date and time are displayed – month/day/year/hour/minute/second. To change the Start Time, select the hour and click on the up or down arrows at the right to increase or decrease the hour. Repeat for the minute and second settings. The date does not have to be changed.
6. The End Time is the concluding time that the PC modem will cease attempting to make contact with the remote panel modem on that day. By default, the current date and time are displayed. To change the End Time, select the hour and click on the up or down arrows at the right to increase or decrease the hour. Repeat for the minute and second settings. The date does not have to be changed unless the End Time crosses over midnight.
7. Click on the down arrow to the right of Every, and select a day interval from the drop down list.
8. Click on the down arrow to the right of Remote Connection Hang Up Time. This is the amount of time the modems communicate before the host modem terminates the connection. Select a time from the drop down list. The recommended time is 5 minutes for each ACU that is in the modem communication loop. As an example, if there were 4 ACUs, set the time to 20 minutes.
9. If not pre-selected, click in the radio button to the left of Active to enable this field and make the schedule active.
10. Click on the Add Unit button.
11. Click on the Save & Exit button to return to the Site Information form.

SMTP Email Settings

If you are going to use Vantage's email functions, such as sending alarm messages, use the SMTP Email Settings to by-pass routing email through MS Outlook. Newer versions of Windows can prevent routing of alarm notification email messages because of network permissions.

In order to use the SMTP Email Settings, email must be routed through a mail server or exchange server with the SMTP mail function enabled. This task must be performed by the IT department, since settings are based on established mail server protocols.

Procedures

►Steps to Setup SMTP Email

1. From the Client main screen, select the System Settings menu > Site Setup.
2. Double click on the appropriate site name in the Site Search Information form.
3. From the Site Information form, select the SMTP Email Settings button.
4. From the SMTP Email Setup form, enter the address in the SMTP Email Server text box.
5. In the Reply To Email Address text box, enter the sender's address that appears in the From line of the email.
6. In the SMTP User Logon text box, enter the authorized log on name.
7. In the SMTP User Password text box, enter the password.
8. In the Authentication Type, select the appropriate authentication type specified by the Internet Service Provider.
9. Enter the port number in the SMTP Port text box.
10. In the SMTP Timeout (Milliseconds), enter a value (1000 = 1 second) that exceeds the normal amount of time to access the server. If the time to access the server is less than that specified in the timeout text box, the System VII Client will abort the request to send the email alarm.
11. Select the Save & Exit.

Door Time Zones

Set Door Time Zones

The Door Time Zones form allows you to set time zones for doors controlled by access control units. When you create door time zones it is important to think in terms of the Door Groups and the times that those groups will access the various doors in the building. We suggest you pre-plan before you start entering time zones as well as read and understand the conventions and format of time zones.

- Time zones/schedules are based on a 24-hour clock
- Maximum of 254 named time zones
- Combined total of time zones and schedules is 512
- Maximum range of a time zone or schedule is 00:01 to 23:59
- Inputs and outputs are assigned to door time zones

The default setting of 00:00 in the Keyscan software represents No Time. It does not represent midnight. If either the start time or the end time is assigned 00:00 the following conditions will result:

- If the start time is set to 00:00 – The time zone does not start
- If the end time is set to 00:00 – The time zone does not end

Schedules

You may have multiple schedules that are within a time zone. Unlike time zones, however, schedules are not specifically named and reside within the time zone. A schedule could be used when you have shifts. As an example, the first shift works from 7:00 to 15:00 and the second shift works from 15:30 to 23:30, Monday through Friday. The hours 7:00 to 15:00 could be saved as Time Zone # 1, and the second shift 15:30 to 23:30 could be saved as a schedule within Time Zone # 1.

Holiday 1, Holiday 2, Holiday 3

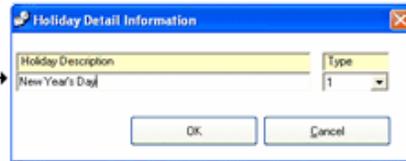
You will note on the Door Time Zones form three boxes - Holiday 1, Holiday 2, Holiday 3. These 3 holiday fields are designed to allow you create special hours for statutory holidays, plant shutdowns, or any other type of occasion where you need an alternative time period from the hours specified in the time zone/schedule. The times specified in Holiday 1, Holiday 2, Holiday 3 and when assigned a calendar date in the Holidays form act as an override to the time zone or schedule. When you are creating time zones you should also think of the appropriate time periods for Holiday 1, Holiday 2, and Holiday 3 relative to statutory holidays and or any other days that require a 1day substitution from normal hours.

We have created 3 examples with the following holiday times to show how it affects door groups, doors with auto unlock, and any inputs/outputs associated with the time zone:

- Holiday 1- Time 00:00 to 00:01



January 1 - New Year's Day Assigned Type 1 (Holiday 1) in the Holidays Form

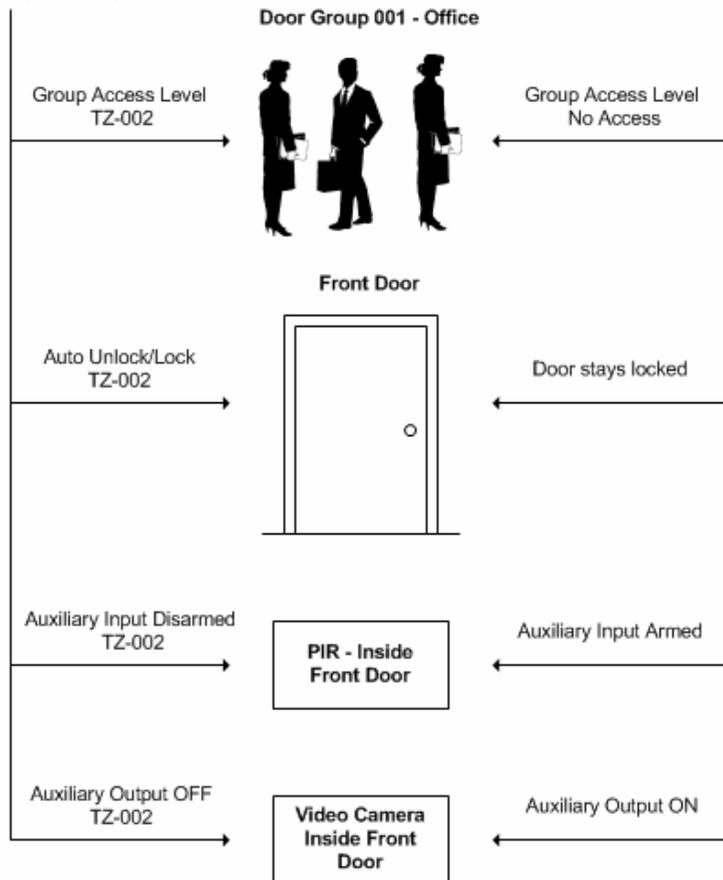


Holiday 1
00:00 to 00:01
(time zone not enabled)

On New Year's Day
Holiday 1 (Type 1)
overrides TZ-002

Note
When Holiday 1, 2, or 3
are assigned a calendar
date in the holiday form
they override the Time
Zone or Schedule

TZ-002 Office
Monday - Friday
8:30 to 17:00 (5:15 P.M.)



- Holiday 2 - Time 08:30 to 13:00 (1:00 P.M.)



July 3 - 1/2 Day Shutdown Assigned Type 2 (Holiday 2) in the Holidays Form

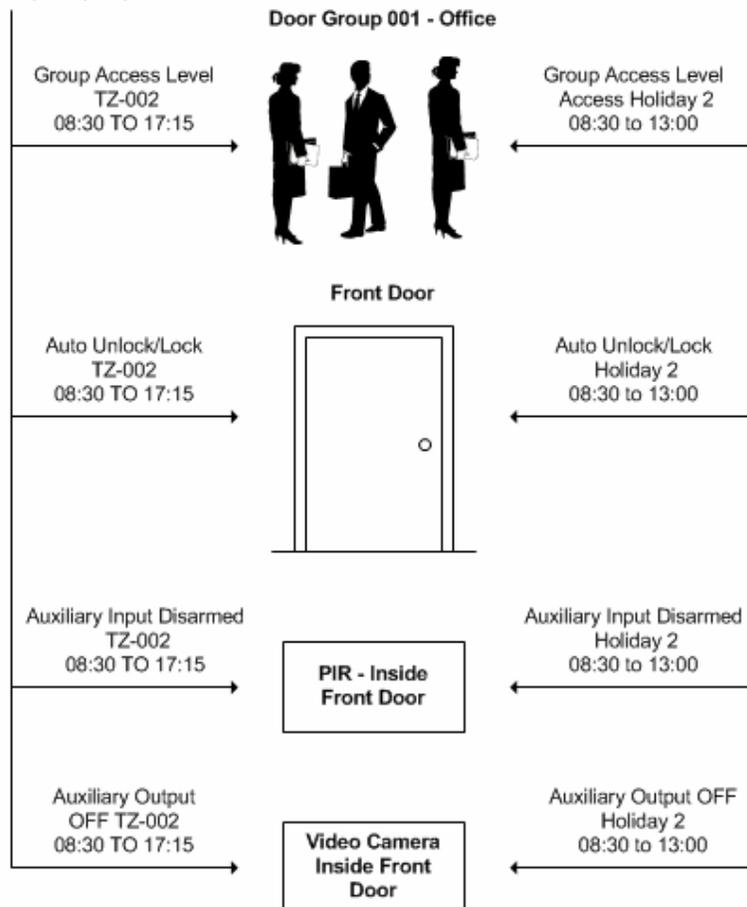


On July 3 - 1/2 Day Shutdown Holiday 2 (Type 2) overrides TZ-002

Holiday 2
08:30 to 13:00 (1:00 P.M.)

Note
When Holiday 1, 2, or 3 are assigned a calendar date in the holiday form they override the Time Zone or Schedule

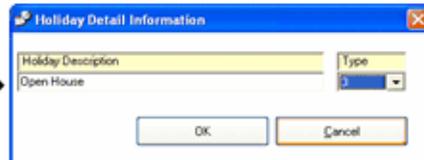
TZ-002 Office
Monday - Friday
08:30 to 17:15 (5:15 p.m.)



- Holiday 3 - Time 07:00 to 23:00 (11:00 P.M.)



April 10 - Open House Assigned Type 3 (Holiday 3) in the Holidays Form

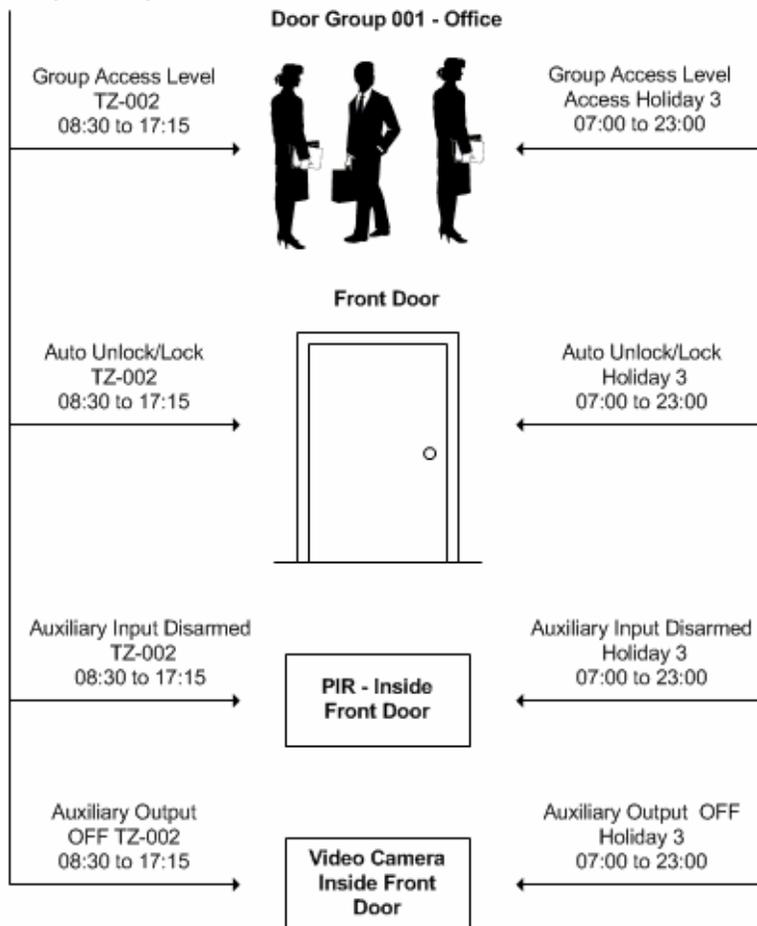


On April 10 - Holiday 3 (Type 3) overrides TZ-002

Holiday 3
07:00 to 23:00 (11:00 P.M.)

Note
When Holiday 1, 2, or 3 are assigned a calendar date in the holiday form they override the Time Zone or Schedule

TZ-002 Office
Monday - Friday
08:30 to 17:15 (5:15 P.M.)



We strongly suggest you create only 3 holiday times and apply those same 3 holiday times across all time zones for easier system management. Holiday 1, Holiday 2 or Holiday 3 times are not enacted unless assigned to a calendar date in

the Holidays form.

Security Levels

If you are enforcing security levels for system users, you can enforce those levels on the Door Time Zones form, such that a system user with a lower level cannot alter time zones set by a system user with a higher security level. Setting security levels is not recommended unless you are an advanced user and require a high level of system operator security. Security levels are set up in the System User Information form. Select the link below for more information.

First Person In

For information about First Person In, select the link below.



Setting door time zones does not regulate elevators. Elevator time zones are set in the Assign Elevator Banks to Time Zones form found in the Elevator Controllers menu.

Auxiliary inputs and supervised inputs/outputs, if assigned to time zones, use time zones created in the Door Time Zones form.

Procedures

►Steps to Add a Door Time Zone

1. From the main screen, select the Quick Buttons menu > Time Zone / Schedules > Door Time Zones.
2. Click on the Add New Time Zone button. The program assigns a Time Zone #.
3. Enter a descriptive title in the Time Zone Description text box to identify the time zone.
4. In the Mon time boxes, the upper box is the start time and the lower box is the end time, select the hour in the upper box and click the up or down arrow at the right to set the start hour.
5. Select the minutes and click the up or down arrow to set the start minutes. You should still be in the upper box under Mon.
6. Select the hour in the lower box under Mon and click the up or down arrow at the right to set the end hour.
7. Select the minutes and click the up or down arrow to set the end minutes.
8. Repeat steps 4 to 7 for each day that falls within the time zone or, if applicable, use one of the Copy buttons on the left of the Door Time Zones form to set the times for the remaining days if the times are the same as

Monday.

9. If you are setting holiday hours, continue to the next step, if not go to step 15.
10. Below Holiday 1, in the upper box, set the start hour. Use the arrows if other than 00:.
11. Set the start minutes. Use the arrows if other than 00.
12. In the lower box under Holiday 1, set the end hour, if other than 00.
13. Set the end minutes. Use the arrows.
14. Repeat steps 10 to 13 if setting times for Holiday 2 and or Holiday 3.
15. If you are enforcing security levels for system users, click on the down arrow to the right and select a security level. Setting security levels is not recommended unless you are an advanced user and require a high level of system operator security.
16. Click on the Save Schedule button.
17. To add another time zone, click on the Add New Time Zone button and repeat steps 2 to 9. To return to the main screen, click on the Exit button.

► *Steps to Add a New Schedule*

1. Click on the down arrow of the Time Zone # and select the time zone from the drop down list.
2. Click on the Add New Schedule button.
3. From the Warning box "Adding multiple schedules to the current time zone...", select Yes.
4. In the Mon time boxes, the upper box is the start time and the lower box is the end time, select the hour in the upper box and click the up or down arrow at the right to set the start hour.
5. Select the minutes and click the up or down arrow to set the start minutes. You should still be in the upper box under Mon.
6. Select the hour in the lower box Under Mon and click the up or down arrow at the right to set the end hour.
7. Select the minutes and click the up or down arrow to set the end minutes.
8. Repeat steps 4 to 7 for each day that falls within the time zone or, if applicable, use one of the Copy buttons on the left of the Door Time Zones form.
9. Click on the Save Schedule button.

10. To add another schedule, click on the Add New Schedule button and repeat steps 2 to 9. To return to the main screen, click on the Exit button.

Related Topics

▶ *Example Time Zones*

▶ *Security Levels*

▶ *First Person In*

Door Time Zone Examples

The tables below illustrate examples of time zones that fall within a twenty-four hour clock, overlap midnight, and run continuously over 5 days.

Time Zone - Stays within 24 Hour Clock

Example - Monday to Friday 9:00 A.M. to 5:00 P.M.							
	Mon	Tue	Wed	Thur	Fri	Sat	Sun
Start	09:00	09:00	09:00	09:00	09:00	00:00	00:00
End	17:00	17:00	17:00	17:00	17:00	00:00	00:00

Time Zone - Overlaps Midnight - 7 Days

Example - Monday to Sunday 5:00 P.M. to 2:00 A.M.							
	Mon	Tue	Wed	Thur	Fri	Sat	Sun
Start	17:00						
End	02:00						

Time Zone - Overlaps Midnight - 5 Days

Example - Monday to Friday 5:00 P.M. to 2:00 A.M. (Time Zone concludes Saturday A.M.)							
	Mon	Tue	Wed	Thur	Fri	Sat	Sun
Start	17:00	17:00	17:00	17:00	17:00	00:00	00:00
End	02:00	02:00	02:00	02:00	02:00	02:00	00:00

Time Zone - Continues Across Multiple Days

Example - Monday to Friday Continuous - TZ concludes at Friday 7:00 P.M. - Resumes Monday 7:00 A.M.							
	Mon	Tue	Wed	Thur	Fri	Sat	Sun
Start	07:00	00:01	00:01	00:01	00:01	00:00	00:00
End	00:00	00:00	00:00	00:00	19:00	00:00	00:00

Door Setup

Setting Up Doors

Setting up doors involves naming the readers/doors, establishing door groups, setting inputs and outputs, assigning time zones to doors, and assigning door group access levels. The topics listed in the Door Setup cover all the forms that pertain to setting up door information.

The forms that pertain to supervised and auxiliary inputs and outputs may not require completion depending on your site configuration. Your service vendor/installer should be able to assist you in determining which of these forms require completion.

Door Group Names

Creating Door Group Names allows you to place cardholders into specific groups based on their security and access levels. When creating door group names, they should correspond to descriptions that are generally applied to groups within your organization.

Door groups are listed under the Group Description field. Unassigned or open door groups appear as 001-Group # 001 to 511-Group # 511.



When creating door group names, the Client software makes door groups #001 to #016 active by default. If you create door group names from door group #017 to #511, ensure that you enable the Group Active field otherwise those door groups can't be assigned access levels in the Door Group Access Levels form.

Copy Group Descriptions to Other Sites

On the Search Door Groups form is a Copy Group Description to Other Sites(s) button. If you have more than 1 site, this function copies the group descriptions to other selected sites which not only saves duplication of effort, but maintains consistent door group descriptions at all sites. This can be especially important where cardholders have access to multiple sites. Keeping consistent door group descriptions, makes it easier to assign consistent cardholder access levels across multiple sites.

Security Levels

If you are enforcing security levels for system users, you can enforce those levels on the Door Group Information form, such that a system user with a lower level cannot alter door group names set by a system user with a higher security level. Setting security levels is not recommended unless you are an advanced user and require a high level of system operator security. Security levels are set up in the System User Information form. Select the link below for more information.

Procedures

► *Steps to Create Door Group Names*

1. From the main screen, select Door Maintenance > Modify Door Group Names
2. Double click on the first unassigned door group.
3. From the Group Information form, type the name of the door group in the Group Description text box.
4. Do one of the following:
 - For door groups #001 to #016, leave the Group Active field enabled.
 - For door groups #017 to #511, click in the Group Active box. The box has a check mark when this function is enabled.
5. If you are enforcing security levels for system users, click on the down arrow to the right and select a security level. Setting security levels is not recommended unless you are an advanced user and require a high level of system operator security.
6. Select the Save & Exit button.
7. To add another door group name, repeat steps 2 to 6, or to return to the main screen, select the Exit button.

Related Topic

► *Security Levels*

Set Door and Reader Parameters

Readers control doors within the Keyscan system. There are two forms to complete in order to set up the readers at each door:

- Reader Information form
- Door Output # form

Reader Information Form

The Reader Information form is used to name the doors that each reader controls. These are referred to as reader port locations. It is best to use clear and descriptive names such as Main Front Door, Employee Door, or Shipping Door etc. The Reader Information form is also used to specify the direction of access IN or OUT and, if applicable, to invoke the Anti-Passback option. Refer to Anti-passback below for more information.

Door Output Form

The Door Output # form is used to set the Door Relay Unlock Time, the Door Held Open Time, the Door Operation Mode, and door outputs.

Anti-Passback

Anti-Passback prevents one individual from passing his or her card back to another individual for later use. When anti-passback is employed, after a card enters a controlled enter/exit environment, the card must exit before the system permits the card to enter again. To have a controlled enter/exit environment with anti passback requires readers on both sides of the door or in some configuration that monitors and controls in/out activity.



If you are not using the anti-passback function, proceed to Steps to Create Reader Port Names without anti-passback.

Types of Anti-passback

Only one access control unit and its designated in/out readers can be used to control an enter/exit environment. Anti-passback modes for a single ACU.

- Hard Anti-passback Mode – With hard mode, a cardholder presents a credential at a designated IN reader. After access is granted at the IN reader, the cardholder must present the credential at the OUT reader. Presenting a credential consecutively at IN or OUT readers results in an access denied and generates an Access Denied with Anti-passback Violation in the Online Transactions.
- Hard Anti-passback (Soft Anti-passback in Communications Failure) Mode – not applicable for a Single ACU configuration.
- Soft Anti-passback Mode – With soft mode, a cardholder presents a credential at a designated IN reader. After access is granted at the IN reader, the cardholder must present the credential at the OUT reader. Presenting a credential consecutively at IN or OUT readers, however, results in an access granted but generates an Access Granted with Anti-passback Violation in the Online Transactions.
- Timed Anti-passback Mode – Timed anti-passback mode can be used in a controlled enter/exit environment with IN/OUT readers or where a single reader is designated with anti-passback.
 - Controlled enter/exit environment with IN/OUT readers - A credential cannot be presented consecutively to IN or OUT readers within the specified time otherwise access is denied and an Anti-passback violation is generated in the Online Transactions. However, when access is granted at the IN reader, and the cardholder presents the credential at the OUT reader, the timer is re-set to zero until the next IN or OUT read.
 - Single reader designated with anti-passback - A credential cannot be presented consecutively at the reader within a specified time limit otherwise access is denied and an Anti-passback violation is generated in the Online Transactions.

- Executive Access exempts cardholders in the specified door groups from anti-passback restrictions. Executive Access can be one door group or a consecutive range of door groups.
- Global Executive Access is not applicable for a single ACU configuration.

Door Operation Modes

When assigning a door operation mode in the Door Output form, you have one of the following six options to select from depending on the door configuration.

- Unlocks Door and Shunts Contact - select if the door is equipped with an exit device. The door is unlocked when the exit device is activated. The door unlock timer and the door held open timer start when the contact is shunted.
- Shunts Door Contact Only - select if the door is equipped with a sensor device. The door contact is shunted when the sensor is activated but the door must be physically unlocked via the door latch / strike plate. The door held open timer starts when the contact is shunted.
- Free Egress - Door Held Open Alarm Only - select if the door is not equipped with an exit or sensor device. The door is locked until it is physically unlocked via the door latch / strike plate. The door held open timer starts when the door is opened.
- Unlocks Door and Shunts Contact (No RTE Transaction) - is the same as Unlocks Door and Shunts Contact except that no transaction is recorded in the system log.
- Shunts Door Contact Only (No RTE Transaction) - is the same as Shunts Door Contact Only except that no transaction is recorded in the system log.
- Unlocks Door and Shunts Door Contact (Door closing does not relock door) - is the same as Unlocks Door and Shunts Door Contact except that the door does not relock on closing.

Procedures

► *Steps to Create Door Names and Reader Outputs without Anti-passback*

From the main screen, select Door Maintenance > Set Door & Reader Parameters.

Select the Reader Information tab at the top of the Set Door & Reader Parameters form.

1. If there is more than one access control unit for the site, click on the down arrow on the right side of the Unit ID and select the access control unit from the drop down list. If there is only one access control unit in the system, bypass this step. The correct unit will already be listed in this field.
2. Click the cursor inside the Reader Port #1 text box and type the name of the door where the reader is located.
3. If applicable, specify the direction of the reader if it has an In or Out assignment, otherwise leave the Direction field set on In.

4. Ensure the box to the left of Anti-Passback is unchecked (inactive).
5. Repeat steps 4 to 6 until each door has been assigned a Reader Port name.
6. Click on the Save button and then follow Steps to Assign Door Outputs.
7. If you have multiple access control units, repeat Steps to Create Reader Port Names without Anti-passback and Steps to Assign Door Outputs for each access control unit.

► *Steps to Create Door Names and Reader Outputs with Anti-passback*

1. From the main screen, select Door Maintenance > Set Door & Reader Parameters.
2. From the Set Door and Reader Parameters form, select the Reader Information tab if it is not selected.
3. If there is more than one access control unit, click on the down arrow to the right of Unit ID, and select the access control unit from the drop down list. If there is only one access control unit, bypass this step. The correct unit will already be listed in this field.
4. Click the cursor inside the Reader Port #1 text box, and type the name of the door where the reader is located.
5. Click on the down arrow to the right of Direction and from the drop down list select In or Out depending on the reader's directional assignment.
6. Click in the box on the left side of Anti-passback to enable this option. The box has a check mark when enabled.
7. At the bottom of the Set Door and Reader Parameters form, click on the Anti-passback Setup Mode button.
8. Under Anti-passback Mode, select the mode by clicking in the radio button to the left. Be sure to select a mode that is applicable to your configuration.
9. If certain door groups are exempted from anti-passback restrictions, under Executive Access click on the down arrow to the left of the < > symbols and select either the first door group where a consecutive range of door groups applies or the only door group where a single door groups applies.
10. Under Executive Access, click on the down arrow to the far right of the < > symbols and select either the last door group where a consecutive range of door groups applies or the same door group as selected in the previous step where a single door group applies.
11. If Executive Access was selected in the preceding step, ensure that the box to the left of Global Executive Access is unchecked.
12. Click on the OK button.

13. If Global Executive Access is disabled (unchecked) either for a single ACU configuration or disabled for a multiple ACU configuration where different door groups have Executive Access at different panels, click on the Yes button. If Global Executive Access is enabled, you will not see this prompt.
14. Repeat steps 4 to 6 to complete naming the reader ports, specifying a reader direction, and anti-passback mode.
15. When you have completed the Reader Information form, click on the Save button, and then follow the Steps to Assign Door Outputs.
16. If you have multiple access control units, repeat Steps to Create Reader Port Names with Anti-passback and Steps to Assign Door Outputs for each access control unit. You do not have to reset anti-passback unless your configuration is option B in step 11.

► *Steps to Set Door and Reader Parameters*

If you have more than 1 access control unit, be sure to complete Reader Information and Door Outputs for all ACUs.

1. From the main screen, select Door Maintenance > Set Door & Reader Parameters.
2. Select the Door Output # 1 tab. You will now set door outputs for the door that was assigned to Reader Port Name # 1.
3. Enter a name in the Door Name # 1 text box. The name should reflect the door's location for easy reference.
4. Click on the down arrow on the right side of the Door Relay Unlock Time field and select a time. The range is 2 to 99 seconds. This is the interval that the door remains unlocked after a card has been presented to the reader. (0 toggle = toggles the output state.)
5. Click on the down arrow on the right side of the Door Held Open Time field and select a time. The range is 1 to 99 seconds. This is the time interval that the door may remain open before the system reports a door held open violation.
6. A Door Operation Mode must be selected to prevent an alarm event when someone opens a controlled door to exit. Click on the down arrow to the right of Door Operation Mode, and select one of the following door exit options.
 - Unlocks door and shunts door contact
 - Shunts door contact only
 - Free egress. Door held open alarm only.
 - Unlocks door and shunts contact (no RTE Transaction)
 - Shunts door contact only (no RTE Transaction)

- Unlocks door and shunts door contact only (does not relock door on closing)
7. Click on the down arrow on the right side of the Alarm on Forced Entry Output and select an output. If you select 000 – No Output Assigned, an alarm warning does not occur if there is a forced entry at this door.
 8. Click on the down arrow on the right side of the Alarm Held Open Timer Output and select an output. If you select 000 – No Output Assigned, an alarm warning does not occur if the door remains open longer than the door relay unlock time.
 9. The Handicap Door Timer and the Handicap Door Held Open fields only require completing if you have doors equipped with door operators for handicap accessibility and those door operators have been connected to the proper relays in the Keyscan access control units(s). If applicable, click on the down arrow on the right side of the Handicap Door Timer field and select a time that the handicap output relay will pulse the door operator. The range is 2 to 99 seconds. The Handicap feature is an optional component.
 10. If applicable, click on the down arrow on the right side of the Handicap Door Held Open field and select a time that the door may remain open before the system reports a door held open violation. The range is 1 to 99 seconds.
 11. When the door outputs have been assigned to Door Output # 1, select the Door Output # 2 tab and complete the outputs for Door Name # 2. Repeat for each door output.
 12. Click on the Save Doors button when you have completed naming and assigning outputs to your doors.

Assign Time Zones to Doors

The Assign Time Zones to Automatically Unlock/Lock Doors form allows you to automatically unlock and lock a specific door during a specified time zone. You might use this feature for a front door allowing visitors access to your lobby or reception area during regular business hours.

If you do not wish to have doors automatically lock and unlock during a time zone, leave the doors on the default setting of Not Applicable (N/A).



We suggest you review First Person In Time Zone to understand how this function works and how it acts as a building safeguard.

When you assign time zones to automatically unlock doors, it is strongly recommended to use the First Person In option, especially for exterior doors. This prevents access to your site in the event that the building is unattended after a time zone starts and automatically unlocks the door. An example might be during a

severe storm or a traffic jam and you or your staff can't get to the building before the time zone unlocks an entrance door. Designating the door with First Person In keeps your site secure by stopping the time zone from unlocking the door until someone presents a valid card to the reader.

If a time zone has been set to Shunt Door Contact Only (Door Remains Locked), the time zone is underlined.

Procedures

► *Steps to Assign Time Zones to Doors*

1. From the main screen, select the Door Maintenance menu > Assign Time Zone to Doors.
2. Opposite the appropriate access control unit, double click on the box that is under the door number. The Door Name and Door Output # fields display your selection.
3. In the Time Zone Selection box, click inside the radio button on the left side of the Time Zone Limited Access field to activate this option. The Time Zone Selection box is located in the middle of the Assign Time Zone to Automatically Lock/Unlock Doors form.
4. Click on the down arrow, located above the Time Zone button, and select the time zone from the drop down list. A copy of the time zone is exhibited at the bottom.
5. To set the door for First Person In (recommended if this is an exterior or public access door), click on the Time Zone button and go to the next step. If the door is not being set for First Person In, go to step 14.
6. From the Door Time Zones form, click on the First Person In button.
7. From the Set First Person In form, the appropriate access control unit should be pre-selected. If not, click on the down arrow of the Unit ID field and select the unit.
8. Click in the box to the right of the door to activate the First Person In for that door.
9. Click on the Save button.
10. Click on the OK button in the Save Changes dialog box.
11. Click on the Exit button in the First Person In form, to return to the Time Zone form.
12. Click on the Exit button on the Door Time Zone form.
13. Click on the down arrow, located above the Time Zone button, and re-select the same time zone from the drop down list.

14. Click on the OK button.
15. Repeat the above steps for another door, or click on the Save & Exit button to return to the main screen.

Related Topics

▶ *First Person In Time Zone*

▶ *Door Time Zones*

First Person In

First Person In, accessed from the Door Time Zones form, is a system safeguard that keeps a time zone OFF after its appointed start time until a valid card is presented. It is important to understand that all doors set on auto unlock, all door groups, and all Auxiliary Input Shunt/Auxiliary Output devices assigned to a time zone are affected whenever First Person In is selected.

The Set First Person In form is used to select target readers that enable the time zone. One or multiple readers/keypads can be selected. Until a valid cardholder from an authorized door group presents his or her card to a designated target reader, a time zone designated with first person in remains OFF regardless of its start time.



First Person In is based on time zones; it cannot be set to an individual cardholder.

Procedures

▶ *Steps to Set First Person In*

1. To set a door to First Person In, select Time Zones/Schedules > Door Time Zones.
2. From the Door Time Zones form, click on the down arrow to the right of Time Zone # and select the time zone assigned to the door group whose access will be restricted by First Person In. The door group assigned to this time zone cannot access the door until a valid cardholder from an another authorized door group first presents a card.
3. Click on the First Person In button on the Door Time Zones form.
4. From the Set First Person In form, click on the down arrow of the Unit ID field and select the appropriate access control unit.
5. From the Set First Person In dialog box, click in the box to the right of the door to activate the First Person In for that door.
6. Click on the Save button.

7. Click on the OK button in the Save Changes dialog box.
8. Click on the Exit button in the First Person In form, to return to the Time Zone form.
9. Click on the Exit button in the Door Time Zones form.

Related Topics

▶ *Example of First Person In*

▶ *Assign Time Zones to Doors*

First Person In - Example

In the example Set First Person In screen below, the Front Door is designated as the target reader, indicated by the check. Until a cardholder from a door group assigned to a time zone other than Time Zone 1, presents his or her card at the Front Door reader, all Time Zone 1 assignments remain disabled or OFF affecting the following readers, door groups and devices:

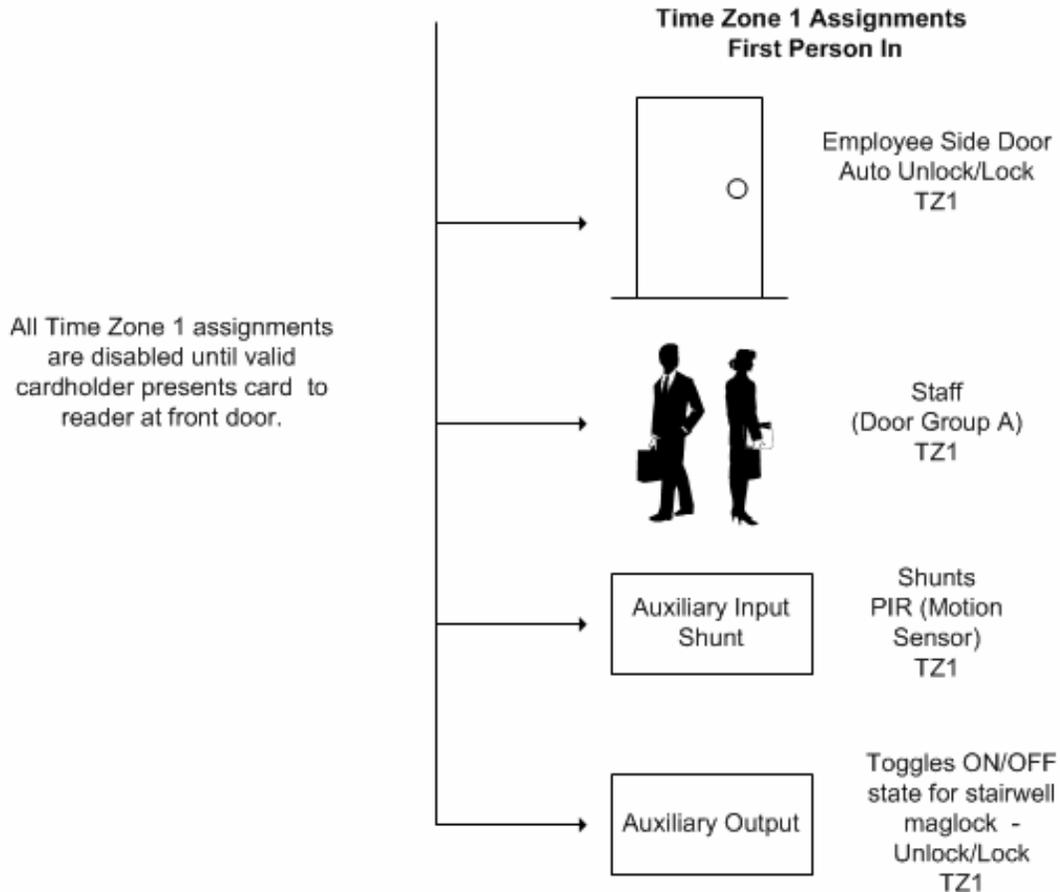
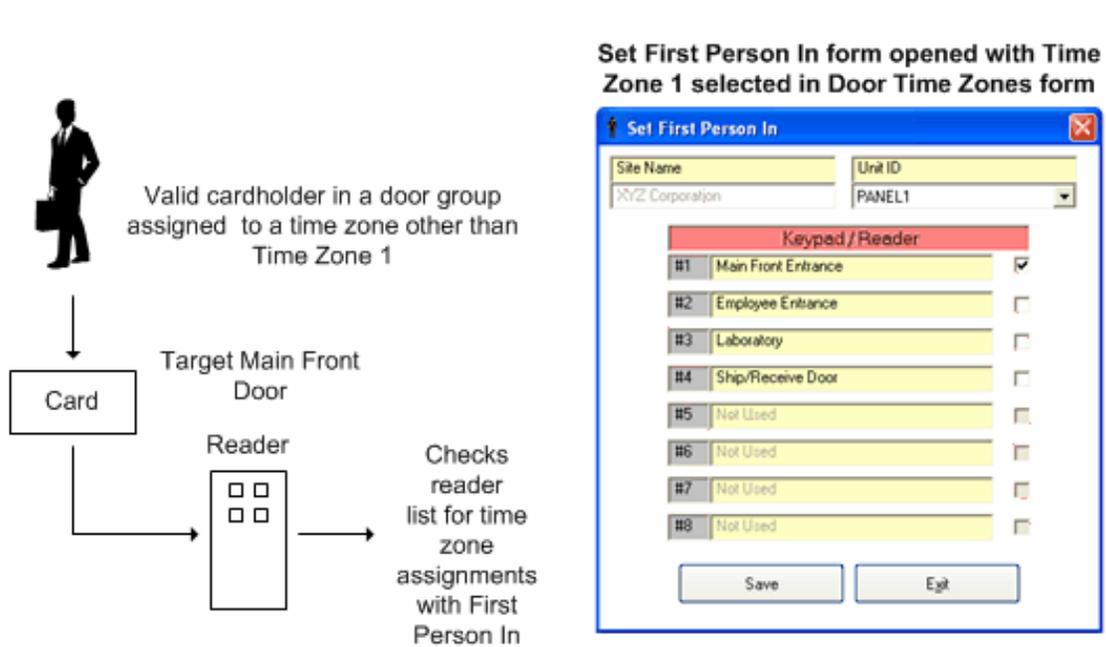
- the Employee Side Door set to automatically unlock at the start of Time Zone 1 remains locked
- cardholders in Admin Staff Door Group cannot access reader-controlled doors assigned to Time Zone 1
- devices remain in their Time Zone 1 OFF state

Remember, when designating a reader or readers, those readers act as the target readers to enable the time zone that was displayed in the Door Time Zones form.

Related Topic

▶ *First Person In*

Example of First Person In Enabled at Main Front Door



Set Auxiliary Output Names & Auxiliary Output Status

The Set Auxiliary Output Names & Set Auxiliary Output Status form is used to assign names to auxiliary outputs in both ON and OFF states. Your dealer/installer should determine these names and settings if the access control system is configured for auxiliary outputs.

Procedures

► *Steps to Set Auxiliary Output Names & Auxiliary Output Status*

1. From the main screen, select Door Maintenance > Set Auxiliary Output Names & Set Auxiliary Output Status > No (if the warning message appears).
2. Click on the down arrow in the Unit ID field and select the access control unit from the drop down list if there is more than one ACU within the site. The total number of auxiliary outputs is listed in the Number of Auxiliary Outputs field.
3. In the table, double click on the auxiliary output to be named.
4. Enter a name in the ON AO Name text box.
5. Enter a name in the OFF AO Name text box.
6. Click on the Apply Changes button.
7. When you have completed naming the auxiliary outputs, click on the Apply Changes button. Wait for the Processing Communications Request form to close.
8. Click on the Exit button to return to the main screen.

Set Auxiliary/Supervised Input Names-Output Assignment

By assigning outputs to auxiliary / supervised inputs, you assign those inputs to activate outputs in alarm conditions. If a Supervised Input Board has been connected to an ACU, select the Add Optional Supervised Inputs button to interface those inputs with the software. Your dealer/installer should determine these settings if applicable.

Procedures

► *Steps to Set Auxiliary/Supervised Input Names-Output Assignment*

1. From the main screen, select the Door Maintenance menu > Set Auxiliary / Supervised Input Names_ Output Assignments.
2. Click on the down arrow of the Unit ID field and select the control panel from the drop down list.
3. Double click on the auxiliary input (AI) or the supervised input (SI) from the appropriate list.

4. Click in the AI Name or SI Name text box and enter the name of the input.
5. Click on the down arrow of the Output Assigned field, immediately below the AI / SI Name text box, and select the output from the drop down list.
6. Click on the OK button.
7. Click on the Save & Exit button to return to the main screen.

Set IOCB1616 Parameters

Setting IOCB1616 parameters requires IOCB1616 input/output control boards connected to the access control panels. The IOCB1616 circuit boards are for special applications. The Set IOCB1616 Parameters form should only be completed by a dealer/installer.

Assign Time Zones to Auxiliary Outputs

The Assign Time Zones to Auxiliary Outputs feature allows you to assign a time zone to an auxiliary output to turn it off and on. If you are not using auxiliary outputs, you can by-pass this procedure. You may wish to consult with your dealer or installer.



You can create time zones from the Assign Time Zones to Auxiliary Outputs form. Double click an output, and select the Time Zone button.

Procedures

►Steps to Assign Time Zones to Automatically Toggle Auxiliary Outputs

1. From the main screen, select the Door Maintenance menu > Assign Time Zones to Auxiliary Outputs.
2. In the table, double click on the appropriate box that lines up with the Unit ID and Output Number that is being assigned a time zone.
3. Click in the radio button to activate Time Zone Limited Access.
4. Click on the down arrow below and to the right of the Time Zone Limited Access field and select the appropriate time zone for the auxiliary output.
5. Click on the OK button.
6. After you have completed assigning time zones to auxiliary outputs, click on the Save & Exit button to return to the main screen.

Related Topic

►Set Auxiliary Output Names & Auxiliary Output Status

Assign Time Zones to Auxiliary Inputs

Use this feature to have a time zone automatically arm and disarm auxiliary inputs or use an input to start and end a time zone depending on your site's security requirements. If you are not using auxiliary inputs, you can by-pass this procedure. You may wish to consult with your dealer or installer.

Input Type

Under the Input Type field, there are two options:

- 1 TZ > AI - the assigned time zone automatically arms & disarms the auxiliary input
- 2 AI > TZ - the assigned auxiliary input automatically starts & ends the time zone

Time Zone & Auxiliary Input States

TZ	➔	AI
ON		Disarmed
OFF		Armed
AI	➔	TZ
Open		OFF
Closed		ON
AI = Auxiliary Input / TZ = Time Zone		



You can create time zones from the Assign Time Zones to Auxiliary Inputs form. Double click an input, and select the Time Zone button.

Procedures

►Steps to Assign Time Zones to Auxiliary Inputs

1. From the main screen, select the Door Maintenance menu > Assign Time Zones to Auxiliary Inputs.
2. Click on the down arrow of the Unit ID field, and select the unit name from the drop down list.
3. Select the auxiliary input from the table that lists all the auxiliary inputs available.
4. Under Input Type, click on the down arrow to the right and select the appropriate assignment, either:
 - 1 TZ > AI
 - 2 AI > TZ

5. Click in the radio button to activate Time Zone Limited Access.
6. Click on the down arrow below and to the right and select the appropriate time zone for the auxiliary input.
7. Click on the OK button.
8. After you have completed assigning time zones to auxiliary inputs, click on the Save & Exit button to return to the main screen.

Assign Time Zones to Supervised Inputs

Use this feature to automatically arm and disarm supervised inputs at designated times depending on your site's security requirements. Supervised inputs cannot be used with the CA 200 model.

If you are not using auxiliary inputs, you can by-pass this procedure. You may wish to consult with your dealer or installer.



You can create time zones from the Assign Time Zones to Auxiliary Inputs form. Double click an input, and select the Time Zone button.

Procedure

► Steps to Assign Time Zones to Supervised Inputs

1. From the main screen, select the Door Maintenance menu > Assign Time Zones - Supervised Inputs.
2. Click on the down arrow of the Unit ID field, and select the access control unit name from the drop down list.
3. Select the supervised input from the table that lists all the supervised inputs available.
4. Click in the radio button to activate Time Zone Limited Access.
5. Click on the down arrow below and to the right and select the appropriate time zone for the supervised input.
6. Click on the OK button.
7. After you have completed assigning time zones to supervised inputs, click on the Save & Exit button to return to the main screen.

Assign Time Zones to Readers/Keypads

The Assign Time Zones to Readers / Keypads form specifies the reader / keypad configuration that is used to gain access when the door's time zone is ON and when the door's time zone is OFF. This form is used when a door has both a card

reader and a keypad.

If the door has only one of the two devices, you can by-pass this step.

The three reader / keypad setup modes are outlined below:

- Card or Keypad – Only 1 of the two is used at the door
- Card Only – Only the card reader is used at the door
- Card and Keypad – The card reader and the keypad are used at the door

As an example, door A has a reader and a keypad. When the door's time zone is in ON, one of the following three conditions would be in effect:

- If Access Zone ON is set to Card or Keypad, valid cardholders can either present their card to the reader to access the door or enter their Personal Identification Number on the keypad to access the door.
- If Access Zone ON is set to Card Only, valid cardholders can only present their card to the reader to access the door, the keypad is excluded from use.
- If Access Zone ON is set to Card and Reader, valid cardholders must present their card to the reader and enter their Personal Identification Number on the keypad to access the door.

The same conventions apply for Access Zone OFF, whichever card/keypad option is selected.



If your system uses either an HID reader/keypad (Keyscan part # HID-5355KP) or an Indala reader/keypad (Keyscan part # P XK501), please be aware of the following procedure. We recommend that when an individual is keying in their Personal Identification Number on one of the aforementioned reader/keypads, he or she press the star * key first, then enter their PIN code. Pressing the star key * clears any previous numbers that may still be stored in the reader/keypad. This procedure eliminates the potential of the keypad misreading a valid PIN entry and denying access. When the system is set to Card and Keypad the card read or PIN entry can be in any order. (Either of these two reader/keypads, should have been purchased through Keyscan so they interface correctly with your Keyscan system.)

Procedures

► *Steps to Assign Time Zones to Readers/Keypads*

1. From the main screen, select the Door Maintenance menu > Assign Time Zones to Reader / Keypad Operations. Wait for the Processing Communications Request box to close.
2. If it is not listed, click on the down arrow below the Unit ID field and select the appropriate access control unit from the drop down list. If you selected a unit other than the one listed, wait for the Processing Communications Request box to close.

3. Click on the down arrow below the Current Access Mode field for the door you are assigning reader / keypad access to and select one of the available options from the drop down list.
4. Under the TZ field, double click in the corresponding white box for the door you are working on. The Time Zone Selection form opens in the middle of the screen.
5. Click inside the radio button on the left side of Time Zone Limited Access field to activate this option.
6. Click on the down arrow, located above the Time Zones button, and select the time zone from the drop down list. A copy of the time zone is exhibited at the bottom.
7. Select OK.
8. Click on the down arrow below the Access Zone ON field and select one of the available options from the drop down list.
9. Click on the down arrow below the Access Zone OFF field and select one of the available options from the drop down list.
10. To assign reader / keypad access to another door, repeat the above steps.
11. Select Save & Exit after you have completed assigning reader / keypad access to the doors in the system. Wait for the Processing Communications Request box to close.

Set Alarm Response Instructions/Alarm Graphic Locations

The Set Alarm Response Instructions & Alarm Graphic Locations is an important form that provides critical information in the event of a system alarm.

When an alarm is tripped, the alarm is listed in the Alarm Monitoring window. The person monitoring the system double clicks on the alarm listing, which opens the Alarm Response Instructions form with contact and response information so the proper authorities can be alerted.

The Set Alarm Response Instructions & Alarm Graphic Locations form is specific to individual doors or devices. You must complete a form for each door or device that is to have response instructions conveyed.



Floor plans or building schematics must be created in the Photo Badge Template Editor before they can be imported in the Set Alarm Response Instructions & Alarm Graphic Locations form. You do not need a license to use the map function in the Photo Badge Template Editor. The Photo Badge Template Editor will also import basic AutoCAD - DXF files.

Procedures

► *Steps Set Alarm Response Instructions/Alarm Graphic Locations*

1. From the main screen, select the Door Maintenance menu > Set Alarm Response Instructions & Alarm Graphic Locations.
2. Click on the down arrow for the Unit ID, Input Name, Connection Number field and select the door or device from the drop down list.
3. In the Location text box, enter a brief description of the door or device location.
4. In the Instructions text box, enter brief instructions to be carried out.
5. Click on the down arrow for the Alarm Contacts field and select a name from the drop down list. You must have entered names on the Site Contact Information form and assigned the person with Notify Contact status under Contact Type. The Site Contact Information form is found under System Settings menu > Site Setup > Site Information.
6. Click on the down arrow for the Emergency Contacts field and select a name from the drop down list. As above, you must have entered names on the Site Contact Information form and assigned the person with Notify Contact status under Contact Type.
7. To incorporate floor plans or building schematics, click on the Load Picture button.* (Optional)
8. From the Select Alarm Bitmap dialog box, navigate to the directory and select the diagram file.
9. Click on the OK button.
10. Click on the Save button.
11. To set instructions for another door or device, repeat steps 2 - 10, or select the Exit button to return to the main screen.

Door Group Access Levels

Assign Door Group Access Levels

The Door Group Access Levels is laid out in a table format showing all details about door access levels. It's used to assign each door group an access level to the doors controlled by the ACUs in your system. There are three access levels as listed below:

- 24 Hour Access – 24 HR
- No Access – N/A
- Time Zone Limited Access – TZ-###

The door group names are listed in a column on the far left, the reader (door) names are listed in a row along the top, and the access levels are set out in a grid in the body of the table.

A time zone that has been tagged with Present 3 has a hand/card icon. A time zone that has been tagged with First Person In is underlined and displayed in red.

Procedures

►Steps to Assign Door Group Access Levels

1. From the main screen, select Quick Buttons> Group Access Levels > Door Group Access Levels.
2. Access levels can be assigned by the following methods:
 - To assign one door group an access level for one door, double click in the table on the grid location that corresponds to the door group / door.
 - To assign the same access level to all door groups for one door, click on the door number listed in the blue row at the top of the table.
 - To assign the same access level to multiple door groups for one or multiple doors, click on the upper left grid location and hold and drag the mouse to the lower right grid location.
3. Select one of the radio buttons to determine the access level:
 - 24 Hour Access (If 24 Hour Access is selected, see step 5)
 - No Access (If No Access is selected, see step 5)
 - Time Zone Limited Access (If Time Zone Limited Access is selected, see step 4.)
4. Click on the down arrow below and to the right of the Time Zone Limited Access field and select the time zone from the drop down list.
5. Select OK.
6. Repeat the above steps until all door groups have been assigned an access level for each door.

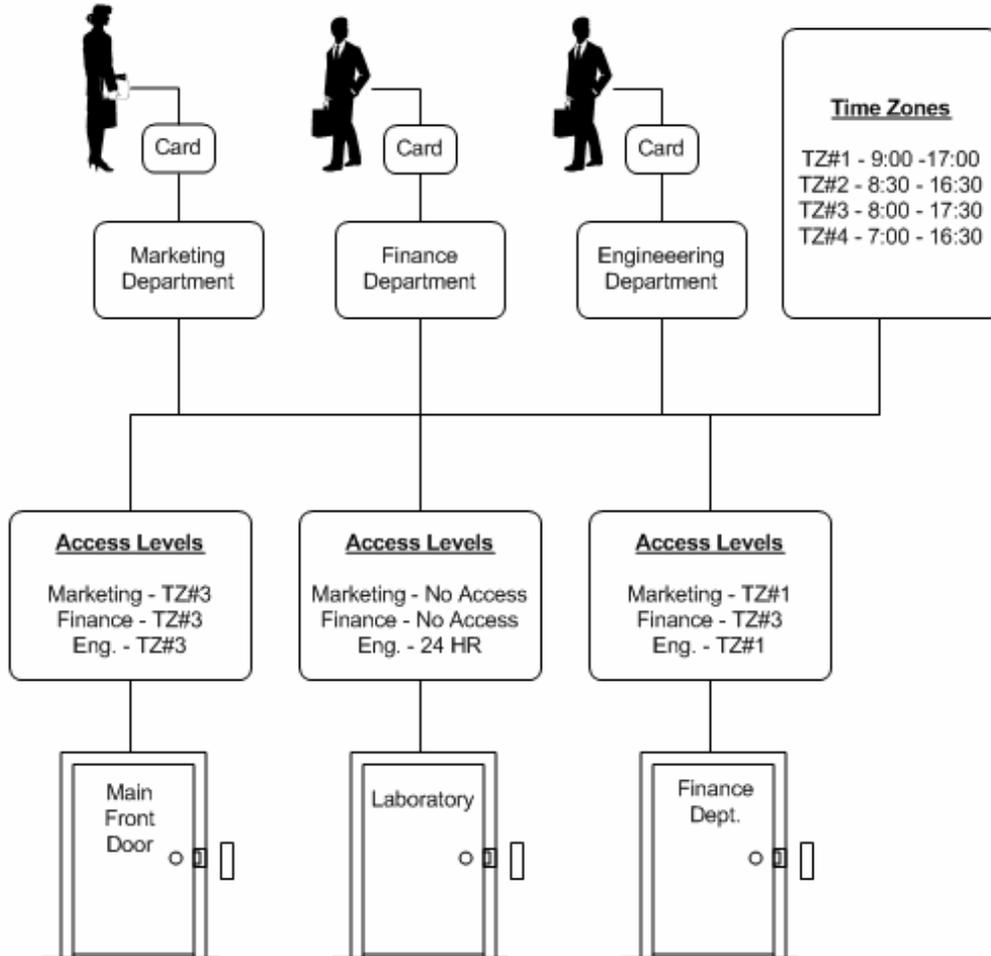
7. Select the Save & Exit button.

Related Topic

- ▶ *Example of Door Group Access Levels*
- ▶ *First Person In Time Zone*
- ▶ *Present 3*

Assign Door Group Access Levels - Example

The following diagram illustrates an example site where there are 3 different door groups Marketing, Finance, and Engineering, and 3 doors that are controlled by an ACU. Door group access levels are summarized above each door. Time Zones are listed on the right. You will note that door groups either have 24 access, no access, or limited access based on a time zone.



Access levels may be set to - time zone access / 24 hour access / no access

Elevator Setup

Setting Up Elevators

The forms within the Elevator Controllers menu define your elevators and establish which cardholders have access to specific floors at specific times within the elevator system.

Valid cardholders present their cards or credentials at the reader and press a floor button. If the cardholders have authorization within the specified time zone for the floor that was selected, the system allows access to the floor. If the cardholders don't have authorization, the floor button is locked out and the elevator remains stationary.



If your site does not have elevators or they are not included in the Keyscan system, leave the forms in the Elevator Controllers menu blank and move to the next setup section.

Elevator Group Names

Creating Elevator Group Names allows you to place cardholders into specific groups based on their security and access levels. When creating a new elevator group name, it should correspond to descriptions that are generally applied to groups within your organization, as well as how you may have named your door groups.



Unassigned elevator groups appear as 001-Group # 1 etc. You may create up to 511 different elevator groups.

When creating elevator group names, the System VII software makes elevator groups #001 to #016 active by default. If you create elevator group names from elevator group #017 to #511, ensure that you enable the Group Active field otherwise those elevator groups can't be assigned access levels in the Assign Elevator Group Access Levels form.

Procedures

►Steps to Add Elevator Group Names

1. From the main screen, select Elevator Controllers > Modify Elevator Group Names.
2. Double click on the first open elevator group from the Search Elevator Groups form to open the Group Information form.
3. Click the cursor inside the Group Description text box and type the name of the elevator group.

4. If it is inactive, click in the Group Active box to activate the elevator group. The box has a check mark when active.
5. Select Save & Exit.
6. To add another elevator group name, repeat the above steps, or select the Exit button to return to the main screen.

Set Elevator Bank Names

Because elevators have access to identical floor numbers or may be in the same tower, creating bank names differentiates one group of elevators from another. You must create elevator bank names before you can set any other elevator parameters.

Procedures

►Steps to Set Elevator Bank Names

1. From the main screen, select Elevator Controllers > Set Elevator Bank Names.
2. Double click on an open elevator bank name from the Set Elevator Bank Names form to open the Elevator Bank Name text box.
3. Type the name of the elevator bank in the Elevator Bank Name text box. The maximum number of elevator banks is 10.
4. Click on the OK button.
5. Repeat the above steps to add another elevator bank name, or click on the Save & Exit button to return to the main screen.

Set Elevator Names and Floor Hold Times

Each elevator in the system must be identified with a name and given a floor button selection time. The floor button selection time is the number of seconds that the authorized elevator floor buttons are active after a valid card is presented to the reader.



Creating elevator names is per each elevator control panel. As such, for EC2000 models, you create only 1 elevator name per panel.

Designed for buildings that have an integrated telephone entry system, the Set Elevator Names form has a Telephone Interface Floor Button Selection Time field. This field sets the number of seconds that the authorized elevator floor buttons are active after a visitor has been "buzzed in" via the telephone system.

Procedures

► *Steps to Set Elevator Names and Floor Hold Times*

1. From the main screen, select Elevator Controllers > Set Elevator Names and Floor Hold Times.
2. Click on the down arrow on the right side of the Unit ID field, and select the appropriate elevator control unit from the drop down list.
3. Click in the Elevator Name # text box, and enter a name for the elevator.
4. Click on the down arrow on the right side of the Floor Button Selection Time, and select a value in seconds from the drop down list.
5. If the elevator controller interfaces with a telephone entry system, click on the down arrow on the right side of the Telephone Interface Floor Button Selection Time, and select a value in seconds from the drop down list.
6. Click on the Save & Exit button.
7. Repeat the above procedures for each elevator control board.

Assign Elevators to Elevator Banks

Because elevators have access to identical floor numbers or may be in the same tower, the elevator must be assigned to an elevator bank even if there is only 1 elevator in the bank.

Before assigning elevators to elevator banks, you must first have completed naming the elevator banks and naming the elevators.

Procedures

► *Steps to Assign Elevators to Elevator Banks*

1. From the main screen, select Elevator Controllers > Assign Elevators to Elevator Banks.
2. Click the down arrow in the Elevator Bank column opposite the elevator listed in the Elevator Name column.
3. From the drop down list, select the correct elevator bank.
4. Repeat the above steps until all the elevators are assigned to elevator banks.
5. Click on the Save & Exit button to return to the main screen.

Set Elevator Floor Names

The Set Elevator Floor Names form is used to identify the names of floors so that access levels can be set in the Elevator Group Access Levels form.

Procedures

► *Steps to Set Elevator Floor Names*

1. From the main screen, select Elevator Controllers > Set Elevator Floor Names.
2. From the Select Elevator Banks dialog box, click the down arrow to the right under the Elevator Bank Name. Select the appropriate elevator bank from the drop down list.
3. Click on the OK button.
4. From the Set Elevator Floor Names form, double click on Floor #1 in the table section of the form.
5. Click in the Floor Name text box and enter a name for the floor. The maximum is 15 characters.
6. Click on the Update button. The floor name is added to the list.
7. Repeat the above steps until you are finished naming floors.
8. Click on the Exit button to return to the main screen.

Set Elevator Banks to Time Zones

The Set Elevator Banks to Time Zones form allows you to set multiple time zones for elevator banks regulated by elevator control units.

Elevator Time Zones

When you create elevator time zones it is important to think in terms of the Elevator Groups and the times that those groups will use elevators in the building. Each time zone may have multiple schedules.

- Time zones/schedules are based on a 24-hour clock
- Maximum of 254 named time zones
- Combined total of time zones and schedules is 512
- Maximum range of a time zone or schedule is 00:01 to 23:59

The default setting of 00:00 in the Keyscan software represents No Time. It does not represent midnight. If either the start time or the end time is assigned 00:00 the following conditions will result:

- If the start time is set to 00:00 – The time zone is not enabled.
- If the end time is set to 00:00 – The time zone is not disabled.

Setting elevator time zones does not regulate doors.

Elevator Schedules

You may have multiple elevator schedules that are nested within an elevator time zone. Unlike time zones, however, schedules are not specifically named and reside within the time zone. A schedule could be used when you have shifts. As an example, the first shift works from 7:00 to 15:00 and the second shift works from 15:30 to 23:30, Monday through Friday. The hours 7:00 to 15:00 could be saved as Time Zone # 1, and the second shift 15:30 to 23:30 could be saved as a schedule within Time Zone # 1.

Procedures

►Steps to Set Elevator Banks to Time Zones

1. From the main screen, select Elevator Controllers > Set Elevator Banks to Time Zones.
2. From the Select Elevator Banks dialog box, click the down arrow to the right under the Elevator Bank Name. Select the appropriate elevator bank from the drop down list..
3. Click on the OK button.
4. Click on the Add New Time Zone button. The program assigns a Time Zone #.
5. Enter a descriptive title in the Elevator Time Zone Description text box to identify the time zone.
6. In the Mon time boxes, the upper box is the start time and the lower box is the end time. Select the hour in the upper box and click the up or down arrow at the right to set the start hour.
7. Select the minutes and click the up or down arrow to set the start minutes. You should still be in the upper box under Mon.
8. Select the hour in the lower box under Mon and click the up or down arrow at the right to set the end hour.
9. Select the minutes and click the up or down arrow to set the end minutes.
10. Repeat steps 6 to 9 for each day that falls within the time zone or, if applicable, use one of the Copy buttons on the left of the Set Elevator Banks to Time Zones form.
11. Click on the Save Schedule button.
12. To add another time zone, click on the Add New Time Zone button and repeat steps 4 to 11. To return to the main screen, click on the Exit button.
13. If you have multiple elevator banks, repeat the preceding steps to create time zones for each elevator bank.

►Steps to Add an Elevator Schedule

1. Click on the down arrow of the Time Zone # and select the time zone from the drop down list. Be sure the Time Zone # is highlighted in blue.
2. Click on the Add New Schedule button.
3. In the Warning dialog box "Adding multiple schedules...", select the Yes button.
4. In the Mon time boxes, the upper box is the start time and the lower box is the end time. Select the hour in the upper box and click the up or down arrow at the right to set the start hour.
5. Select the minutes and click the up or down arrow to set the start minutes. You should still be in the upper box under Mon.
6. Select the hour in the lower box under Mon and click the up or down arrow at the right to set the end hour.
7. Select the minutes and click the up or down arrow to set the end minutes.
8. Repeat steps 4 to 7 for each day that falls within the time zone or, if applicable, use one of the Copy buttons on the left of the Set Elevator Banks to Time Zones form.
9. Click on the Save Schedule button.
10. To add another schedule, click on the Add New Schedule button and repeat steps 2 to 9. To return to the main screen, click on the Exit button.

Set Elevator Time Zones to Automatically Lock/Unlock Floor Buttons

The Assign Elevator Time Zone to Automatically Lock / Unlock Elevator Floor Buttons allows you to assign specific floor buttons to automatically unlock at the start of a time zone and re-lock at the conclusion of the time zone. There are two elevator access modes:

- No Access Without Valid Card – If this option is selected, the elevator floor button is locked out until a valid card is presented to the reader. The floor is not accessible to persons without a valid card. This is the default setting, represented by N/A.
- Time Zone Limited Access – If this option is selected, the elevator floor button is unlocked during its assigned time zone. A card is not required to access the floor while the time zone is in effect.

As an example, your building has 4 floors. During your regular business hours of 9:30 to 4:30, the public needs access to your customer service department located on the 2nd floor. However, 3rd and 4th floor access is restricted to employees. To set the conditions that satisfy this situation, Floor 2 would be assigned Time Zone Limited Access; its time zone would start at 9:30 and end at 16:30. Floors 3 & 4

would retain their default setting N/A - No Access Without Valid Card.



If access to all floors is restricted to valid cardholders, you can bypass this step.

Procedures

► *Steps to Set Elevator Time Zones to Automatically Lock/Unlock Floor Buttons*

1. From the main screen, select Elevator Controllers > Assign Elevator Time Zone to Automatically Lock / Unlock the Elevator Floor Button.
2. From the Select Elevator Banks dialog box, click the down arrow to the right under the Elevator Bank Name. Select the appropriate elevator bank from the drop down list.
3. Click on the OK button.
4. From the table on the left side of the Assign Elevator Time Zone to Automatically Lock / Unlock the Elevator Floor Button form, select the floor.
5. Click in the radio button to activate Time Zone Limited Access. A card is not required to access the floor during the specified time zone.
6. Click the down arrow below and to the right of the Time Zone Limited Access field and select the time zone from the drop down list. (You have the option of creating or editing a time zone by clicking on the Edit Time Zone button.)
7. Click on the OK button.
8. Repeat the preceding steps for each applicable floor.
9. Click on the Save & Exit button to return to the main screen.

Elevator Group Access Levels

Assign Elevator Floors to Group Access Levels

The Assign Elevator Floors to Group Access Levels form is used to assign each elevator group an access level to the elevator banks / elevator floors controlled by the ECUs in your system. There are three access levels as listed below:

- 24 Hour Access – 24 HR
- No Access – N/A
- Time Zone Limited Access – TZ-###

The Assign Elevator Floors to Group Access Levels form is laid out in a table format. The elevator group names are listed in a column on the far left, the floor numbers are listed in a row along the top, and the access levels set in a grid format in the body of the table.

Procedures

► *Steps to Assign Elevator Floors to Group Access Levels*

1. From the main screen, select Elevator Controllers > Assign Elevator Floors to Group Access Levels.
2. From the Select Elevator Banks dialog box, click the down arrow to the right under the Elevator Bank Name. Select the appropriate elevator bank from the drop down list.
3. Select the OK button.
4. Access levels can be assigned by using any of the following methods:
 - To assign one elevator group an access level for one floor, double click in the table on the grid location that corresponds to the elevator group /floor.
 - To assign all elevator groups the same access level for one floor, click on the floor number at the top of the grid.
 - To assign the same access level to multiple elevator groups for multiple floors, click on the upper left grid location and hold and drag the mouse to the lower right grid location.
5. In the Access Levels dialog box, select one of the radio buttons to determine the access level:
 - 24 Hour Access (If 24 Hour Access was selected, go to step 7.)
 - No Access (If No Access was selected, go step 7.)
 - Time Zone Limited Access (If Time Zone Limited Access was selected, go step 6.)
6. Click on the down arrow below and to the right of the Time Zone Limited Access field and select the time zone from the drop down list.

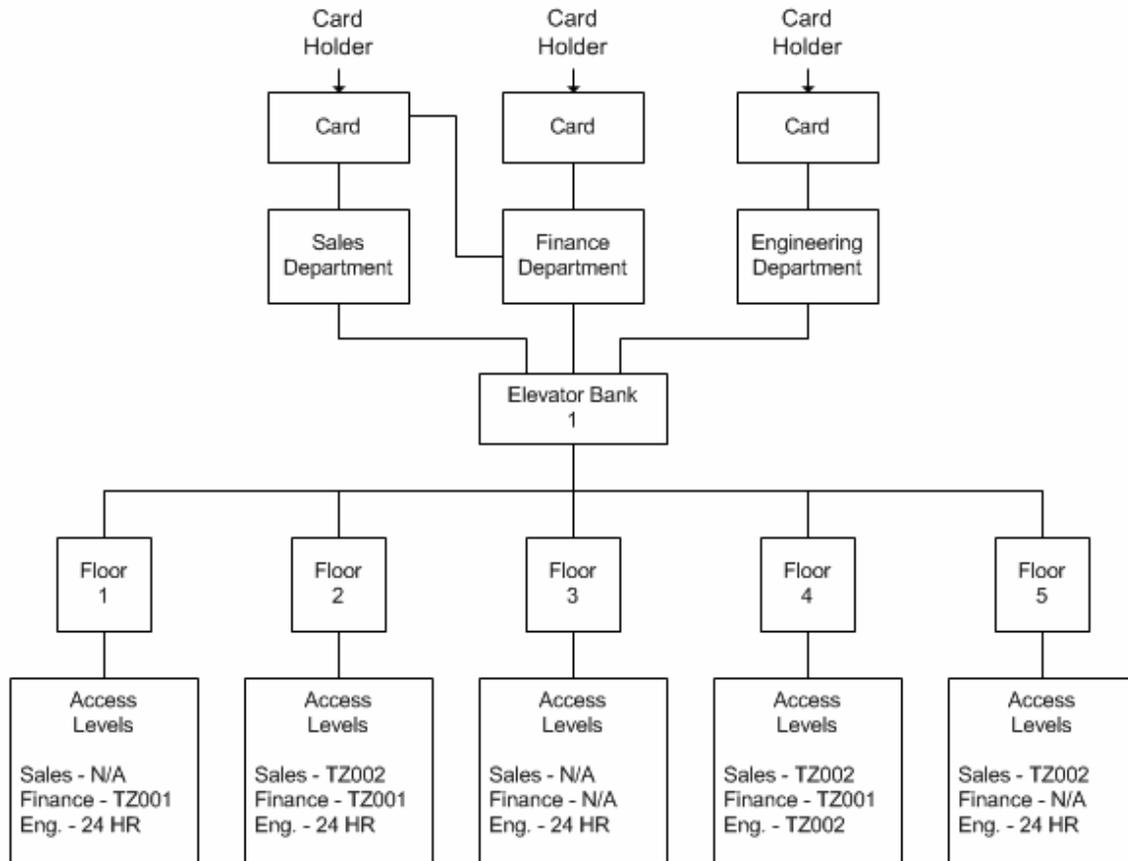
7. Select the OK button
8. Repeat the above steps until all elevator groups have been assigned an access level for each floor.
9. Select the Save & Exit button.
10. If you have multiple elevator banks, repeat the preceding steps for each elevator bank.

Related Topic

▶ *Example of Elevator Group Access Levels*

Elevator Group Access Levels - Example

The following diagram illustrates an example site where there are 3 different elevator groups Sales, Finance, and Engineering, and 1 elevator bank that is controlled by an ECU in a five story building. Each elevator groups's access level is summarized below the floor number. You will note that elevator groups either have 24 hour access, no access, or limited access based on a time zone.



Setup Holidays

Assign Dates to Holiday 1, Holiday 2, or Holiday 3

You assign Holiday 1, Holiday 2, or Holiday 3 to specific calendar dates in the Holidays form which could be for statutory holidays, vacations, facility shutdown days, etc. The maximum number of calendar dates that can be assigned a holiday is sixty-four. Please remember, when assigning either Holiday 1, Holiday 2, or Holiday 3, they override the time zone on that calendar date.

For more information on setting hours for Holiday 1, Holiday 2, or Holiday 3, click on the link to Set Door Time Zones under Related Topic.



You can set recurring holidays that fall on the same calendar date each year, such as New Years Day, so they do not have to be revised each year. Holidays that do not fall on the same calendar date, however, must be set each year. Review and revise those holiday dates at least once a year to maintain an accurate holiday schedule.

Procedures

► *Steps to Assign Dates to Holiday 1, 2, or 3*

1. From the Main Screen, select Quick Buttons > Holidays.
2. Click on the arrows at the top of the calendar to scroll to the desired month and year.
3. Double click on the date of the holiday on the calendar to open the Holiday Detail Information dialog box.
4. Enter the name of the holiday in the Holiday Description text box.
5. Click on the down arrow in the Type field and select the holiday type number from the drop down list.
 - Type 1 = Holiday 1
 - Type 2 = Holiday 2
 - Type 3 = Holiday 3
6. Click on the OK button.
7. From the Do you want this holiday to be a recurring holiday? dialog box, click on the Yes button if the holiday repeats on the same day each year, such as New Year's Day, or click on the No button if the holiday occurs on different dates each year, such as Labour Day.
8. Repeat steps 1 – 6 to add another holiday, or, if you have completed adding holidays, click on the Save & Exit button to return to the main screen.



To remove or undo a holiday, double click on the entry in the Holidays Added to Database table.

Related Topic

▶ *Set Door Time Zones*

Setup Daylight Savings

Daylight Savings

When Daylight Savings is in effect, the clock is moved forward in the spring and moved back in the fall by 1 hour at 2:00 A.M. Accordingly, the system software must be set for daylight savings to maintain accurate time zones and schedules.

When you set the Daylight Savings and the Standard Time dates, the Client software makes the time change at 2:00 A.M. on the assigned dates.



We recommend that you review the daylight savings dates at least once a year.

Procedures

► Steps to Set Daylight Savings

1. From the Main Screen, select System Settings > Daylight Savings.
 - If daylight savings dates have not been set, the Loading Daylight Savings warning box opens. The warning box states that there are no daylight savings entries found in the database, and they must be set manually. Select the OK button to clear the warning box.
2. Under Daylight Savings Begins, click on the down arrow of the box to the left and select First, Second, Third, Fourth etc. depending on when the day occurs in the month. As an example, if daylight savings begins on the second Sunday in the month, you would select Second.
3. Under Daylight Savings Begins, click on the down arrow of the middle box, and select the day of the week when daylight savings begins. Generally, this is on a Sunday at 2:00 A.M.
4. Under Daylight Savings Begins, click on the down arrow of the right box, and select the month when daylight savings begins.
5. Under Standard Time Begins, click on the down arrow to the left box and select when the day occurs in the month.
6. Under Standard Time Begins, click on the down arrow in the middle box and select the day when standard time begins.
7. Under Standard Time Begins, click on the down arrow in the right box and select the month when standard time begins.
8. Click on the Calculate Next Dates button. The daylight savings date is displayed in the Spring Forward box and the standard time date is displayed in the Fall Backward box.
9. If you have more than 1 site and your user account has the necessary permissions, enable the Update All Valid User Sites, by clicking in the box to the left. When enabled, the box has a check mark.

10. Click on the Save & Exit button.

Setup Cardholder Records

Create Cardholder Records

Each person that is assigned a card to access your building or site is referred to as a cardholder. Adding cards / cardholders to the database requires completing the Cardholder form.

The Cardholder form has multiple options that you may or may not require for your records. Also, some functions may not be available, depending on which optional software or hardware you have purchased.

- The optional Photo Badging module is required to attach a cardholder photo on the cardholder record and print photo badges.
- An optional signature tablet is required to capture a signature.

The procedures to complete cardholder records have been divided into topics as they relate to their descriptions on the form. You can access the specific topic and procedures from the contents window on the left or click on the links under Related Topics.



The Client software has the ability to import CSV files from other databases, such as from a human resources database. This is especially beneficial if you have to create a large number of cardholder records. You can import the data to populate the fields, however, importing a CSV file requires some planning and setup.

Related Topics

- ▶ *Complete Cardholder Information and Access Levels*
- ▶ *Temporary Card Options*
- ▶ *Define Optional Fields*
- ▶ *Photo Capture*
- ▶ *Signature Capture*
- ▶ *Import Cardholder Data*
- ▶ *Photo Badges*

Complete Card Information and Access Levels

The Cardholder form serves to identify the cardholder, assign a card, and specify the door/elevator groups for site access.

Door Group Access Levels/Elevator Group Access Levels

You can assign a cardholder to 2 door groups and 2 elevator groups depending on the security requirements of the individual.

Display Access Level Summary

The Cardholder form has a Display Access Level Summary. Because you can assign a cardholder to 2 different door groups and 2 different elevator groups, you may wish to review what the access levels are for those groups. The Display Access Level Summary lets you view both the access levels for the assigned door groups and the assigned elevator groups as well as the hours of the time zones by clicking on the respective buttons.

Accessibility Feature

For cardholders with disabilities, you can use the Accessibility Feature if the Keyscan system has been connected to doors with door operators. When this individual's card is presented to a door, the reader acknowledges the card's disability status and invokes the Handicap Door Timer and Handicap Door Held Open Timer settings. These settings are specified in the Set Door and Reader Parameters form.

Previous/Next Buttons

The Previous and Next buttons on the Cardholder form allow you to scroll through cardholder records without having to return to the Search Access Cardholder Information form. When you select either button it moves back or forth by one record and retains the same tab setting - Group Access Levels, Temporary Card Options, Last Card Transactions, Optional Fields - whichever was the active tab.



When adding cardholder records, when you complete the record select the Next button. You are prompted to save the record, and can create the next record without having to continually exit the form to save time.

If your system uses either an HID reader/keypad (Keyscan part # HID-5355KP) or an Indala reader/keypad (Keyscan part # P XK501), please be aware of the following procedure. We recommend that when an individual is keying in their Personal Identification Number on one of the aforementioned reader/keypads, he or she press the star * key first, then enter their PIN code. Pressing the star key * clears any previous numbers that may still be stored in the reader/keypad. This procedure eliminates the potential of the keypad misreading a valid PIN entry and denying access.

Procedures

► *Steps to Complete Cardholder Information and Access Levels*

1. From the main screen, select the Card Holder Database quick button > Add New Card(s).
2. Click in the First Name text box and enter the cardholder's first name. The maximum is 30 characters.

3. Click in the Last Name text box and enter the cardholder's last name. The maximum is 30 characters.
4. Click in the Batch Number text box and enter the batch number of the card assigned to the cardholder. The batch number is the first three digits on the assigned card. The batch number may also be referred to as the site code or the facility code.
5. Click in the Card Number text box and enter the card number. The card number follows the hyphen after the batch number.
6. Click in the PIN Number text box. The system assigns a 5 digit Personal Identification Number. The cardholder would enter this number where a keypad is in use to gain access. You can either accept the system assigned number or enter your own number. If your access control system is not equipped with keypads leave the system assigned PIN number.
7. If you are assigning security levels for system users, click on the down arrow to the right of Security Levels and select a level. Assigning security levels is not recommended unless you are an advanced user and require stringent system administration security.
8. If applicable, use the Comments text box to enter any remarks or notes about the cardholder.
9. From Telephone Number to Bar Code, complete whichever fields are required.
10. If a cardholder has a disability, and if you have doors equipped with door operators that are connected to the access control system, click the Accessibility Feature button to set it ON. If your system is not connected to door operators for handicap accessibility, bypass this step.
11. Ensure the Group Access Levels tab is selected and click the down arrow on the right side of the Door Group Access Levels A. Select the appropriate door group from the drop down list. Repeat for the other door / elevator groups, if applicable.
12. If that completes the record, click on the Save & Exit button, or complete the other options before saving and exiting the record.

Temporary Card Options

You can make a card temporary such as for visitors or temporary staff etc. Temporary card usage can be restricted by the following parameters:

- a date range
- a limited number of uses
- a date range and a limited number of uses, whichever occurs first

Temporary cards expire 1 minute before midnight on their expiration date.

Procedures

► *Steps to Make a Card Temporary*

1. To make a card temporary, select the Temporary Card Options tab on the Cardholder form.
2. Click inside the Card Limited check box. A tick mark inside the box indicates the field is active.
3. If the card has a usage restriction, enter the maximum usage in the Card Limited to Number of Uses text box. If there is no usage restriction, leave the Card Limited to Number of Uses blank.
4. If the card is temporary based on a date range, click in the box to the left of Include Date Range Values. The box has a tick mark when active. If the temporary card is only valid on today's date, you do not have to set the calendar and can go to step 7 otherwise to set the date range, go to the next step.
5. Under Date Valid From, the current date is circled on the calendar. If the start date is other than the current day, select the correct start day, or click on the arrows at the top of the calendar to scroll to the desired month and year and select the day on the calendar.
6. Repeat the above step to complete the Date Valid To fields.
7. Complete the other relevant cardholder fields.
8. When you have completed the form, select Save & Exit.

Optional (Cardholder) Fields

The Optional (Cardholder) Fields are user-defined that you can use to list supplemental information. These fields are initially blank until you define them.

When you define the optional fields, you can specify 2 of those fields to be listed on the main Cardholder form by using the Display on First Card Tab function. If you elect to use the Display on First Card Tab function, the fields are inserted below the Email Address and the Bar Code fields. You can enter and view data in those 2 fields without having to select the Optional Fields tab. Otherwise, to enter or view optional fields data, select the Optional Fields tab.

From the Optional Fields form, you also have the ability to change the descriptions of any or all of the following fields:

- Telephone Number
- Telephone Extension
- Fax Number

- Email Address
- Card Location
- Parking Spot #
- Car Plate #
- Bar Code



By right clicking on the text box of any defined Optional Field headings, a list of all entries made in that field is viewable in a drop down box.

Procedures

►Steps to Define Optional Fields

1. From The Cardholder Information form, select the Optional Fields tab.
2. From the Optional Fields form, select the Cardholder – Optional Fields Setup button.
3. Click in the Optional Field Name # 1 text box on the right side of the Card Options Setup form and type a caption for that field.
4. Repeat for each subsequent field that you wish to define.
5. Click the down arrow to the right of Display on First Card Tab if you wish to have this field listed on the main cardholder form, and select the optional field.
6. To list a 2nd optional field on the main Cardholder form, click the down arrow to the right of the 2nd Display on First Card Tab, and select the optional field.
7. Click on the Save & Exit button.

Photo Capture

There are two methods to insert an image on the Cardholder form:

- from an existing image of the cardholder
- from a live video capture of the cardholder

You must have a video camera connected to your PC in order to capture a live video image of the cardholder.

Procedures

►Steps to Import an Existing Image

You must have existing images of cardholders to perform this procedure.

1. From the Cardholder Information form, click on the Capture Photo button.

2. From the Capture Card Photo form, click on the Import File button.
3. From the Select User Graphic File dialog box, navigate to the directory that contains the image file of the cardholder.
4. Select the image file.
5. Click on the Open button.
6. To re-frame the image, use the keys as instructed below the image on the left side of the Capture Card Photo form.
7. From the Capture Card Photo form, click on the Save & Exit button to import the file into the Cardholder form.
8. Be sure to click on the Save & Exit button on the Cardholder form to save the cardholder's photo with his or her record.

► *Steps to Capture a Live Video Image*

You must have a video camera with the proper interface connections to perform this task.

1. From the Cardholder Information form, click on the Capture Photo button.
2. From the Capture Card Photo form, click on the Acquire Image button.
3. With the Capture Still image form open, position the cardholder in front of the camera to obtain the desired image.
4. If the image is satisfactory, click on the Save & Exit button to import the image into the cardholder record, otherwise repeat to re-acquire a satisfactory image.
5. Click on the Save & Exit button on the General Card Holder Information form to save the cardholder's photo with his or her file.

Signature Capture

This requires an optional signature capture device.

Procedure

► *Steps to Capture a Signature*

1. Click on the Capture Signature button on the Cardholder form.
2. With the signature capture device's pen, have the cardholder sign his or her name on the glass face of the signature capture tablet. The signature is transferred to the Card Holder Signature box.
3. If the signature is not acceptable, click on the Clear Signature button and repeat the above steps. If the signature is acceptable, continue to complete

the remainder of the Cardholder form.

Create System Users

About System Users

System users are created in the System User Information form. A System User account prevents unauthorized persons from accessing the System VII software and regulates individual user privileges to protect the integrity of your access control system. Also, by creating system user accounts, the system log shows individual operator actions and data input for activity audits or investigations.

From within the System User Information form, you identify the individual, assign a unique User Name and Password for logging on and specify user authority levels.

The System User Information form is designed to give you broad flexibility. How you set individual user accounts will greatly depend on the nature of your organization and the levels of security required.



You may wish to review all the related topics listed below so you understand the conventions of system users before starting to setup accounts.

Procedure

► *Steps to Create a System User Account*

1. From the Main Screen, select System Settings > Add/Edit System Users.
 - To add a new system user to another site you must have Master Login Account status.
 - To add a new system user to the logged on site, you must have System Administrator or Master Login Account status.
2. From the Find System Users form, click on the Add New button to open the System User Information form.
3. In the User Name text box, enter a name the individual will use to log on. Generally, this is either the person's first initial and last name or first name and last initial. It must be unique to all other system users. The User Name is what the person enters in the Log On dialog box.
4. Enter the person's first name in the First Name text box.
5. Enter the person's last name in the Last Name text box.
6. Complete the fields from User Location to Email Address, whichever fields are applicable.
7. Enter a password in the Password text box. You may wish to consult with the system user for an appropriate password that can be easily recalled. Passwords are case sensitive. When logging on, the user must type his or her password exactly as it is entered on the System User Information form. The maximum is 10 characters.

8. Re-enter the password exactly as it was entered above in the Confirm Password text box.
 - When the system user logs on for the first time he or she will be prompted to confirm the password.
9. Click on the down arrow to the right of Language and select English from the drop down list.
10. Click the down arrow on the right side of Site Name. From the drop down list, select the site the system user is authorized to access. A Master Login account can select all sites; a System Administrator can only select the currently logged on site.
11. If you are assigning security levels, click on the down arrow to the right of Security Levels and select a level. Implementing security levels is not recommended unless you are an advanced user and require stringent system administration security.
12. If the system user is to have Master Login Account status, click in the box to the left to activate this field.
13. If the system user is to have System Administrator status, click in the box to activate this field. The box has a tick mark when active.
 - For individuals deemed solely as System Users, leave the System Administrator and Master Login Account designations inactive.
14. If the person is to have Enable Viewing of All Sites Transactions privileges, click in the box to the left to activate this field. Enabling this field allows the individual to view Alarm Events and Online Transactions for all sites. The System User must have a Master Login Account designation and have the Enter Online Transaction Modes switch enabled in the User Authority Levels panel to use this function.
15. Under the User Authority Levels, activate the appropriate fields for the system user by clicking inside the field's box, or select one of the radio buttons:
 - Authority Level 1 – enables most view functions
 - Authority Level 2 – enables most view and edit functions
 - Authority Level 3 – enables most view, edit, and add functions
 - Select All – enables all functions
 - De-select All – use to clear all currently selected User Authority Levels functions
 - For individuals who are only monitoring the system, such as security guards, you may wish to leave the Exit Software (Quit) field inactive so the System VII Client cannot be closed.
16. Select the Save & Exit button.

17. To create another system user, click on the Add New button and repeat the procedures or click on the Exit button in the Find System Users form to return to the main screen.

Related Topics

- ▶ *System User Account Types*
- ▶ *User Authority Levels*
- ▶ *Security Levels*
- ▶ *Example of System Users - Single Site*
- ▶ *Example of System Users - Multiple Sites*

System User Account Types

It is important to understand the conventions and types when creating system user accounts. Each individual who has an account to access the System VII software is considered a system user. There is, however, three system user designations. The following highlights the functional differences between those three designations.

System User Account Types & Privileges

Master Log In Account	System Administrator	System User
Create new sites	Display/Clear/Delete/Export system log events	Excluded from the Master Login Account and System Administrator rights
Delete sites	Display/Search/Print PIN card numbers	
Add system users to any site	Reset user passwords	
Purge Transactions	Add system users to the current site	
Re-index Database	Import Cards (CSV files)	
Compress Database	Clear All Alarms	



A system user can have one, both, or neither Master Login Account and System Administrator designations depending on the desired range of functionality.

You must have 1 system user that has a Master Login Account designation for every site you create. This can be the same person or several persons depending on the structure of your organization.

On a multiple site configuration, only a system user with a Master Login Account designation can create or copy system user accounts to a remote site.

User Authority Levels

After determining the individual's System User designation, you further define the individual's range of operability by enabling or disabling specific program functions in the User Authority Levels panel on the right side of the form.

User authority levels, in many cases, are divided into three states:

- Add – the user has permission to add a new record to the database
- Modify – the user has permission to modify an existing record in the database
- View – the user only has permission to view a record in the database

In cases where you designate an individual as either Master Login Account or System Administrator or both, you must activate the corresponding functions in the User Authority Levels panel as shown in the table plus any other desired system functions.

	Master Log In	System Administrator	System User
User Authority Levels	Add Site View Site Edit Site Delete Site Add/Edit System Users	View Cards Add/Edit System Users Perform Printing Tasks	Discretionary

Security Levels

The Security Level feature on the System User information form has been developed for advanced users that require more rigorous system administration security controls.



Keyscan suggests that this function only be used in cases where your organization requires an exceptionally high level of system administrator security.

Security Levels, in essence, prevent any system user assigned with a lower number from viewing or altering any system user account with a higher security

ranking. The security levels are from 1 to 10.

- 1 = lowest security level
- 10 = highest security level

A system user with a lower security level is excluded from viewing, editing, or deleting cardholder information, group names, time zones, and group access levels associated with or assigned to any system user with a higher security level.

A system user account must have one of the following settings enabled to access and assign security levels:

- Master Login Account – can set security levels from 1 to 10
- System Administrator – can set security levels equal to or lower than his or her account

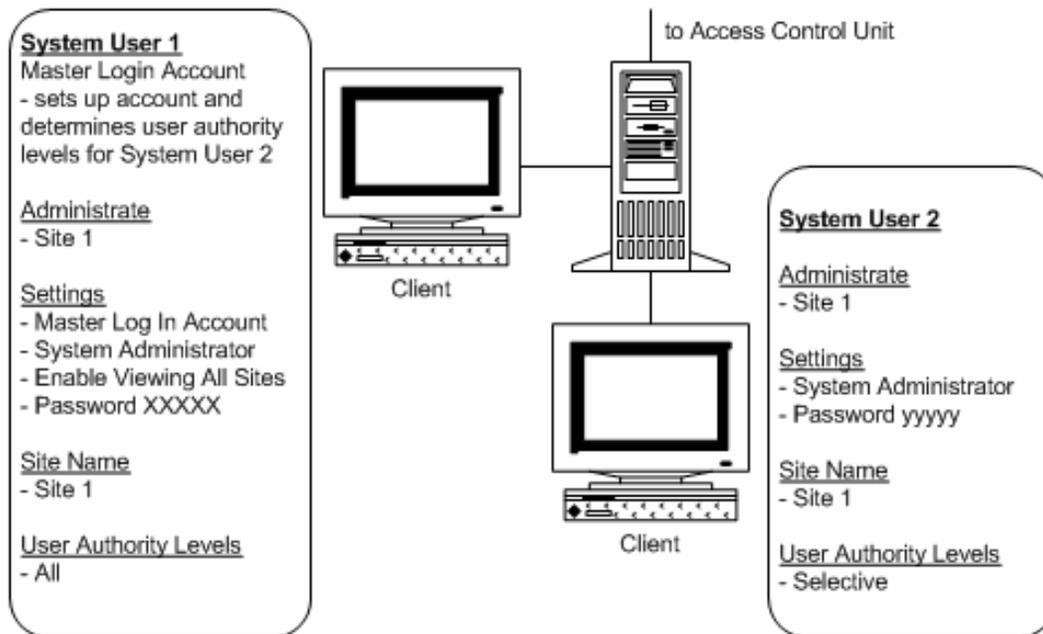
The Security Levels function is unavailable to system users not assigned either Master Login Account or System Administrator.

Example of Single Site with Multiple Users

In this example of a single site setup, System User 1 has System Administrator and Master Login Account designations. This person is responsible for operating and maintaining the entire access control system.

System User 2, in this example, is a Human Resources administrator and has to add, edit, or delete cardholder records, review log events and have the option to add another system user. In this case System User 1 would activate the System Administrator option and set the corresponding User Authority Levels for System User 2.

Single Site with 1 Master Login Account System User and 1 System Administrator User

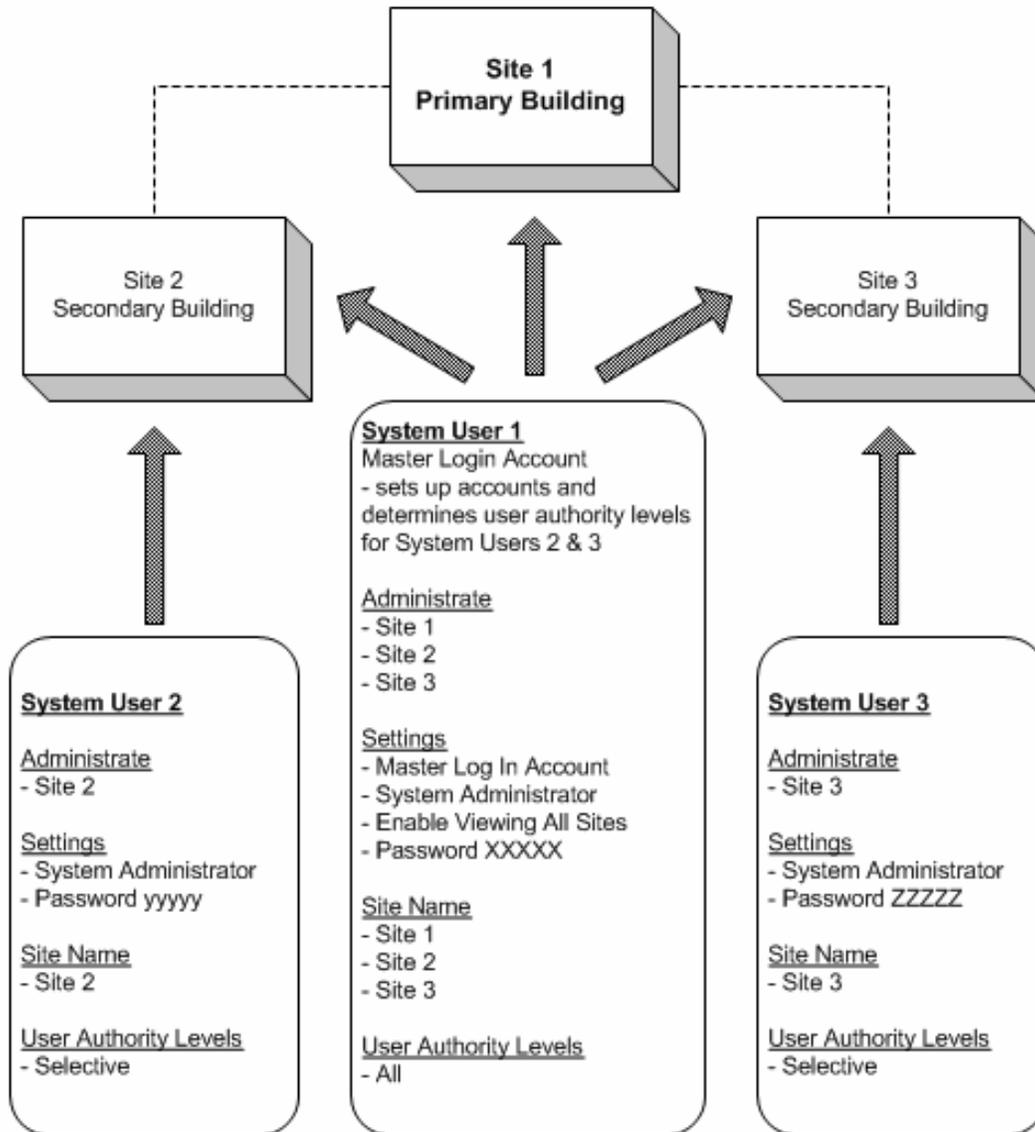


Example of System Users - Multiple Sites

In this example of a three-site setup, System User 1, who is located at Site 1, is responsible for operating and maintaining the entire access control system at all three sites. This person would have System Administrator and Master Login Account designations. To have access to all sites, System User 1 must be entered as a system user on all three sites.

System User 2 and System User 3 each work at their respective locations and only need to access the database for their specific site. In this example, System User 1 would activate the System Administrator option and enable the required User Authority Levels for System User 2 at Site 2 and System User 3 at Site 3.

Master Log In Account vs. System Administrator for Multiple Sites



Email Alarm Notification

Setup Email for Alarm Notification

The System VII Client allows you the option of sending an alarm notification to an email address using the Email Setup. You can specify the types of alarm events for specific doors (readers), or inputs, or outputs. When an alarm is triggered, the System VII software transmits the alarm notice to the recipient email address.

You can also send email notifications based on individual cardholder transactions by enabling the Email with Cardholder Selection function. This feature was primarily designed to notify an email recipient that a cardholder had arrived or entered the premises by selecting access granted for a specific door.

SMTP Email Setup

To have the System VII software send email alarm notifications, you must configure the SMTP Email Settings form so that the email alarm notifications are routed through a mail server or exchange server. SMTP Email Settings must be performed by the IT department, since settings are based on established mail server protocols. SMTP Email Settings are reviewed in Site Setup. If your IT department has already set this up, continue to the procedures below.



The setup for Email Alarm Notification is different for systems that have CCTV than the procedures described here. If your system has CCTV, click on the CCTV link below for setting up Email Alarm Notification.

Command Line Option

This option instructs the System VII software to shell out to another application.

Load Active Map on Alarm Event

Opens a map on an alarm event if you have created maps with device assignments in the System VII Photo Badge Template Editor and you have loaded those maps in the Set Alarm Response Instructions & Alarm Graphic Locations form.

Procedures

► *Steps to Setup Email Alarm Notification (Non CCTV Systems)*

1. From the main screen, select the System Settings menu > Email Setup
2. From the Email Setup form, click on the down arrow to the right of Unit ID and select the appropriate access control unit.
3. In the table that lists the # | Device Type | Device Name, double click on the name of the Door, Input, or Output.

4. In the Transaction Type panel, click in the box to the left of the alarm event. You may choose multiple alarm events.
5. Type the recipient's address in the Email Address text box.
6. If applicable, enter the appropriate text in the Command Line Option field to have the System Vllshell out to that application.
7. If applicable, click on the down arrow to the right of Load Active Map on Alarm Event and select the desired map form the list. If you did not load maps in the Alarm Response Instructions & Alarm Graphic Locations form, the drop down list will be empty.
8. Click on the Update Email Settings button.
9. To add another device to the Email Alarm Notification, repeat steps 2 to 8, or click on the Exit button to return to the main screen.

► *Steps to Setup Email with Cardholder Selection*

Generally, this function is used with access granted to notify the email recipient that a cardholder has arrived or entered the premises. After the cardholder has presented his or her card at the reader, the system would automatically issue an email message with Keyscan Message as the subject and the following data:

- Transaction Type
 - Unit ID
 - Site ID
 - Device Name
 - Card Batch (#)
 - Card Number
 - Cardholder Name
 - Alarm Date Time
1. From the Email Setup form, click on the down arrow to the right of Unit ID and select the appropriate access control unit.
 2. In the table that lists the # | Device Type | Device Name, double click on the name of the Door.
 3. In the Transaction Type panel, click in the box to the left of the Access Granted, or the desired field. You may choose multiple events.
 4. Click in the box to the left of Email with Cardholder Selection.
 5. If you have cardholder records with photos and the recipient's receiving device is capable of displaying photos, click in the box to the left of Email with Cardholder Pictures if you wish to send the cardholder's photo with the email.

6. Click on the Show Email Settings for Cardholder Selection button.
7. Type the recipient's address in the Email Address text box.
8. Type the cardholder's card batch number in the Batch field. (The 3 digit number.)
9. Type the cardholder's card number in the Card Number box.
 - You can enter 5 additional Email addresses with the same card number or five different cardholders.
10. Click on the Update Email Settings button.
11. To return to the main screen, click on the Exit button.

Related Topic

 **CCTV**

Setup Database Backup

Schedule Automatic Database Backups

It is extremely important to make backup copies to the System VII database. You can program the System VII software to make backup copies of the database at regularly scheduled intervals. The PCs with the Communication Manager or Service and the Keyscan System VII database must be running at the time the backup occurs. The Clients do not have to be open during the backup.

In addition to performing scheduled backups at regular intervals, we strongly recommend that you copy your backup database files to another medium such as a writable CD or another network location.

Default Database Backup Folder

We recommend that you backup the System VII database to the location as listed depending on whether the System VII software modules were installed on a single PC or multiple PCs.

Single PC Installation

By default, the software creates a database backup folder in the following location:

- Program Files\Keyscan7\Backup

Multiple PC Installation

On a multiple PC setup where the database was installed on a separate PC from any of the Clients, by default the System VII software creates the database backup folder on the PC with the database in the following location:

- Program Files\Keyscan7\Backup

On a multiple PC installation you may require the assistance of the IT department to specify a valid path and network permissions.

Email Notification

As an option, you can specify an Email address to notify a recipient that the System VII access control database was backed up on the scheduled date. The email also advises if any errors occurred.



On a multiple PC installation, when you specify the backup folder location from the Client, it must be the folder location on the PC with the database module. You only have to perform the backup procedure once from any Client.

Procedures

► *Schedule Backups of the Database*

1. From the Client main screen, select System Settings > Database

Maintenance.

2. From the Database Setup form, click on the Database Backup button.
3. Do one of the following steps:
 - If the Database module and the Client are on different PCs, click on the Browse button, navigate to the PC with the Database > Program Files > Keyscan System VII > Backup.
 - If the Database module and the Client are on the same PC, click on the Browse button and navigate to Program Files > Keyscan System VII > Backup.
4. In the File Name text box, enter Keyscan. The file extension defaults to .ksd.
5. Click on the Save button.
6. If you wish to notify a recipient each time a scheduled backup occurs, complete the Email Address text box.
7. Under Backup Schedule, in the Backup Time box, select the 00 representing hours. Use the up or down arrows to set the hours. Then select the 00 representing the minutes. Use the up or down arrows to set the minutes. Select a time when there is nominal site activity.
8. In the Select the Day(s) of the Week, click in the boxes of the days when the database is backed up. Each successive time the database is backed up, the System VII software creates a new file with a date stamp.
9. In the Delete backup older than # of days, use the up or down arrows to set the system to automatically delete older backup files. We recommend not deleting backup files that are less than 28 days old.
10. Click on the Save Schedule button.
11. From the Save Schedule confirmation box, click on the OK button.
12. After saving the schedule, you can backup the database immediately (recommended). Click on the Backup Now button.
13. Click on the OK button in the Backup Completed confirmation box.
14. Click on the Exit buttons to return to the main screen.

Database Location

The Database Location form must specify either the IP address or computer name for a single PC setup or specify the IP address of the PC where the database was installed on a network setup. When you open the Client for the first time, the Database Location form opens and prompts you for the location of the database.

If at any time the database is moved on a network and the IP address changes

from the current address, you must update the Database Location with the revised IP address so the Keyscan Client can communicate with the database. If more than one Keyscan Client application has been installed on the network, you must update the Database Location form for each Keyscan Client.

Setup Communication Service

Communication Service Setup

As an option, the Communication Manager can be configured to run as a service. We do not recommend this unless you are running the Communication Manager from a server which is inaccessible to end-users. Please consult with the IT department for assistance. You must have Administrator status to perform the configuration procedures.

Preliminary

To setup the Communication Service, you must know the Window's User ID and Password to log on to the PC and specify whether communication is local or over the network. Follow the appropriate procedures to set up the Communication Service, either for a Local / Workgroup or on a Network / Domain. After you have setup the Communication Service, follow the steps in Verify Communication Service Setup to ensure the correct settings are in place.

Important

If you have already installed and configured the Communications Manager as outlined in the System VII Software Installation Guide, be sure to disable Auto Start Communication Manager before starting the procedures below.

Procedures - Local / Workgroup

▶ Setup the Keyscan System VII Communication Service

1. From Windows, select **start** > Run and select the Browse button.
2. Navigate to the Program Files folder > Keyscan 7 folder.
3. Double click on Keyscan7Comm.exe.
4. In the Open field text box from within the Run dialog box, insert the cursor to the far right following the closing quotation mark (").
5. Press the Space bar to insert a single space following the quotation mark (").
6. Enter a forward slash / followed by INSTALL in upper case as shown in the example - "C:\Program Files \Keyscan7\Keyscan7Comm.exe" /INSTALL
7. Select the OK button.
8. From the Keyscan System VII Communication Service Setup dialog box, enter your Window's user name in the Service Login text box.
9. Enter your Window's password in the Service Password text box. Passwords are case sensitive.
10. Click In the box to the left of Local User Account to enable this option.

11. Click on the OK button.
12. Select Start > All Programs > Keyscan System VII > Keyscan System VII Settings.
13. From the Keyscan Language Selection dialog box, click on OK.
14. From the Keyscan Settings form, select the Communication Service Setup button.
15. From the Communication Service Setup dialog box, enter your user name in the Service User ID (Main) text box. This is the user name assigned in the Keyscan System User Information form. You can also use the default user name KEYSKAN.
16. In the Service Site ID text box, enter the name of your site exactly as specified in Site ID on the Site Information form.
17. Click on the Save Settings button.
18. From the Keyscan Settings form, select the Save Settings button.

Note

To uninstall the Communication Service enter a forward slash / followed by REMOVE as shown in the example - "C:\Program Files \Keyscan7\Keyscan7Comm.exe" /REMOVE

Procedures - Network/Domain

► Setup Keyscan System VII Communication Service - Network

1. From Windows, select **start** > Run and select the Browse button.
2. Navigate to the Program Files folder > Keyscan 7 folder.
3. Double click on Keyscan7Comm.exe.
4. In the Open field text box from within the Run dialog box, insert the cursor to the far right following the closing quotation mark (").
5. Press the Space bar to insert a single space following the quotation mark (").
6. Enter a forward slash / followed by INSTALL in upper case as shown in the example - "C:\Program Files \Keyscan7\Keyscan7Comm.exe" /INSTALL.
7. Select the OK button.
8. From the Keyscan System VII Communication Service Setup dialog box, enter your Window's user name in the Service Login text box. (Power User or Administrator required.)
9. Enter your Window's password in the Service Password text box.

10. In the Service Domain field, enter the network domain of the PC.
11. Click on the OK button.
12. Select Start > All Programs > Keyscan System VII > Keyscan System VII Settings.
13. From the Keyscan Language Selection dialog box, click on OK.
14. From the Keyscan Settings form, select the Communication Service Setup button.
15. From the Communication Service Setup dialog box, enter your user name in the Service User ID (Main) text box. This is the user name assigned in the Keyscan System User Information form. You can also use the default user name KEYSKAN.
16. In the Service Site ID text box, enter the name of your site exactly as specified in the Site ID field in the Site Information form.
17. Click on the Save Settings button.
18. From the Keyscan Settings form, select the Save Settings button.

Note

To uninstall the Communication Service, enter a forward slash / followed by REMOVE as shown in the example - C:\Program Files \Keyscan7\Keyscan7Comm.exe" /REMOVE

Communication Service Verification

► *Verify Communication Service Setup*

1. Select Start > Control Panel > Administrative Tools.
2. From the Administrative Tools window, select Services.
3. From the Services window, scroll down and double click on Keyscan Service Comms.
4. From the Keyscan Service Comms Properties window, ensure that Automatic is selected as the Startup Type. If Startup Type is not on Automatic, click on the down arrow to the right and select Automatic from the list.
5. Ensure that Started is displayed to the right of Service Status. The Start button is dimmed. If Service Status is Stopped, select the Start button.
6. Select the Log On tab to verify the local or domain setting
 - local\workgroup - .user
 - network - domain\user (requires power user or admin)

7. If you made any changes, click on the OK button to exit. If you did not change any settings, click on the Cancel button to exit.

Upload Access Control Units

Uploading the Access Control Panels

After you have entered the information for your site, the final step is to upload the data to the access control units. On the System VII main screen, the Panel Upload quick button flashes a red message Update Changes anytime data has changed and the panels require an update.



If it is necessary to abort uploading the panels, press the Esc key to terminate the procedure. This may take several seconds. At the moment when the Esc key is pressed, the Communication Service continues uploading data from the current field until that field is completely uploaded to maintain continuity between the database and the ACU(s). The Panel Upload form updates itself and lists the fields that still must be uploaded to the ACU(s).

Pressing F4 after a specific access control unit has been selected in the Unit Selection box pulls up a message window that lists the panel serial number and the panel model.

Procedures

► *Steps to Upload the Access Control Units*

1. From the main screen, select the Quick Buttons menu > Update Changes (opens the Panel Updates form).
2. Click on the down arrow of Unit Selection and select the access control unit. If more than one ACU is to be uploaded, select All Units.
3. Click on the Select All button.
 - Items that have changed since the last time the ACUs were uploaded are listed in red and pre-selected. Below the Upload Type window, a status caption informs you how many items require uploading.
4. Select the Upload button. Wait for the panels to be updated.
5. Select the Exit button.

Operate the System

Alarms

Alarm Monitoring

Near the bottom of the Client main screen is the Alarm Monitoring panel. When alarms are tripped, the Alarm Monitoring panel lists specific criteria to inform you where and when alarms occurred as outlined below:

- Site ID – identifies the site location of the alarm
- Unit ID – identifies the access control unit that registered the alarm
- Alarm Type – identifies the state of the alarm at the source - Alarm Tripped, Alarm Cleared, Comms Failure, Unit Marked Inactive
- Device Type – Door, Input, Output, or ACU
- Device Name – Door (Reader Port Name), Input Name, Output Name, or Serial # (ACU)
- Date & Time – lists the Month/Day/Year/Time of the alarm
- Status
 - New - the alarm has not been cleared
 - Hold - the alarm is pending for further investigation

Procedures

To close Alarm Monitoring, select the X (close) button in the upper right corner of the window. If you close the window, you should have Alarm Notification enabled in the Utilities menu so the system still advises you of any alarm conditions.

To open the Alarm Monitoring window either press the F8 key (the System VII main screen has to be the active window on the desktop) or from the main screen, select the Quick Buttons menu > Restore Alarm Monitoring Window.

To access Alarm Instructions, double click on the specific event in the Alarm Monitoring panel to view the Alarm Response Instructions form.

Related Topics

▶ *Alarm Response Instructions*

▶ *Set Alarm Notification*

Alarm Response Instructions

The Alarm Response Comments form lists emergency instructions and the names of persons to contact. In addition, this form has text boxes for alarm comments and is used to place an alarm event on hold or clear it from the Alarm Monitoring panel. If the access control system is interfaced with CCTV, the form can call up images captured by the cameras if the cameras were programmed to respond on an alarm condition.

You must have completed the Set Alarm Response Instructions/Alarm Graphic Locations form for system controlled doors and/or devices.



When an alarm is completed and cleared from the Alarm Monitoring panel on the main screen, the record of the alarm is still retained in the database and can be viewed in the Alarm Listings form. For more information, see Alarm Listings.

Procedures

▶ Alarm Response Comments Form Overview

- At the top of the Alarm Response Instructions & Map Locations form, the Alarm Type, Input Type, Input Name, Alarm Date, Site ID, and Unit ID lists the alarm event details.
- The system user has the option to record who was contacted in the Person Contacted text box.
- The system user can also enter comments pertaining to the alarm in the Alarm Response Comments text box.
- Activating the Alarm Completed option clears the alarm listing from the Alarm window on the main screen. This action does not delete the alarm record from the database.
- Activating the Alarm on Hold option changes the status of the alarm event from New to Hold. Generally this is selected if the alarm is to be investigated. Putting the alarm on hold keeps the alarm listed in the Alarm Monitoring window. It cannot be removed until its status is changed to Alarm Completed.
- The information listed in the Response Location and Response Instructions panels is entered in the Set Alarm Response Instructions and Alarm Graphics Locations form accessed from the Door Maintenance menu.
- If there are persons to contact, they are listed in either:
 - the Response Alarm Contacts panel
 - the Response Emergency Contacts panel.
 - The names in these two panels - Response Alarm Contacts and Response Emergency Contacts are entered in the Site Contact Information form accessed from the System Settings menu > Site Setup.
- Click on the Show Map button if a site map was loaded in the Set Alarm Response Instructions and Alarm Graphics Locations form.
- If the system has CCTV and is set to capture still images on specific alarm event types, the user can view those images by clicking on the Display CCTV Alarm Picture(s).
- To print a copy of the Alarm Response Instructions/Map Locations form, click on the Print box.
- To save the entries made in the Alarm Response Comments form, click on the Save & Exit button. This retains those entries when the alarm listing is viewed at a later date.

- If no information was entered or no switches were set, click on the Exit button to return to the main screen.

► *Acknowledge and Remove an Alarm from the Alarm Monitoring Panel*

1. From the Alarm Monitoring window, double click on the alarm event.
2. At the top of the Alarm Response Instructions & Map Locations form, the Alarm Type, Input Type, Input Name, Alarm Date, Site ID, and Unit ID are listed.
3. Click in the box to the left of Alarm Completed. This acknowledges that a system user has seen the alarm and clears the listing from the Alarm Monitoring window on the main screen. Clearing the alarm listing from the Alarm Monitoring window does not delete the alarm record from the database.
4. Click on the Save & Exit button to return to the main screen.

► *Put an Alarm on Hold*

1. From the Alarm Monitoring window, double click on the alarm event.
2. At the top of the Alarm Response Instructions & Map Locations form, the Alarm Type, Input Type, Input Name, Alarm Date, Site ID, and Unit ID are listed.
3. Click in the box to the left of Alarm on Hold. Activating the Alarm on Hold option changes the status of the alarm event from New to Hold. Generally this is selected if the alarm is to be investigated. Putting the alarm on hold keeps the alarm listed in the Alarm Monitoring window. It cannot be removed from the Alarm Monitoring window until its status has been changed to Alarm Completed.
4. Click on the Save & Exit button to return to the main screen.

Related Topic

► *Set Alarm Response Instructions/Alarm Graphic Locations*

Alarm Listings

The Alarm Listings form is used to view new/pending alarms or search for alarms by a date range. The Alarm Listings form identifies alarms by the following criteria:

- Site Name – identifies the site location of the alarm
- Unit ID – identifies the access control unit that registered the alarm
- Alarm Type – identifies the state of the alarm at the source - Alarm Tripped, Alarm Cleared, Comms Failure, or Unit Marked Inactive
- Device Type – Door, Input, Output, or ACU

- Device Name – Door (Reader Port Name), Input Name, Output Name, ACU Serial #
- Date & Time – lists the Month/Day/Year/Time of the alarm
- Status – New or Hold



From the Alarm Listings form, you can also clear all new alarms from the Alarm Monitoring window.

Any alarms that were put on hold in the Alarm Response Comments form cannot be cleared until they are given an Alarm Completed status.

Procedures

▶ *Clear All New Alarms*

1. From the Client main screen, click on the Alarm Listings quick button.
2. From the Alarms Listing form, click in the box to the left of New or Pending Alarms in the Search Alarms panel, if it is not active.
3. The alarms listed on this form are the same as those listed on the main screen.
4. Click on the Clear All Alarms button at the bottom of the screen.
5. From the Client warning box – Do you wish to clear all alarms in the system?, click on the Yes button. All new alarms are removed from the Alarm Listings form and the Alarm Monitoring window.
6. Click on the Exit button to return to the main screen.

▶ *Viewing Alarms – New, On-hold, or By Date*

1. From the Client main screen, click on the Alarm Listings quick button.
2. By default, when the Alarms Listing form opens, the New or Pending Alarms option in the Search Alarms panel is selected. New or pending alarms are listed in the Alarm Events panel in the lower section of the form. To view alarms by a date range, click in the box to the left of Alarm by Date Range in the Search Alarms panel.
3. Click on the up or down arrow of the From box, to scroll back or forward to the desired month.
4. Select the day and click on the up or down arrow to scroll to the desired day.
5. Select the year and click on the up or down arrow to scroll to the desired year.
6. Repeat steps 3 - 5 for the To date.

7. To find specific alarms, either enter or select data in the appropriate search fields:
 - Device Name
 - Device Type
 - Alarm Type
 - Unit ID
 - Site Name
8. Click on the Search button.
9. To view an alarm record, double click on the alarm listing in the Alarm Events panel in the lower section of the form.
10. To perform another search, select new To and From dates and specify search criteria, then click on the Search button.
11. To clear the search results and reset the Alarm Events panel back to the current alarm listings, click in the New or Pending Alarms radio button.
12. Click on the Search button.
13. Click on the Exit button to close the Alarm Listings form and return to the main screen.

Alarm Warning

The system can be programmed to open an Alarm Warning dialog box whenever an alarm event is tripped. Alarm Warning dialog boxes open whether the Client is the active application on the desktop or it has been minimized. To activate the Alarm Warning dialog box feature, enable Alarm Notification in the Utilities menu. Click on the Alarm Notification link below for more information.

To clear the Alarm Warning dialog box, click on the OK button.

Related Topics

▶ *Alarm Monitoring*

▶ *Alarm Response Instructions*

▶ *Alarm Notification*

Alarm Types

The following list identifies the various types of alarms and the cause of the alarm in the System VII software.

Alarm	Device/Cause of Alarm
ACU Master Comms	Slave ECM CANBUS 2 communication failure with

Failure	master ECM
ACU Master Comms Restore	Slave ECM CANBUS 2 communication has been restored with master ECM
Alarm Cleared	Door - a door that was previously forced open has now been closed Auxiliary Input – a monitored auxiliary input point that was previously in an alarm condition has been cleared
Alarm Duress	A cardholder has keyed in *9 preceding their PIN code to indicate some type of problem or emergency
Alarm Tripped	Door – a monitored door was accessed without a valid card presentation (forced open) Auxiliary Input – a monitored auxiliary input point was tripped
Comms Failure	An access control unit has lost communication with the access control software
Comms Restored	An access control unit, previously marked as Unit Inactive, has had communications restored and is now active
Door Closed	A door previously in violation of the Door Held Open Time setting has now been closed
Door Held Open	A door was accessed with a valid card but was not closed within the designated Door Held Open Time setting
ECM/GCM Trouble	A CANBUS communication error
ECM/GCM Message Trouble	Communication on CANBUS interrupted because of heavy network traffic
Invalid Card/Keypad Code	An invalid card or PIN code has been presented at a reader or keypad more than 5 times
IO Comm Card Failure	IO to ACU communication failure
IO Comm Card Restore	IO to ACU communication has been restored
Power Fail Detect	An access control unit has lost power
Trouble Open	Indicates that a wire has been cut or is broken
Trouble Short	Indicates the wire has a short circuit
Unit Marked Inactive	ACU Model Type – an access control unit that lost communication has now been marked inactive by the access control system

Cardholders

Add a Cardholder

If you are adding a new cardholder to your database, click on the link below for information about the cardholder information form and the procedures.

Related Topic

▶ [Add a New Card](#)

Add a Block of Cards

The Add a Block of Cards form lets you quickly enter a group of cards in the Keyscan database for immediate use without having to enter names and other personal information for individual cardholders. This is a fast method to enter cards, however, the drawback is that you have no record to identify cardholders by name or the specific cards they received.



You can only use the Add a Block of Cards option if the cards have the same batch number and the card numbers are in sequence.

The Add a Block of Cards is accessed from the Quick Buttons menu > Card Holder Database > Search Access Card Holders > Add Block of Cards button at the bottom of the Search Access Card Holders form.

Procedures

▶ *Steps to Add a Block of Cards*

1. From the main screen, click on the Quick Button menu > Card Holder Database > Search Access Cardholders.
2. From the Search Access Cardholders form, select the Add Block of Cards button.
3. In the Starting Card Number text box, enter the first card number.
4. In the To text box, enter the last card number.
 - Based on the range of card numbers you entered above, the software calculates and enters the value in the Total Number of Cards To Be Added box when you move to step 5 or 6.
5. If you wish the system to Add Door Group A Description As Last Name, click in the box to the left. If this option is selected, the Name fields below are inactive.
6. If you did not use step 5, enter a Block Last Name and a Block First Name that gives a unique description to this block of cards. This provides a reference in case you have to archive or delete the block of cards at a later

date.

7. In the Batch Number text box, enter the batch number for all cards in this block. The batch number may also be referred to as the site code or facility code.
8. For Door Group Access Levels or Elevator Group Access Levels, click on the down arrow and select the appropriate doors or elevator groups.
9. If the block of cards is temporary, perform steps 10 to 13, otherwise leave the Temporary Card Options inactive, and proceed to step 14.
10. Click inside the Card Limited check box. A tick mark inside the box indicates the field is active.
11. If the cards have a usage restriction, enter the maximum card usage in the Card Limited to Number of Uses text box. If there is no restriction, leave the Card Limited to Number of Uses blank.
12. Under Date Valid From, the current date is displayed in the window and pre-selected. If the Date Valid From is other than the current date, click on the down arrow to the right. Use the arrows to scroll to the desired month and year. Select the day on the calendar.
13. Repeat the above step to complete the Date Valid To fields.
14. Click on the Save & Exit button.
15. From the Batch Card Holder warning box, select the Yes button.
16. To verify the cards have been entered, click on the Find All Cards button on the Search Access Card Holders form to list the cards.
17. Click on the Exit button to return to the main screen.

Card Enrollment Feature

The Card Enrollment Feature is a convenient method using the Online Transaction window to determine a card number where one of the following circumstances applies:

- For an unknown card format, usually with more than 5 digits, in which the system re-creates a new card number compatible with Keyscan
- As above, except that a large number of cards have to be enrolled
- Where the number has worn off and is no longer visible on the card

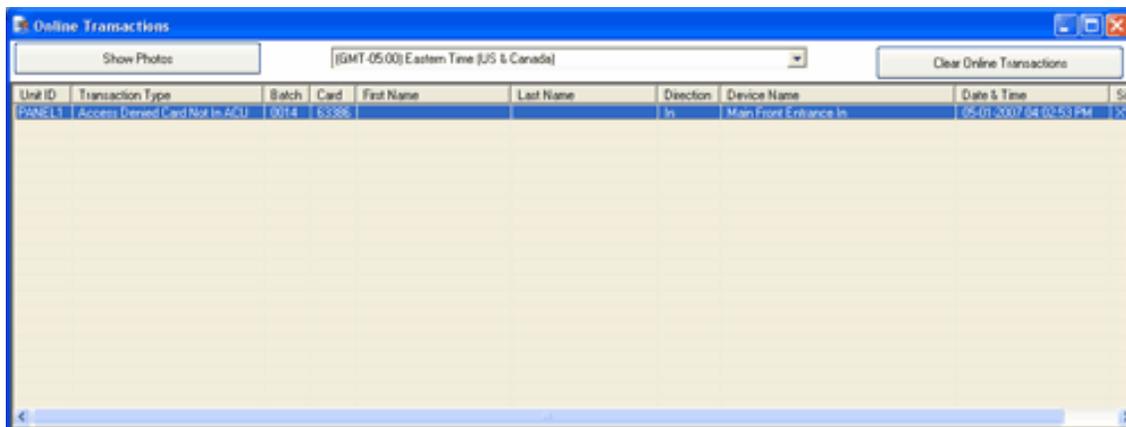
The Card Enrollment requires the use of a reader.

Procedure

►Steps to Use the Card Enrollment Method

1. From the Client main screen, select the Display Online Transactions quick button.
2. Present the card at a conveniently located reader.
3. In the Display Online Transactions window, the card is listed as Accessed Denied Card Not In ACU.
4. Hold down the Ctrl key and double click on the card number in the Display Online Transactions window.
5. The Cardholder Information form opens with the batch number and card number inserted in the two respective fields.
6. Complete the relevant cardholder fields.
7. Click on the Save & Exit button when you have completed entering the cardholder's information.

Online Transactions window after Card Scanned at Reader



Searching for Cardholders

The Search Access Card Holders form acts a central hub to access cardholder records and conduct user defined searches to perform cardholder record maintenance.



You may use multiple fields to conduct your cardholder record search.

In text boxes, you can enter the full name or number or a segment of the alpha or numeric characters. As an example, if you wanted to list all cardholders whose last name has the letter M, type M in the Last Name field.

Wild Cards

When performing a cardholder search using the First Name or Last Name fields,

please note the use of the (^) caret and (~) tilde characters as wild cards.

- ^S - lists all names that start with the letter S. Without the ^ caret, the search would list all names that have a letter S anywhere in the name. You can use single or multiple characters. As an example, ^Sta would list all the names that start with those 3 letters.

- ~S - lists all the names that end with the letter S. Without the ~ tilde, the search would list all names that have a letter S anywhere in the name. You can use single or multiple characters. As an example, ~ny would list all names that end with those 2 letters.

Procedures

► *Explanation of Search Access Cardholder Fields*

Menus

Import and Export Cardholder Information

Import Cardholder Information – opens the form to import a CSV file to create or update cardholder records

Export Cardholder Information – opens the form to export , as a CSV file, cardholder records that are listed in the table based on search criteria

Reports

Cardholder - Reader Access Level Reports – lists access levels at selected doors for each cardholder listed in the table based on search criteria for either the current site or all sites

Reader Access Level Reports – lists door group access levels at selected doors with the option of including a listing of cardholders in the in the door group

Deleted Cardholder Report – lists cardholders whose records have been deleted from the database

Update Cardholder Security Level – allows changing the security level of selected cardholders in the table to prevent a system administrator with a lower security level from altering a card record assigned a higher security level

Utilities

Reset Anti-passback – allows resetting anti-passback for selected card records in the table or resets anti-passback for all cardholders

Search for Records

General Cardholder Information Fields

Use one or multiple fields to find card records from the General Cardholder Information fields.

Additional Cardholder Information Tab

Use one or multiple fields to find card records from the Additional Cardholder Information fields.

Optional Cardholder Information Tab

Use one or multiple fields to find card records from the Optional Cardholder Information fields.

Not Used Since

Use to find cards that have not been active since the specified date.

Sort By Field

The Sort By Field option allows you to specify the order of how cardholder records are sorted in the cardholder record window.

- Alphabetical Fields A – Z
- Numerical Fields 0 – 9

Find Cards

Clicking on the Find Cards button displays cardholder records based on the specified search criteria.

Find All Cards

Clicking on the Find All Cards button displays all cardholder records in the cardholder database. The Find All Cards button ignores any search criteria.

Clear Find

Clicking on the Clear Find button clears all cardholder records from the cardholder record window.

New Card

Opens the Cardholder record form to create a new record.

Add a Block of Cards

Opens the Add Cardholders – Block form to quick load a group of cards which must have the same batch code (facility code) and sequential card numbers.

Delete Cards

Selected cards are deleted from the system.

Archive Cards

Selected card records are retained in the database, however, cards are de-activated and cannot access system controlled doors until the archive status is

cancelled.

Print Listing

Lists the card records displayed in the table which can be printed from the Keyscan System VII Report Previewer.

Print Photo Badge

Opens the Print Photo Badge form to print badges for selected card records in the table.

Copy Card to Another Site

Opens the Site Selection form and copies selected card record to specified site(s).

► Perform a Search for Specific Cardholder Records

1. From the main screen, select the Quick Buttons menu > Card Holder Database > Search Access Card Holders.
2. In the appropriate field, enter the criteria to search for the cardholder record(s), by either:
 - Typing the criteria in the text box.
 - Clicking on the down arrow and selecting the criteria from the drop down list.
 - You may use multiple fields to conduct your cardholder record search.
 - In text boxes, you can enter the full name or number or a segment of the alpha or numeric characters. As an example, if you wanted to list all cardholders whose last name has the letter M, type M in the Last Name field.
3. Click on the down arrow under Card Type and select the appropriate option:
 - All Cards
 - Temporary Cards
 - Exclude Archived and Temp Cards
 - Archived Cards
 - Non-archived and Temp cards
4. If you wish to display cards Not Used Since, click on the down arrow to the right and specify the date. At the top of the calendar, click on the arrows to scroll back or forward to the month and year. Click on the day in the body of the calendar. The calendar then closes with the date now selected. The check mark in the box to the left indicates this search criteria is active.
5. Click on the down arrow to the right of Sort By Field and select an option from the drop down list to specify how the cards are listed in the cardholder records window.

6. Click on the Find Cards button. The results of your search are listed in the cardholder records window.
7. To clear the cardholder records window and perform another search, click on the Clear Find button.

Edit/Delete Cardholders

When you select the Edit/Delete Card(s) option, you can edit individual cardholder records or delete individual or multiple cardholder records from the database.

When you select the Edit/Delete Card(s) option, the Search Access Card Holders form opens first. This form acts as the hub to perform most cardholder tasks. Select the cardholder record(s) you are either editing or deleting. You can either scroll through all cardholder records or use search criteria to locate specific cardholder records.



Before you can edit or delete a cardholder, you must either select the Find All Cards button to list all cardholder records or specify search criteria and select the Find Cards button to list cardholder records in the lower section of the Search Access Card Holder form. When this form opens no records are listed until you initiate one of the previously mentioned steps. If you are not sure how to perform a cardholder search, click on the link above.

The Edit/Delete Card(s) option is accessed from the Quick Buttons menu > Card Holder Database or from the Card Holder Database quick button on the main screen.

Procedures

▶ *Edit a Cardholder Record*

1. Select the Find All Cards button or enter cardholder data in one of the appropriate fields and select the Find Cards button.
2. Double click on the cardholder record in the lower section of the Search Access Card Holders form where the records are listed.
3. Edit the necessary fields from within the Cardholder Information form.
4. Click on the Save & Exit button.
5. Click on the Exit button in the Search Access Card Holder form to return to the main screen.

▶ *Delete a Cardholder Record*

1. Select the Find All Cards button or enter cardholder data in one of the appropriate fields and select the Find Cards button.

2. Select the cardholder record in the lower section of the Search Access Card Holders form where cardholder records are listed.
3. Click on the Delete Card(s) button.
4. Click the Yes button in the Delete Card Holder(s) warning box.
5. If applicable, click on the Yes button in the Delete Card(s) from Sites warning box. This removes the cardholder record from all sites the system administrator has authority to see. If you are only deleting the record from the current site, click on the No button.
6. Click on the Exit button in the Search Access Card Holder form to return to the main screen.

► *Delete Multiple Cardholder Records*

1. Select the Find All Cards button or enter cardholder data in an appropriate field and select the Find Cards button.
2. To delete multiple cardholder records, use one of the following techniques:
 - To delete consecutive cardholder records, select the first record in the group of records to be deleted. By default the first record listed in the cardholder records panel is pre-selected. While pressing down the Shift key, select the last record in the group to be deleted. All records between the first and last records are now selected.
 - To delete non-consecutive cardholder records, select the first record in the group of records to be deleted. While pressing down the Ctrl key, select the remaining records in the group to be deleted.
3. Click on the Delete Card(s) button.
4. Click the Yes button in the Delete Card Holder(s) warning box.
5. If applicable, click on the Yes button in the Delete Card(s) from Sites warning box. This removes the cardholder records from all sites the system administrator has authority to see. If you are only deleting the record from the current site, click on the No button.
6. Click on the Exit button in the Search Access Card Holder form to return to the main screen.

Archiving Cardholder Records

Archive a Card Holder is an option that can be used when you wish to maintain the cardholder record in the database but de-activate the card for an interim period of time. When Archive a Card Holder is switched on, the card issued to the cardholder is denied access to doors and elevators controlled by the Keyscan

system. A typical example might be when an employee is taking a leave of absence, or a club member is expected to renew their membership at a later date. To re-activate an archived cardholder, you turn the switch off.



You cannot re-activate multiple archived cardholders simultaneously. Archived cardholders must be re-activated individually from the Cardholder Information form.

Procedures

▶ Archive a Cardholder

1. From the main screen select the Quick Buttons menu > Card Holder Database > Search Access Card Holders.
2. Select the Find All Cards button or enter cardholder data in an appropriate field and select the Find Cards button.
3. Select the cardholder record in the lower section of the Search Access Card Holders form where cardholder records are listed.
4. Click on the Archive Card(s) button.
5. Click the Yes button in the Archive Card(s) warning box.
6. If applicable, click on the Yes button in the Archive Card(s) from Sites warning box. This archives the cardholder record in all sites the system administrator has authority to see. If you are only archiving the record in the current site, click on the No button.
7. Click on the Exit button in the Search Access Card Holder form to return to the main screen.

▶ Archive Multiple Cardholders

1. From the main screen select the Quick Buttons menu > Card Holder Database > Search Access Card Holders.
2. Select the Find All Cards button or enter cardholder data in an appropriate field and select the Find Cards button.
3. To archive multiple cardholder records, use one of the following techniques:
 - To archive consecutive cardholder records, select the first record in the group of records to be archived. By default the first record listed in the cardholder records panel is pre-selected. While pressing down the Shift key, select the last record in the group to be archived.
 - To archive non-consecutive cardholder records, select the first record in the group of records to be archived. While pressing down the Ctrl key, select the remaining records in the group to be archived.

4. Click on the Archive Card(s) button.
5. Click the Yes button in the Archive Card(s) warning box.
6. If applicable, click on the Yes button in the Archive Card(s) from Sites warning box. This archives the cardholder records in all sites the system administrator has authority to see. If you are only archiving records in the current site, click on the No button.
7. Click on the Exit button in the Search Access Card Holder form to return to the main screen.

Copy Card Records to Other Sites

In cases where you have existing cardholders who require access to more than one site, you can copy cardholder records to multiple sites.

When you copy a cardholder record from one site to another site, you must bear in mind that the software copies door and elevator group information based on the three digit number that precedes the group name.

Initially, when you created door and elevator groups, there was a three digit number, 001 to 511, that preceded the group name. When the cardholder record is copied to the new site, the software only copies the three digit number.

Example of 2 Sites with different Door Group Name/Number Assignments

Site A	Site B
001 Sales Department	001 Finance Department
002 Finance Department	002 Sales Department

As you can see In the above example, Sales Dept. cardholders at Site A would be in the Finance Dept door group at Site B. You would have to edit the record to assign the cardholder to the correct door or elevator group.

To copy multiple cardholder records to another site, we recommend exporting the card records, edit the records in a spreadsheet, and then import them to the other site.

Procedure

► Steps to Copy Existing Cardholders to Multiple Sites

1. Select the Quick Buttons menu > Card Holder Database > Search Access Card Holders.
2. Select the Find All Cards button or enter cardholder data in an appropriate field and select the Find Cards button.
3. Locate and select the cardholder record in the cardholder records window of the Search Access Card Holders form.
4. Click on the Copy Card to Another Site button.

5. From the Site Selection box, click in the box to the left of the Site Name to select the site where the records are copied. The Found in Site field indicates whether the cardholder record is currently copied (Yes) or not copied (No) in the listed sites.
6. Click on the OK button in the Site Selection box.
7. Click on the Exit button in the Search Access Card Holder form to return to the main screen.

Related Topic

▶ *Import Export Cardholder Information*

Replace Lost or Stolen Card

In the event a card is lost or stolen, issue a new card, enter the new card number in the cardholder's record, and save the record. The old card number is deleted from the system and is no longer valid if someone tries using the card to gain access. If the card is returned at a later date, it can be re-assigned to another cardholder.



If you have the Disable Auto Updates function engaged on the Site Information form, you will have to manually upload the panels to affect the change otherwise the lost or stolen card will still be active.

Procedure

▶ *Assign a New Card to an Existing Cardholder*

1. From the main screen, select the Quick Buttons menu > Card Holder Database > Search Access Card Holders.
2. Enter the cardholder's first and last name or other appropriate field and select the Find Cards button.
3. Double click on the cardholder record in the lower section of the Search Access Card Holders form where cardholder records are listed.
4. Click in the Batch text box and enter the batch number of the new card if it is different from the previous batch number.
5. Click in the Card Number text box and enter the new card number.
6. Click on the Save & Exit button.
7. Click on the Exit button in the Search Access Card Holder form to return to the main screen.

Create a Temporary Card

When you assign cards to cardholders, you have the option to make the card temporary, restricting the number of times the card can be used, limiting the card to a date range, or both. Some typical examples for issuing temporary cards would be for visitors or guests, trades people who require limited access for a period of time, or for members who have joined a club and whose membership is limited to a certain number of visits or a specified period of time.

Select the Card Holder Database quick button from the main screen to make a temporary card and select the corresponding menu - Add New Card(s) for a new temporary card, Add Block of Cards for a block of temporary cards, or Edit/Delete Cards to make an existing card temporary.

Procedures

► *Make an Existing Card Temporary*

1. Select the Quick Buttons menu > Card Holder Database > Search Access Card Holders.
2. Select the Find All Cards button or enter cardholder data in an appropriate field and select the Find Cards button.
3. Locate and double click on the cardholder record in the lower section of the Search Access Card Holders form where cardholder records are listed.
4. Select the Temporary Card Options tab on the Cardholder form.
5. Click inside the Card Limited check box. A tick mark inside the box indicates the field is active.
6. If the card is to be restricted by usage, enter the maximum number of times the card can be used in the Card Limited to Number of Uses text box. If there is no usage restriction, leave the Card Limited to Number of Uses blank.
7. If the card has a temporary date range, click in the box to the left of Include Date Range Values. The box has a tick mark when active.
8. Under Date Valid From, the current date is circled on the calendar. If the start date is other than the current day, select the correct start date, or click on the arrows at the top of the calendar to scroll to the desired month and year and select the day on the calendar.
9. Repeat the above step to complete the Date Valid To fields.
10. Select Save & Exit.
11. Select the Exit button on the Search Access Card Holder form to return to the main screen.

Related Topics

▶ *Create a Block of Temporary Cards*

▶ *Create a New Temporary Card*

Find Cards with "Not Used Since" Feature

The Not Used Since feature allows you to search for inactive cardholders. If you wanted to know all the cardholders who had not used their cards within a given period of time, you would activate the Not Used Since field and specify a not used since date. The software searches through the database and lists all the cardholders who had not recorded any transactions since the date specified. You can also narrow your search by specifying other search criteria in conjunction with the Not Used Since feature.

The Not Used Since feature is a convenient utility to maintain up-to-date records by allowing you to search for inactive cardholders who you may wish to archive or delete from the database.

Procedure

▶ *Steps to Find Cardholders with "Not Used Since" Feature*

1. Select the Quick Buttons menu > Card Holder Database > Search Access Card Holders.
2. From the Search Access Card Holders form, click on the down arrow to the right of Not Used Since and specify the date to display inactive cardholder records. At the top of the calendar, click on the arrows to scroll back or forward to the month and year. Click on the day in the body of the calendar. The calendar closes with the Not Used Since date selected. The check mark in the box to the left indicates this search criterion is active.
3. The Sort By Field option allows you to specify the order of how cardholder records are sorted in the cardholder record window.
 - Alphabetical Fields A – Z
 - Numerical Fields 0 – 9
4. Click on the Find Cards button. The results of your search are listed in the cardholder records window.
5. To clear the cardholder records window and perform another search, click on the Clear Find button.

Print Cardholder Records

You can print a copy of cardholder records. To print cardholder records you must open the Search Access Card Holders form accessed from the Card Holder Database quick button on the main screen.

Procedures

►Steps to Print Cardholder Records

1. Select the Quick Buttons menu > Card Holder Database > Search Access Card Holders.
2. From the Search Access Card Holder form, either click on the Find All Cards button to list all cardholders or for specific cardholder records, specify the appropriate search criteria and click on the Find Cards button.
3. Click on the Print Listing button.
4. From the Print Card dialog box, either click on the Yes button for a detailed report listing all cardholder information, or click on No for an abbreviated report.
5. Click on the Printer icon located at the bottom of the Keyscan System VII Print Previewer.
6. From the Print dialog box, specify the Printer, Page range and Number of Copies.
7. Click on the Print button.
8. Select the Exit button on the Keyscan System VII Print Previewer form.
9. Select the Exit button on the Search Access Card Holders form to return to the main screen.

Print Photo Badges

If you have created photo badge templates with the System VII Photo Badge Template Editor and have a card printer connected, you can print cardholder badges from the Cardholder form.



You cannot change the badge's orientation from Portrait or Landscape in the Print Badge form; it is based on the orientation at the time the template was created in the Photo Badge Template Editor.

Printing Multiple Photo Badges

You can print multiple cardholder photo badges from the Search Access Card Holders form. Please note that you can only print from one photo badge template at a time, therefore, if you use multiple photo badge templates, ensure that the group of cardholders selected are associated to the same template. Use the search criteria to list cardholders in groups that are relevant to a template.

Procedures

► *Steps to Print a Cardholder Photo Badge*

A single badge can be printed from the Cardholder Information form with the appropriate cardholder record open or from the Search Access Cardholder Information form with the cardholder record selected in the record table.

1. Click on the Print Photo Badge button.
2. From the Print Card Badge form, click on the down arrow to the right of Select Badge Template and select the template from the drop down list. The orientation of the template is indicated by the radio button.
3. If the card is to be printed on both sides, click on the Double Side button and repeat step 2, otherwise go to the next step.
4. Click on the Print Current button to print a badge for the current cardholder.
5. To return to the main screen, click on Exit > Exit.

► *Steps to Print Multiple Cardholder Photo Badges*

1. Select the Card Holder Database button > Search Access Card Holders.
2. From the Search Access Card Holder form, click on the Find All Cards button to list all cardholders or for specific cardholder records, specify the appropriate search criteria and click on the Find Cards button.
3. For consecutive records, select the first cardholder record at the top of the table, hold the Shift key, and select the last cardholder record or to select non-consecutive records hold down the Ctrl key and select individual records.
4. Click on the Print Photo Badge button.
5. From the Print Card Badge form, click on the down arrow to the right of Select Badge Template and select the template from the drop down list. The orientation of the template is indicated by the radio button.
6. If the card is to be printed on both sides, click on the Double Side button and repeat step 5, otherwise go to the next step.
7. Click on the Print All button.
8. To return to the main screen, click on Exit > Exit.

Export Records in PDF Format

Cardholder records can be exported as Portable Document Files (PDF), which can be emailed to other system users or management for maintaining external records of your cardholders.

Procedure

► *Steps to Export Cardholder Records in PDF Format*

1. From the main screen, click on the Card Holder Database quick button > Search Access Card Holders.
2. From the Search Access Card Holder form, click on the Find All Cards button to list all cardholders or for specific cardholder records, specify the appropriate search criteria and click on the Find Cards button.
3. Click on the Print Listing button.
4. From the Print Card dialog box "Do you wish to run a detailed report?", select either:
 - No to list only card #, group access and PIN
 - Yes to list all cardholder information.
5. From the Keyscan Report Previewer form, click on the Export to PDF button.
6. From the Select a PDF export file dialog box, name the file and specify a file folder.
7. Click on the Save button.
8. To return to the main screen, click on Exit > Exit.

Import/Export Cardholder Information

The Import/Export Card Holder Information form allows you to export or import cardholder records in CSV file format.

If you have an existing database that includes information common to the Keyscan database, such as first name, last name, telephone number etc., rather than re-enter that data, importing your database in a CSV formatted file is an option that can save you time and effort. Before you do this, however, you must be aware of the conventions to successfully import a CSV file.



The CSV file cannot have any commas between names for any field, otherwise the import will fail. Edit out any commas in the CSV file from a spreadsheet before you import the file into the Client software.

Conventions for Importing CSV Files

Before you import a CSV formatted file to the System VII Client software, there are conventions that must be followed. This may entail adding fields to the System VII Client software and revamping part of your CSV formatted file once you have opened it in the spreadsheet. Since there are an infinite number of possible variations to the structure and content of databases, we can only provide some

general guidelines. You may have to experiment before attaining successful results.

▶ *View Conventions for Importing CSV Files*

Procedures

▶ *Steps to Export Cardholder Information*

1. From the main screen, click on the Card Holder Database quick button > Search Access Card Holders.
2. From the Search Access Card Holder form, click on the Find All Cards button to list all cardholders or for specific cardholder records, specify the appropriate search criteria and click on the Find Cards button.
3. In the upper left corner of the Search Access Card Holders form, click on the Import and Export Card Holder Information menu > Export Card Holder Information.
4. From the Import and Export Card Holder Information form, click in the box to the left of the fields to be captured in the data export. You can also use the Select All button to automatically select all data fields.
 - You cannot de-select required fields. They must be included in the data export.
5. Click on the Export Card Holder Information button.
6. From the Keyscan Export Card File dialog box, locate a directory by clicking on the down arrow to the right of the Save In box.
7. Enter a file name in the File Name text box.
8. Click on the Save button.
9. From the Card Holders Export Completed box, click on the OK button.
10. Click on the Exit button to return to the Search Access Card Holders form.
11. Click on the Exit button to return to the main screen.

▶ *Steps to Import Cardholder Information*

Important

You must have the 6 required field headings listed in your CSV file to import. If you do not have elevators, you must still have a column heading ElevatorGroupANumber. Enter a zero (0) in the ElevatorGroupANumber column for each cardholder record. Review Conventions for Importing CSV Files.

1. From the main screen, click on the Card Holder Database quick button > Search Access Card Holders.

2. In the upper left corner of the Search Access Card Holders form, click on the Import and Export Card Holder Information menu > Import Card Holder Information.
3. Select the appropriate fields that are in the CSV file that you are importing.
4. If you are updating existing cardholder records, select the Update Cardholder Information box. If you are adding new cardholder records, leave the Update Cardholder Information box unchecked.
5. Click on the Import Cardholder Information button.
6. From the Keyscan Import Card File dialog box, select the CSV file that you are importing, then click on the Open button.
7. The Import and Export Card Holder Information form lists the cardholder records that failed to be imported. If the form is empty, all records were successfully imported. Any records displayed on the form were not imported. Review your CSV file and try re-importing only those records which failed.
8. From the Card Holder Import Completed box, click on the OK button.
9. Click on the Exit button.
10. Click on the Exit button in the Search Access Cardholders form to return to the main screen.

Related Topic

▶ *Schedule Importing Cardholder Information*

Import CSV Files - Conventions

We strongly urge that you have some familiarity with the System VII Client software before you import the CSV file. You should setup door and, if applicable, elevator groups. Review the Cardholder Information form to see how they compare to your current CSV fields. Use the Optional Card Holder form to create fields not covered by the Cardholder Information form so your CSV file dovetails as closely as possible to the System VII Client cardholder fields.

You can also delete cardholder records. In the CSV file that is used for updating records type *DELETE* in the FirstName and LastName fields. Ensure that you include the asterisks and use upper case.

The CSV file cannot have any commas between names for any field, otherwise the import will fail. Edit out any commas in the CSV file from the spreadsheet before you import the file into the Client software.

Please note the following if you use Excel when saving CSV formatted files:

- Blank cells in the last column may cause Excel to fail to save all entries in the column

- Columns with long numbers may be truncated. See Microsoft’s knowledge based article Q216023 on their web site for more details.
- Dates must be formatted as follows: Day/Month/Year

Mandatory Cardholder Database Fields

You must include the following 6 data field headings in your CSV file. They must be formatted exactly as they are shown below since headings are case sensitive. You cannot have spaces between words in the headings. The column headings can be in any order. Any of these data fields can be empty if there is no matching or comparable content. But these six headings must be included.

Field Heading	Character
CardNumber	Numeric
CardBatch	Numeric
FirstName	Alpha
LastName	Alpha
GroupANumber	Numeric
ElevatorGroupANumber	Numeric

The mandatory Field Headings listed above are shown as they would appear in the first row of a spreadsheet.

A	B	C	D	E	F
CardNumber	CardBatch	FirstName	LastName	GroupANumber	ElevatorGroupANumber

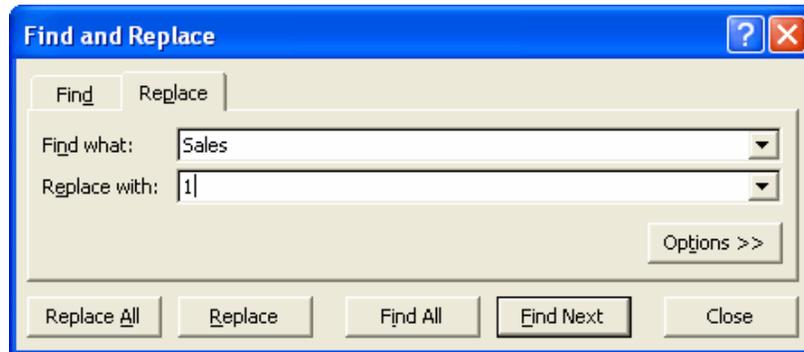
GroupANumber refers to a Door Group assignment in the System VII Client software and is generally expressed as a department name. The System VII Client software, however, assigns each Door Group a number from 001 to 511. The GroupANumber field in the CSV file must list the number, not the alpha description. You can change an alpha description to a numeric value in the spreadsheet. You do not have to enter the zeros that precede the number.

ElevatorAGroup refers to an Elevator Group assignment. The same conventions apply as with GroupANumber.

Door Group as seen in Search Door Groups form – Client software

Group Description	Group Active
001-Sales	Active
002-Finance	Active

Replace form in Microsoft Excel



Non-mandatory Cardholder Database Fields

The following fields are found on the Cardholder Information form in the Keyscan Client software that are non-mandatory. These fields are optional and would only be included if your CSV file had a comparable field. They must be formatted exactly as they are shown below since headings are case sensitive. You cannot have spaces between words in the headings.

Field Heading	Character
GroupBNumber	Numeric
ElevatorGroupBNumber	Numeric
ArchivedCard	Not Applicable
CardLimitedNumber	Numeric (1-249)
ValidFrom	Date - Format (MM/DD/YY) Must be equal to today or greater
ValidTo	Date - Format (MM/DD/YY) Must be equal to today or greater
PhotoLocation	Path to users picture file (c:\Pictures\)
PhotoName	Filename of picture (MaryAnn.jpg)

Non-mandatory Additional Cardholder Fields

The following fields are the Additional Cardholder Information in the System VII Client software. These fields are optional and would only be included if your CSV file had a comparable field. They must be formatted exactly as they are shown below since headings are case sensitive. You cannot have spaces between words in the headings.

Field Heading	Character
TelephoneNumber	Numeric with no hyphens
TelephoneExt	Numeric
FaxNumber	Numeric
EmailAddress	Alpha/Numeric
CardLocation	Alpha/Numeric
Parkingspot	Alpha/Numeric
Carplate	Alpha/Numeric

Non-mandatory Optional Cardholder Fields

There are 10 Optional Card Holder fields that are user-defined in the Keyscan Client software. If you have fields in your CSV file not represented by the preceding cardholder fields, open the Card Holder Optional Fields form in the Utilities menu. Define any required cardholder fields.

After you have created your optional fields in the Keyscan Client software, return to the CSV file in the spreadsheet and enter the applicable OptionalField# as the heading. Do not use the description you gave the optional field for the heading. The headings must be formatted exactly as shown. Headings are case sensitive. You cannot have spaces between words in the headings.

Field Heading	Character
OptionalField1	exactly as shown
OptionalField2	exactly as shown
OptionalField3	exactly as shown
OptionalField4	exactly as shown
OptionalField5	exactly as shown
OptionalField6	exactly as shown
OptionalField7	exactly as shown
OptionalField8	exactly as shown
OptionalField9	exactly as shown
OptionalField10	exactly as shown

If there are any redundant fields that are not relevant to the System VII Client cardholder fields, delete those fields before you import the CSV file.

Schedule CSV Imports

You can schedule the System VII software to automatically import CSV files to either add new cardholder records or update existing cardholder records with the Schedule Imports function. CSV files can be imported on multiple days over the course of a full week.



Keyscan recommends creating two separate CSV files: one for new records and one for updating records.

You can also automatically delete cardholder records using this procedure. In the CSV file that is used for updating records type *DELETE* in the FirstName and LastName fields. Ensure that you include the asterisks and use upper case.

The CSV path/file name cannot exceed 200 characters in total. Store the CSV file in a path/folder location that complies with this convention.

When using the schedule feature, the Client must be open during the scheduled days of the week and the logged on user must have permissions to access the CSV file(s) if it is at a location other than the Client PC.

Keyscan recommends doing both of the following procedures so that you have addressed adding new records and updating existing records.

Procedures

► *Steps to Schedule Importing New Cardholder Records*

1. From the main screen, click on the Card Holder Database quick button > Search Access Card Holders.
2. In the upper left corner of the Search Access Card Holders form, click on the Import and Export Card Holder Information menu > Import Card Holder Information.
3. Select the appropriate fields that are in the CSV file that you are importing. Note the required fields. Ensure that the Update Cardholder Information box unchecked.
4. Click on the Schedule button.
5. From the Import and Export Card Holder Information – Report Schedule dialog box, either enter the path and file name in the Import File text box , or select the Browse button, navigate to the file location, select the CSV file, then click on the Open button.
6. Select the days of the week to add the new records.
7. Select the Save & Exit button.
8. Select the Exit buttons on the open forms to return to the Client main screen.

► *Steps to Schedule Importing Updated Cardholder Information*

1. From the main screen, click on the Card Holder Database quick button > Search Access Card Holders.
2. In the upper left corner of the Search Access Card Holders form, click on the Import and Export Card Holder Information menu > Import Card Holder Information.
3. Select the appropriate fields that are in the CSV file that you are importing. Note the required fields.
4. Select the Update Cardholder Information box so it is checked.
5. Click on the Schedule button.
6. From the Import and Export Card Holder Information – Report Schedule

dialog box, either enter the path and file name in the Import File text box, or select the Browse button, navigate to the file location, select the CSV file, then click on the Open button.

7. Select the days of the week to update the existing cardholder records.
8. Select the Save & Exit button.
9. Select the Exit buttons on the open forms to return to the Client main screen.

Related Topic

► *Import/Export Cardholder Information*

Reports - Access Levels

The Reports menu, located in the Search Access Card Holders form, presents 2 report formats for viewing access levels:

Cardholder – Reader Access Level Reports – lists the door group, access level, time zone at specified readers (doors) for each requested cardholder.

Reader Access Level Report – lists the door groups, access levels, time zones and cardholders at each requested reader (door). As an option the report will list cardholders assigned to each door group.

Deleted Cardholder Report – lists cardholders whose records have been deleted from the database.

Update Cardholder Security Level – allows changing the security level of selected cardholders in the table to prevent a system administrator with a lower security level from altering a card record assigned a higher security level. Creating security levels is not recommended unless you are an advanced user and require stringent system operator controls.

In essence, both reports display the same information, but it is displayed from different perspectives – cardholder-centric or reader-centric.

Procedures

► *Steps to Run a Cardholder Reader Access Level Report*

1. From the main screen, select the Card Holder Database quick button > Search Access Card Holders.
2. From the Search Access Card Holder form, click on the Find All Cards button to list all cardholders or for specific cardholder records, specify the appropriate search criteria and click on the Find Cards button.
3. If viewing 1 cardholder record, select the record in the yellow table. If viewing multiple records, select the 1st record in the yellow table, press the Shift key and select the last record.

4. Select the Reports menu > Cardholder – Reader Access Level Report. From the flyout menu, select either All Sites or Current Site, depending on the report you are running. You may not see All Sites if your system user account does not have authority to view multiple sites.
5. From the Reader Access Level Report, in the boxes to the left, select the readers you wish to include in the report.
6. Click on the Run Report button.
7. Select either Yes or No in the Time Zone Details dialog box, depending on whether you wish to include those details in your report.
8. The Keyscan Report Previewer lists a summary of the requested report.
9. Click on the Exit buttons to close the forms until you return to the main screen.

► *Steps to Run a Reader Access Level Report*

1. From the main screen, select the Card Holder Database quick button > Search Access Card Holders.
2. From the Search Access Card Holder form, select the Reports menu > Reader Access Level Report.
3. From the Reader Access Level Report, in the boxes to the left, select the readers you wish to include in the report.
4. If you wish the report to display cardholder information under each reader, click in the radio button to the left of Include All Active Cards.
5. If you wish to omit groups with no access at the selected readers in the report, click in the Exclude Groups with No Access box.
6. Click on the Run Report button.
7. Select either Yes or No in the Group/Reader Report dialog box, depending on whether you wish to include those details in your report
8. Select either Yes or No in the Time Zone Details dialog box, depending on whether you wish to include those details in your report.
9. The Keyscan Report Previewer lists a summary of the requested report.
10. Click on the Exit buttons to close the forms and return to the main screen.

► *Steps to Run a Deleted Cardholder Report*

1. From the main screen, select the Cardholder Database quick button > Search Access Cardholders.
2. From the Search Access Cardholders form, select the Reports menu >

Delete Cardholder Report.

3. From the Detailed Cardholder Report warning box, select Yes if you wish to include General, Additional and Optional card details, select No for General card details on the Deleted Cardholder report.
4. You can print or export (PDF) the report by selecting the printer icon or selecting the Export to PDF button.
5. To close the report and return to the main screen, select the Exit buttons.

Related Topic

▶ *Security Levels*

Last Card Transactions

On the Cardholder form is a tab entitled Last Card Transaction. When the tab is selected, the Last Card Transaction window opens. The window lists the device name, the direction, and the date and time of the transaction. The button shows the date and time this function was accessed. Transactions are cleared from the window each time the cardholder record is closed.

Last Card Transactions are retained for the past 7 days to a maximum of 25 transactions.

The transactions displayed in this window are contingent on the system user's authority level.

To Display Transactions

From the Cardholder form, select the Last Card Transactions tab. Click on the Last Card Transactions button to list transactions.

Communication Requests

Processing Communications Request

When the Client software is requested to perform a task that interacts with the access control units or elevator control units, the Processing Communications Request window opens. An example would be when you access the Door Lock/Unlock Status quick button on the main screen. When communications via the Communications Server are established the Processing Communications Request window closes and you are linked to the panels to perform the relevant tasks.

To abort the communications request, click on the Cancel Request button.

Door Status/Manually Lock/Unlock Doors

Door Lock/Unlock Status

The Door Lock/Unlock Status form allows you to view the current status of all doors regulated by access control units in the Keyscan system. From this form, you can also do any of the following tasks:

- Lock or unlock individual doors
- Lock or unlock all doors controlled by a specified access control unit
- Lock or unlock all doors controlled by all access control units
- Unlock a door for a specified period of time to a maximum of 7 days
- Unlock a door momentarily using "Pulse"

The Door Lock/Unlock Status form is accessed with the quick button from the main screen.



The software re-opens the Door Lock/Unlock Status form with the last selected serial or network connected ACU. This feature excludes modem connected ACUs, in which case no ACU is selected in the Unit ID – Site ID box.

Procedures

► Overview of Door Lock/Unlock Status

Unit ID - Site ID allows selecting sites, if the user has authority to view multiple sites, and the access control units. The form displays the doors controlled by the selected panel.

Unit ID - Door List - Site ID is a directory of all site access control units and the doors that each panel regulates.

Door Status indicates the door's current status

- Locked
- Unlocked
- No Status (door has not been used since connected to access control system)

The button to the left of each door allow you to do the following manual actions:

- Lock/Unlock a door
- Pulse a door open
- Time Unlock a door

Lock/Unlock a door by clicking on the button. The button changes from Lock to Unlock, depending on the current door status.

Unlock a door open momentarily by clicking on the Pulse button.

Unlock a door for a specified time period by clicking on the Timed Unlock button.

For Timed Unlock, use the date and clock to set the door's unlock time before it re-locks. Select date or time component and click on the up/down arrows. After the re-lock time is set, click on the Apply Timed Unlock button.

The Lock All – Current Site button locks all doors controlled by all the access control units at the logged on site.

The Unlock All – Current Site button unlocks all doors controlled by all the access control units at the logged on site.

The Lock All – Current Unit button locks all doors controlled by the selected access control unit.

The Unlock All – Current Unit button unlocks all doors controlled by the selected access control unit.

The Refresh button re-displays the current door status.

The Exit button closes the Door Unlock/Lock Status form.

Keyscan Admin User Account

Keyscan Admin User Account

Each time that you create a new site, the client creates a Keyscan Admin user account for that site. As an example, if you have created 3 sites, you would have 3 Keyscan Admin system user accounts with one listed under each site. This account, by default, is always designated with the following settings:

- User Name (User ID) – Keyscan
- Password – KEYSKAN
- Status – Master Login Account

Depending on the level of security required for your access control system, you may wish to neutralize the Keyscan Admin account by deleting or archiving it. If you have limited experience using the System VII Client software, we suggest you archive the Keyscan Admin account until you gain a better understanding of the software. Archiving the Keyscan Admin system user account retains the record in the database but makes the account inactive so that no one can log on to the site using the keyscan User Name and the KEYSKAN Password.



Before you delete or archive the Keyscan Admin user account for a particular site, you must have 1 system user account with Master Login status for that site with the proper authority levels to log on a given site before deleting or archiving the Keyscan Admin account. An easy method to create a new system user account that replicates the settings of the Keyscan Admin account is use the Create New Users from Current Authority Levels function. Open the Keyscan Admin account in the System User Information form, select the Create New Users from Current Authority Levels button, and enter a new user ID and password, as well as other user information. Leave all the user functions and authority levels intact.

Procedures

► *Steps to Archive a Keyscan Admin Account*

1. Log on using a system user account with Master Login Account status or System Administrator status. Do not log on with the Keyscan Admin account.
2. From the main screen, select the System Settings menu > Add/Edit System Users.
3. From the table where the system users are listed, select the Keyscan Admin account that is to be archived. You will have a corresponding Keyscan Admin account for every site that you have created, unless previously deleted. You may have to click on the Find Users button to list the system users.

4. Double click on the Keyscan Admin account you are archiving.
5. From the System User Information form, click in the box to the left of Archived User to activate this option.
6. Click on the Save & Exit button to return to the Find System Users form.
7. From the Find System Users form, click on the Find Users button to update the user list.
8. Scroll to the User Status column. The Keyscan Admin account is marked as Inactive.
9. Click on the Exit button to return to the main screen.

► *Steps to Delete a Keyscan Admin System User Account*

1. Log on with a System User account that has Master Login Account status or System Administrator status. Do not log on with the Keyscan Admin account.
2. From the main screen, select the System Settings menu > Add/Edit System Users.
3. From the table where the system users are listed, select the Keyscan Admin account that is to be deleted. You will have a corresponding Keyscan Admin account for every site that you have created, unless previously deleted. You may have to click on the Find Users button to list the system users.
4. With the Keyscan Admin account selected, click on the Delete button.
5. Click on the Yes button in the warning dialog box. The Keyscan Admin system user account is removed from the system user list in the Find System User form.
6. Click on the Exit button to return to the main screen.

Log On/Passwords

Log On to a Site

When you open the System VII Client or log off, usually to enter another site, you are prompted by the system to log on. This safeguards the system so that only valid users may operate the software and the access control system.

If you have multiple sites, to log on to other sites, you must have the necessary permissions which are set in the System User information form.

Procedures

►Steps to Log On

1. From the main screen, select the File menu > Log Off.
2. From the Client Log On form, click on the down arrow to the right of Site Name and select the site from the drop down list.
3. Enter your User Name.
4. Enter your Password.
5. Click on the OK button.

Passwords

Log On Password

As a security precaution, each system administrator is assigned a password, which they must enter when logging on to the Client software.



System administrators can change passwords at any time. You must have System Administrator enabled and System Users checked in the User Authority Levels table to change a password.

Password Confirmation

When an account has been created for a new system user and that user is logging on to the Client application for the first time, the system user must complete the Password Confirmation dialog box.

Procedures

►Steps to Confirm a Password

1. Enter your password in the New Password text box.
2. In the Confirm Password text box, enter the same password that you entered in the New Password text box.

3. If you are a system user registered on multiple sites, click in the box to the left of Update All Valid User Sites, otherwise leave this field inactive.
4. Click on the OK button.

► *Steps to Change a Password*

1. Log on to an authorized site.
2. Select the System Settings menu > Add/Edit System Users.
3. Double click on the user's name whose password is to be changed.
4. Click on the Reset Password button at the bottom of the System User Information form. The Client software temporarily changes the system user's password to KEYSCAN (upper case). You cannot change the password from the System User Information form.
5. Click on the Save & Exit button.
6. Click on the Exit button in the Find System Users form to return to the main screen.
7. From the main screen, select the File menu > Log Off.
8. From the Log On – Client dialog box, if appropriate, click on a language button.
9. If appropriate, select the system user's site by clicking on the down arrow to the right of the Site Name text box.
10. Enter the User ID in the User Name text box.
11. Type KEYSCAN (upper case) in the Password Text box.
12. Click on the OK button.
13. From the New System User Password dialog box, enter the new password in the New Password text box. Please remember, passwords are case sensitive.
14. Re-enter the same password in the Confirm Password text box as you entered above.
15. If the system user is listed on multiple sites, activate Update All Valid User Sites, by clicking in the box to the left.
16. Click on the OK button. The system user's new password is now in effect.

Database Options

Database Maintenance Options

The Database Setup form has the following 5 database options:

- Database Backup
- Database Restore
- Purge Transactions
- Compress Database
- Re-index Database

As well as the five preceding database maintenance functions, the form indicates the current database file size. The maximum file size for the Keyscan database is 4 gigabytes. The Keyscan software will automatically warn when the database file reaches 75% of its allowable capacity.

Please observe sound database maintenance procedures to safeguard your site data. You should regularly backup the database as well as make a copy to another medium such as a writable CD or to another network location.

As your database gets larger, especially if it nears the 75% threshold, you should purge it of older entries. Ensure you have backed it up first. After purging your database of older entries, compress it, then re-index it.

In the lower left corner, selecting the Calculate First and Last Transaction Dates will inform you of the date ranges of your live database. Before you purge it of older entries, ensure that you have a backup dated on or after the first transaction date of the live database.

Related Topics

▶ *Backup the Database*

▶ *Restore the Database*

▶ *Purging Transactions*

▶ *Compress and Re-index the Database*

Restore the Database

In the event that you had to replace the computer or hard drive in your Keyscan Access Control System where the Database Maintenance module was installed and you have had to re-install that module, use the Restore a Database option to retrieve your site data to get your system operating again.



You must have backed up your database and either copied it to another medium such as a writable CD or copied it to another PC or server location where it was safely stored and can be retrieved. If you did not backup your

database, you cannot use the Restore a Database option.

The Restore Database should only be used if you had to replace the computer or hard drive where the Database Maintenance module was installed. The Restore (Database) Backup allows you to retrieve your site data after you have re-installed the Database Maintenance module. If you are not an experienced computer user, we strongly recommend that you call Keyscan technical support for assistance to restore your database.

You cannot perform the Restore Database function from the System VII Client.

Networks

If your system is operating on a network and you have re-installed the Database module on a computer with a different IP address from where it was originally installed, you must open each Keyscan Client and specify the new IP address in the Database Location form which is accessed from the System Settings menu.

Procedures

► Steps to Restore the Database

Prior to using the Restore Database function, you must close all System VII Clients and Photobadge Template Editor(s). If applicable, you must also stop the Keyscan System VII Communication Service.

Preliminary

1. Close all System VII Clients, Communications Managers and ,if applicable, all Photobadge Template Editors. (You can use the Display software Connections in the Utilities menu to determine which System VII applications are open.)

Steps to Stop the Keyscan System VII Communication Service

If you are not running the Communication Managers as a service, by-pass this procedure.

1. Locate the PC where the Keyscan System VII Communication Service is installed.
2. Select Start > Control Panel > Administrative Tools.
3. From the Administrative Tools window, select Services.
4. From the Services window, scroll down and double click on Keyscan Service Comms.
5. From the Keyscan Service Comms Properties window with the General tab selected, click on the Stop button.
6. Click on the OK button.

7. Exit the Control Panel windows to return to the desktop.
8. If you have more than 1 Keyscan System VII Communication Service installed, repeat the stop procedures at each applicable PC.

Steps to Restore the Database

Locate the computer with the Keyscan System VII DBUtility.

1. Right click on the Start button in the lower left corner and select Explore.
2. Navigate to the Program Files > Keyscan7 > Database folder and double click on the Keyscan DBUtil.exe file.
3. From the Select a Language dialog box, click on the OK button.
4. From the Database Maintenance dialog box, click on the Restore Backup button.
5. From the Restore Backup form either, a) enter the drive, folder location, and backup file name in the File Name text box, or b) click on the Browse button and navigate to the folder location and select the backup file. Click on the Open button.
6. Click on the Restore button.
7. From the Restore Backup query box: Are you sure you want to restore the backup file?, click on the Yes button.
8. From the Keyscan System V – Database Util confirmation box, click on the OK button.
9. From the Restore Backup form, click on the Exit button.
10. Click on the X button in the upper right corner to close the Database Maintenance form.

Re-Start the Keyscan System VII Communication Service

If you do not run the Communications Manager as a service, by-pass this procedure.

1. Locate the PC where the Keyscan System VII Communication Service is installed.
2. Select Start > Control Panel > Administrative Tools.
3. From the Administrative Tools window, select Services.
4. From the Services window, scroll down and double click on Keyscan Service Comms.
5. From the Keyscan Service Comms Properties window with the General tab

- selected, click on the Start button.
6. Click on the OK button.
 7. Exit the Control Panel windows to return to the desktop.
 8. If you have more than 1 Keyscan System VII Communication Service installed, repeat the stop procedures at each applicable PC.

Related Topic

▶ *Backup the Database*

Purging Transactions

Purging deletes data entries from the transactions history. Generally transactions should be purged when the database nears or crosses 75% of the 4 gigabyte maximum. Be sure that you backup the database and save it to another medium or network location before you purge the database of older transactions.

If you purge transactions, we recommend that you also compress and re-index the database.

You can produce a daily transaction count, which the system saves as ArchiveCounts.csv saved in the Keyscan System VII directory. This file lists the number of transactions that occurred each day during the bracketed purge date range.

The Purge Transactions Data Options form allows selecting which sites are purged of data and which transaction types are purged. You must purge transactions from the current logged on site. At least 1 transaction type must be selected for purging.

The Purge Transaction function is accessed from the System Settings menu > Database Maintenance.

Procedure

▶ *Steps to Purge Database Transactions*

1. From the Database Setup form, click on the Purge Transactions button.
2. From the Purge Options message box, Do you wish to continue with the purge option, if you have backed up your database, click on the Yes button. If you have not backed up the database, click on No and first backup your database and save it on another medium or network location, then return to the Purge Transactions instructions.
3. From the Calculate Oldest Transaction Date message box, select Yes if you wish to view the oldest transaction date or No to bypass this function. If Yes was selected, the oldest date is entered in the From box of the Purge Transactions Data Options form.

4. If applicable, de-select any sites) listed in the upper left you do not wish to purge transactions from. By default, all sites you are permitted to view are pre-selected.
5. If applicable, de-select any transaction types that you do not wish to purge from the database.
6. The From date box in the Purge Transactions form lists the current date unless you selected to view the oldest transaction in step 3. To change the date, click on the down arrow to the right of From, use the arrows to scroll to the desired month/year, and select a day in the calendar.
7. The To date box lists the current date. To change to an earlier date, click on the on the down arrow to the right of To, use the arrows to scroll to the desired month/year, and select a day in the calendar.
8. Optional. To produce a daily transaction count saved in a CSV file, click on the Export Daily Counts button. A file called ArchiveCounts.csv is saved in the Keyscan > Client directory. This file lists the all the transactions that occurred each day during the bracketed purge date range. The count does not reflect counts based on de-selecting sites or transaction types in steps 4 & 5. From the Export Count Completed confirmation box, Click on the OK button.
9. Click on the Start Purge Transactions button.
10. From the WARNING: Archive Data message box, click on the Yes button.
11. When the purging is completed, click on the OK button in the Purge Transaction Data Completed message box.
12. From the Remove Deleted Cardholders warning box, if you wish to remove deleted cardholder records from the database, click on the Yes button otherwise click on the No button to retain deleted cardholder records.
13. From the Compress Data message box, either: click on the Yes button (recommended) to compress the database and continue to step 14, or click on the No button to return to the Database Setup form.
14. If you compressed the database, click on the OK button in the Compress Database Completed confirmation box.
15. From the Database Setup form, click on the Reindex Database button.
16. Click on the Yes button in the Reindex Database message box.
17. Click on the OK button in the Reindex Database Completed confirmation box.
18. From the Database Setup form, click on the Exit button to return to the main screen.

Related Topic

▶ *Compress and Re-index the Database*

Compress and Re-index the Database

Compressing the database reduces its size. If you have a site with a large volume of cardholders producing a heavy volume of daily transactions, compressing the database helps reduce the frequency of purging. After compressing the database, we recommend that you also re-index the database.

The Compress Database and Re-index Database functions are accessed from the System Settings menu > Database Maintenance.

Procedure

▶ *Steps to Compress and Re-index the Database*

1. From the Database Setup form, click on the Compress Database button.
2. From the Compress Data message box, click on the Yes button.
3. From the Compress Database Completed confirmation box, click on the OK button.
4. From the Database Setup form, click on the Reindex Database button.
5. Click on the Yes button in the Reindex Database message box.
6. Click on the OK button in the Reindex Database Completed confirmation box.
7. From the Database Setup form, click on the Exit button to return to the main screen.

Site Contacts

Find Site Contacts

The Search Site Contacts form acts as the hub to search for add, edit, delete, or print a listing of site contacts. The Find Site Contacts form is accessed from the System Settings menu > Site Setup > Site Information Search form > Site Information form.



You may use multiple fields to conduct your site contacts search.

Procedures

► *Review of Find Site Contacts Form*

Contact First Name – To find a site contact by first name, enter the first name in the text box.

Contact Last Name – To find site contact by last name, enter the last name in the text box.

Contact Location – To find a contact by site, enter the site name in the text box. You must have authorization to view other sites.

Contact Type – To find a contact by type, click on the down arrow and select the appropriate option:

- Emergency Contact
- Notify Contact
- Other Contact
- Visitor Contact

Find Contacts – Click on this button after specifying search criteria or to view all site contacts if no criteria is specified.

Clear Find button – Click on this button to clear the site contacts from the list panel.

List of Contacts Table – Lists the site contacts after clicking on the Find Contacts button

Print Listing button – Click on this button to print a listing of site contacts.

Add New button – Click on this button to add a new site contact. (Opens the Site Contacts Information form.)

Delete button – Click on this button to delete the site contact record from the database.

Exit button – Click on this button to return to the Site Information form.

► *Steps to Search for a Site Contact*

1. From the main screen, select the System Settings menu > Site Setup.

2. From the Site Information Search form, double click on the desired site.
3. From the Site Information form, select the Site Contacts button.
4. In the appropriate field, enter the criteria to search for the site contact, by either: typing the criteria in the text box or clicking on the down arrow and selecting the criteria from the drop down list.
5. Click on the Find Contacts button.
6. The results of your search are shown in the table.
7. To clear the site contacts from the search list and perform another search, click on the Clear Find button.
8. Click on the Exit button to return to the Site Information form.

System Users

Add System Users

For details and procedures on adding system users, click on the link below.

▶ [Add System Users](#)

Find System Users

The Find System Users form acts as the central hub, not only to search for system users, but also add, edit, archive, or delete system users.

System users with Master Login status have a broader range of functionality than system users with just System Administrator status.

You may use multiple fields to conduct a system user search.

The Find Users form, is accessed from the main screen in the System Settings menu > System Users.

Procedures

▶ [Comparison between Master Login and System Administrator](#)

Function	Master Login Account	System Administrator
System User List	lists all system users for all sites	lists system users for logged on site only
Search By	First Name Last Name User Language User Status Site Name	First Name Last Name User Language User Status
Print	Yes	Yes
Copy User to Another Site	Yes	No
Print Listing	Yes	Yes
Clear Find	Yes	Yes
Add New	Any Site	Logged on Site
Delete	Any system user at any site except a higher security level if in effect	Any system user on logged on site, except system user with Master Login Account status or higher security level if in effect.

▶ [Overview of Find System User Form](#)

First Name – to find a system user by first name, enter the first name in the text box.

Last Name – to find system a user by last name, enter the last name in the text box.

User Language – to find system users by language, click on the down arrow and select the appropriate language option:

- English
- French (N/A)
- Spanish N/A)

User Status – to find system users by status, click on the down arrow and select the appropriate status option:

- All User status
- Active Users
- Inactive (Archived) Users

Site Name (Master Login Account only) – to find system users by site, click on the down arrow and select the appropriate site.

Find Users button – click on this button after specifying system user search criteria.

Copy User to Another Site button (Master Login Account only) – click on this button after selecting system user to be copied to another site.

Print Listing button – Click on this button to print the system users.

Clear Find button – Click on this button to clear the system users from the system users list table.

Add New button – Click on this button to add a system user. (Opens the System User Information form.)

Delete button – Click on this button after selecting the system user to be deleted.

Exit button – Click on this button to return to the main screen.

► *Steps to Search for System Users*

1. From the main screen, select the System Settings menu > Add/Edit System Users.
2. From the Find System Users from in the appropriate field, enter the criteria to search for the system user, by either: typing the criteria in the text box or clicking on the down arrow and selecting the criteria from the drop down list.
3. Click on the Find Users button. The results of your search are listed in the system user accounts window.
4. To clear the system user accounts window and perform another search, click on the Clear Find button or double click on the system user in the yellow table to edit or archive the record in the System User Information form.
5. Click on the Exit button to return to the main screen.

Delete or Archive System Users

Periodically, you may find that you have to either delete a system user who has perhaps left your organization or been assigned other responsibilities or archive a system user (de-activate user) who has taken an extended vacation or a leave of absence.

Deleting the system user permanently removes the account from the database.

Archiving the system user de-activates the account, but retains it in the database. The system user cannot log on while his or her account is archived.

Procedures

► *Steps to Archive a System User Account*

1. From the main screen, select the System Settings menu > System Users.
2. From the yellow table where the system users are listed, select the account that is to be deleted or archived.
3. If it is not listed, enter the last name in the Last Name text box. Click on the Find Users button and select the system user account.
4. Double click on the System User's account you are archiving.
5. From the System User Information form, click in the box to the left of Archived User to activate this option.
6. Click on the Save & Exit button to return to the Find System Users form.
7. From the Find System Users form, click on the Find Users button to update the user list.
8. The status of system user's account has changed to Inactive in the User Status column.
9. Click on the Exit button to return to the main screen.

► *Steps to Delete a System User Account*

1. From the main screen, select the System Settings menu > System Users.
2. From the yellow table where the system users are listed, select the account that is to be deleted or archived.
3. If it is not listed, enter the last name in the Last Name text box. Click on the Find Users button and select the system user account.
4. With the system user account selected, click on the Delete button.
5. Click on the Yes button. The system user account is removed from the system user list in the Find System User form.

6. Click on the Exit button to return to the main screen.

Transaction Reports

Transaction Reports

The Transaction Reports forms allow you to review site activity based on specific criteria that you define. You can create a one-time report, create and save a named report for repeated use, schedule when reports are run, email reports (PDF), or save reports in CSV or PDF format.



In order to Schedule a report, you must first name and format the report.

Transaction Reports has 3 forms.

- Date Options and Other Settings - This form is used to specify the dates of the transactions, the transaction types, and how the transactions are sorted.
- Cardholders, Optional Fields - This form is used to specify which cardholders are included in the report. This can be a single cardholder, a group of cardholders, or all cardholders.
- Devices, Direction - This form is used to specify an individual device, a group of devices, or all devices for either doors, elevators, auxiliary inputs, and supervised inputs.

Transaction Reports are accessed from the Quick Buttons menu or the quick button on the main screen.

Overview

► *Date Options and Other Settings*

This form is used to specify the dates of the transactions, the transaction types, and how the transactions are sorted.

Date Options presents three choices: Date Range, Last # of Days, One Day.



When a Date Option is selected, the two other option boxes are dimmed and unavailable. To re-select a date option, de-select the active option, then select your alternative choice.

Each date option has a different Date Settings panel to set the dates and times of the report.

If Date Range is selected, specify the From and To dates under Date Settings, the date Start Time and End Time, and the transaction Start Time and End Time under Transaction Settings.

- Start Time commences at Hour + 00 minutes, 00 seconds
- End Time concludes at Hour + 59 minutes, 59 seconds

If Last # Days is selected, specify the number of days, and the date Start Time and End Time in the Date Settings panel.

If One Day is selected, specify the day, and the date Start Time and End Time in the Date Settings panel.

In the Transaction Type panel, specify which transactions the report includes. You can select specific transaction types by clicking in the individual boxes to the left or you can select all transaction types by clicking in the box to the left of the Transaction Type heading.

The Sorting Options panel lets you specify how the transactions are displayed:

- Date
- Door Name
- Direction
- Card #

► *Cardholders, Optional Fields*

This form is used to specify which cardholders are included in the report. This can be a single cardholder, a group of cardholders, or all cardholders.

List cardholder(s) with specified First Name.

List cardholder(s) with specified Last Name.

Search for cardholder(s) based on Card Type

- All Cards
- Temporary Cards
- Archived Cards

List cardholder(s) with specified Batch Number.

List cardholder(s) with specified Card Number.

List cardholder(s) with specified Personal Identification Number.

List cardholder(s) in specified (Door) Group.

List cardholder(s) in specified Elevator Group.

In Exceptions specify:

- Do Not List
- List At End

If cardholders are included in the report, the selected fields in the Include Card Fields window are included with the cardholder information.

Include Card Fields, select if any of these fields are to be listed on the report with cardholder information.

When selected, Include Deleted Cards lists cards deleted from the system.

Additional Cardholder Information

Search for cardholders using the Additional Information fields. Entries must have

been previously made in the Additional Card Holder Information fields to a perform search.

- Telephone Number
- Telephone Extension
- Fax Number
- Email Address
- Card Location
- Parking Spot
- Car Plate #
- Bar Code

Optional Cardholder Information

Search for cardholders using the Optional Information fields. Optional fields must have been defined and entries must have been previously made in the Optional Card Holder Information form to perform a search.

Clicking on the Find Cards button displays cardholder records based on the specified criteria.

Clicking on the Clear button clears all cardholder records from the cardholder record window.

►Devices, Direction

This form is used to specify an individual device, a group of devices, or all devices for either doors, elevators, auxiliary inputs, and supervised inputs.

The Door List panel lets you specify which door(s) the transaction report includes. You can select specific doors by clicking in the box to the left of the Unit ID column or click in the box to the left of Door List to select all doors.

The Elevator List panel lets you specify which elevator(s) the transaction report includes. You can select specific elevators by clicking in the box to the left of the Unit ID column or click in the box to the left of Elevator List to select all doors.

The Auxiliary Inputs List panel lets you specify which auxiliary inputs the transaction report includes. You can select specific inputs by clicking in the box to the left of the Unit ID or click in the box to the left of Auxiliary Inputs List to select all auxiliary inputs.

The Auxiliary Outputs List panel lets you specify which supervised outputs the transaction report includes. You can select specific auxiliary outputs by clicking in the box to the left of the Unit ID column or click in the box to the left of Auxiliary Outputs List to select all auxiliary outputs.

The Supervised Inputs List panel lets you specify which supervised inputs the transaction report includes. You can select specific supervised inputs by clicking in the box to the left of the Unit ID column or click in the box to the left of Supervised Inputs List to select all supervised inputs. Requires Supervised Input Board.

The IO Description panel lets you specify which inputs/outputs the transaction report includes. You can select specific I/Os by clicking in the box to the left of the Unit ID column or click in the box to the left of IO Description to select all doors. Requires special hardware.

The IOCB Inputs panel lets you specify which inputs/outputs the transaction report includes. You can select specific IOCB Inputs by clicking in the box to the left of the Unit ID column or click in the box to the left of IOCB Inputs to select all doors. Requires IOCB1616 circuit boards.

The Direction panel is for a controlled enter/exit environment where readers are on both sides of doors. Specify a direction by clicking inside the appropriate radio button, otherwise leave the default setting on All.

Procedures

► *Name, Format, Run, and Save a Report*

1. From the main screen, select the Transaction Reports quick button.
 - To name and run a report, continue to the next step.
 - To run a one time report, go to step 4.
2. From Report Options form, click on the Add New button at the bottom of the form.
3. Enter a name for the report in the Report Name text box.
4. Select the Date Options and Other Settings tab if that form is not open.
5. From the Date Options and Other Settings, specify the Date Option, and the relevant dates, the Transaction Types and the Sorting Option.
6. Select the Card Holders, Optional Fields tab at the top.
7. From the Card Holders, Optional Fields form, select the appropriate criteria.
 - If you want all cardholders listed, do not specify any criteria.
 - Use the Clear button to reset cardholder criteria.
8. If you specified cardholder criteria in step 6 or you want all cardholders listed in your report, click on the Find Cards button.
 - If you do not want any cardholders in your report, do not click on the Find Cards button.
9. Select the Devices, Direction tab at the top of the form.
10. From the Devices, Direction form, specify those devices to be included in the report.
11. If you are running a one-time report, by-pass saving it. If you named the report and wish to retain the format, click on the Save button at the bottom.

12. Click on the Run Report button to view the report in the Report Previewer.
13. Click on the Exit button to return to the Report Options form.

► *Save a Report In PDF Format*

You must first format the report or have an existing report before you can save it in PDF format.

1. From the main screen, select the Transaction reports quick button.
2. From within any of the Transaction Report forms, click on the Report Name down arrow and select the report.
 - If you have not named the formatted report, by pass this step.
3. Click on the Run Report button.
4. Click on the Export to PDF button from the Report Preview window.
5. From the Select a PDF export file dialog box, name the file and specify a file folder.
6. Click on the Save button.
7. Click on the Exit button in the Keyscan Report Previewer to return to the Report Options form.

► *Save a Report in CSV Format*

You must first format the report or have an existing report before you can save it in CSV format.

1. From the main screen, select the Transaction Reports quick button.
2. From within any of the Transaction Report forms, click on the Report Name down arrow and select the report.
 - If you have not named the formatted report, by pass this step.
3. Click on the Run Report button.
4. Click on the Export to CSV button from the Report Preview window.
5. From the Select a PDF export file dialog box, name the file and specify a file folder.
6. Click on the Save button.
7. Click on the Exit button in the Keyscan Report Previewer to return to the Report Options form.

► *Print a Report*

You must first format the report or have an existing report before you can print it.

1. From the main screen, select the Transaction Reports quick button.

2. Click on the Report Name down arrow and select the report.
 - If you have not named the formatted report, by pass this step.
3. Click on the Run Report button.
4. From the Report Preview window, click on the Print icon near the bottom of the window.
5. From the print dialog box, specify the Print range and Number of copies.
6. Click on the OK button or the Print button.
7. Click on the Exit button in the Keyscan Report Previewer to return to the Report Options form.

▶ *Delete a Report*

1. From the main screen, select the Transaction Reports quick button.
2. From any of the Transaction Report forms, click on the Report Name down arrow and select the report to be deleted.
3. Click on the Delete button near the bottom of the form.
4. From the Delete Report warning box, click on the Yes button.
5. Click on the Exit button.

Related Topics

▶ *Schedule & Email a Report*

▶ *Keyscan Report Previewer*

▶ *Cumulative Hours Reports*

Schedule/Email a Report

The Schedule Report form allows you to schedule when a formatted report is run and email it. The report is emailed as a PDF file.

Procedure

▶ *Schedule and Email a Report*

You must have a named report to use the Schedule/Email a Report feature.

1. From the main screen, select the Transaction Reports quick button.
2. From the Transaction Report form, click on the Report Name down arrow and select the report.
3. Click on the Schedule button in the lower left corner.
4. If the report is to be emailed, enter the address in the Email Address text

box.

5. To set the time when the report is run, in the Schedule Time box, select the 00 representing the hours and either type hours or use the up and down arrows to set the hours.
6. Repeat to set the minutes.
7. In the Select the Day(s) of the Week panel, click in the box(es) to the left of the appropriate day(s).
8. Select either Print & Email Report or Email Report Only. If you are only scheduling the report to be printed, select the Print & Email Report option and do not enter an email address.
9. Click on the Save & Exit button.
10. Click on the Exit button to return to the main screen.

Keyscan Report Previewer

The Keyscan Report Previewer allows you to preview reports in the System VII Client. You can also print reports or save them in PDF or CSV format.

Overview

► *About the Keyscan Report Previewer*

Use the Back and Forward buttons to scroll through a multi-page report. In the centre of the scroll bar to the right are two sets of numbers divided by a slash mark - 12/29. The first numbers indicate the current page you are viewing in the report and the last numbers indicate the total number of pages in the report.

To change the View, click on the down arrow to the right of the magnifying glass on the toolbar and select a view option from the pop-up menu.

To search for words or phrases in the report, click on the Search button. Enter the word or phrase in the Keyscan Search Text Preview text box. Click on the OK button or press the Enter key. The first occurrence of the word or term is underlined in red. To highlight the next occurrence of the word or phrase, press the Enter key again. The next occurrence of the word or term is underlined in red.

To Print a report, click on the Printer icon on the far right of the toolbar.

To save the report as an Adobe Acrobat PDF file click on the Export to PDF button.

To save a report as a CSV (Comma Separated Value) file, click on the Export to CSV button.

To close the Keyscan Report Previewer, click on the Exit button.

Related Topics

► *Transaction Reports*

Utilities

System Log

The System Log Entries form, accessed from the Utilities menu, lists entries and actions made by system users based on the level set in the System Logging Level field on the Site Information form. Each entry specifies the date, the user, the log entry, the site, and the computer. The form is designed to allow you to perform searches, organize entries by field, export entries as CSV files, print or save as PDF files, and clear the entries.

Procedures

► *Search by Date Range, User ID, or System Log Entries*

You can use the Search feature to find specific system log entries by selecting one or a combination of the following search criteria:

- Date Range
- User ID
- System Log Entries

To Search for System Log Entries

1. Click in the appropriate Search by box. You can select any combination.
2. Enter or select the appropriate criteria in the search fields:
3. For User ID - Type the user's log on name.
4. For Date Range – Click on the From down arrow. Use the arrows at the top of the calendar to scroll to the month. Click on the date in the calendar. Repeat for the To date.
5. For System Log Entries - Type the name of the system entry field.
6. Click on the Search button.

► *Organize System Log Entries*

The System Log Entries can be organized based on the Date, starting from the most recent entry to the oldest entry, or by User ID, System Log Entry, Site ID, or Computer # in alpha/numeric order.

To organize entries by Date, User ID, System Log Entries, Site ID, or Computer #, click on the heading in the Title Bar. To reverse the order, click on the same heading in the Title bar.

► *Export History (CSV files)*

For archival purposes, you can export system log entries. The System VII software saves the system log entries as CSV files, which can be opened in most spreadsheets. By default, CSV files are saved in the Keyscan System VII directory in the following file name and format: System Log - Year - Month - Day.CSV.

To Save System Log Entries

1. From the main screen, select the Utilities menu > View System Log.
2. From the System Log Entries form, select the Export History button.
3. From the Export System Log dialog box, click on the OK button.
4. From the Export System Log Export Completed confirmation box, click on the OK button.
5. From the System Log Entries form, click on the Exit button to return to the main screen.

To Open a CSV file (System Log File)

1. Open the spreadsheet application.
2. From the File menu, select Open.
3. From the Files of Type box, click on the down arrow and select the CSV file format.
4. Navigate to the Keyscan System VII directory.
5. Select the System Log XXXX.CSV file
6. Click on the Open button.

► *Print System Log Entries*

1. From the main screen, select the Utilities menu > View System Log.
2. From the System Log Entries form, click on the Print Listing button.
3. From the Keyscan System VII Report Previewer, click on the Printer icon.
4. From the main screen, select the Utilities menu > View System Log.
5. Click on the OK button.
6. Click on the Exit buttons until you return to the main screen.

► *Save System Log Entries as PDF files*

1. From the main screen, select the Utilities menu > View System Log.
2. From the System Log Entries form, click on the Print Listing button.
3. From the Keyscan Report Previewer, click on the Export to PDF button.
4. From the Select a PDF export file dialog box, name the file and specify a file folder.
5. Click on the Save button.

6. Click on the Exit buttons until you return to the main screen.

► *Clear Log Entries*

When you clear the log entries, they are permanently deleted. If you wish to maintain an archival record of system log entries, first, export them. Clearing System Log Entries is based on the site that you are currently logged on to.

To Clear All System Log Entries

1. From the main screen, select the Utilities menu > View System Log.
2. Select the Clear System History button.
3. From the Delete System Log Entries warning box, click on the Yes button.
4. From the second Delete System Log Entries warning box, click on the Yes button.
5. From the Delete System Log Entries confirmation box, click on the OK button.
6. Click on the Exit button to close the System Log Entries form and return to the main screen.

Cardholder Optional Fields

The Card Holder Optional Fields form is used to create the captions for the Optional Card Holder Information form. The 10 fields in the Card Holder Optional Fields form are initially blank. As its heading implies, the Card Holder Optional Fields form allows you to define your own specific information fields. The Card Holder Optional Fields form is accessed from the Utilities menu.

You can also re-define the Additional Cardholder fields from Cardholder Optional Fields form in the same manner as the optional fields.

You can also edit cardholder optional fields at a later date. However, if you change an existing caption, the cardholder data entered under the previous caption remains unchanged. You will have to edit the data for the newly created caption for each cardholder.

When you define the optional fields, you can specify 2 of those fields to be listed on the main Cardholder form by using the Display on First Card Tab function.



From the Optional Cardholder Information form, by right clicking on the text box of any defined Optional Field headings, a list of all entries made in that field is viewable in a drop down box.

Procedures

► *Define Cardholder Optional Fields*

1. Select Cardholder – Optional Fields Setup from the Utilities menu on the main screen.
2. Click in the Optional Field Name # 1 text box on the right side of the Card Holder Optional Fields form and type a caption.
3. Repeat for each subsequent field that you wish to define.
4. Click the down arrow to the right of Display on First Card Tab if you wish to have this field listed on the main cardholder form, and select the optional field.
5. To list a 2nd optional field on the main Cardholder form, click the down arrow to the right of the 2nd Display on First Card Tab, and select the optional field.
6. Click on the Save & Exit button to save the entries and return to the main screen.

► *Delete Optional Fields*

To delete a single caption

1. Select Cardholder – Optional Fields Setup from the Utilities menu on the main screen.
2. Click in the text box of the Optional Field Name to highlight your selection.
3. Press the Delete key on your keyboard.
4. If you had specified an Optional Field Name in either of the Display on First Card Tab boxes, select the Not Assigned option from the drop down list.
5. Click on the Save & Exit button to return to the main screen.

To delete all captions

1. Select Cardholder – Optional Fields Setup from the Utilities menu on the main screen.
2. Click on the Clear All button.
3. Click on the Save & Exit button to return to the main screen.

Photo Shape Setup

The Photo Shape Setup is used in conjunction with the optional Photo Badging module and allows you to specify the height to width ratio of cardholder images shown in the Cardholder Information form, as well as any images printed on reports or cards. Assigning a value to the width alters the image. The width ratio must be between 0.3333 and 3.0 to the height, which is a fixed value.



The factory default ratio of 1.333 is the recommended setting. The image can become distorted if the width becomes too great in relation to the height.

Procedure

► *Change the Photo Shape Ratio*

1. Select Photo Shape Setup from the Utilities menu on the main screen.
2. Click in the Width text box and enter a value.
3. The Image box changes according to the width or ratio value.
4. Click on the Save & Exit button to save the new ratio.
5. From the Save Changes warning box, click on the Yes button.

Default Panel Outputs & Protocols

The Default Panel Outputs and Protocols form allows you to set, edit, or view outputs for power failures, invalid codes, or keypad duress, as well as specify the manufacturer code where a keypad is used without a reader. The Default Panel Outputs and Protocols form is accessed from the Utilities menu.



Your installer or service provider should determine these settings. Please do not change them.

Procedures

► *Assign an Output for a Power Failure*

In the event that an access control unit experiences a power failure (AC) or brown out, you can assign a power failure alarm to an output.

To assign an output for a power failure

1. From the main screen, select the Utilities menu > Default Panel Outputs and Protocols.
2. Click on the down arrow under Unit ID, and select the name of the access control unit.
3. In Panel Feature section, click on the down arrow under Output opposite Output for Power Failure and select an output.
4. Click on the Save & Exit button.

► *Assign an Output for an Invalid Code*

An Invalid Code alarm is triggered when an invalid card has been presented to a

reader more than 5 times or a keypad code has been entered more than five times. An example for the output could be that it initiates a VCR to record activity at the door.

To assign an output for an invalid code

1. From the main screen, select the Utilities menu > Default Panel Outputs and Protocols.
2. Click on the down arrow under Unit ID, and select the name of the access control unit.
3. In Panel Feature section, click on the down arrow under Output opposite Output for Invalid Card/Keypad Code and select an output.
4. Click on the Save & Exit button.

▶ *Assign an Output for Keypad Duress*

An alarm is triggered when a cardholder keys in a "9" before his or her keypad code. The alarm automatically resets after 10 minutes. A typical example for the keypad duress would be to activate a signaling device to a central or monitoring station. If a cardholder is under duress and their normal PIN is *41234#, they would key in *941234#. The door would unlock and activate a duress alarm.

To assign an output for keypad duress

1. From the main screen, select the Utilities menu > Default Panel Outputs and Protocols.
2. Click on the down arrow under Unit ID, and select the name of the access control unit.
3. In Panel Feature section, click on the down arrow under Output opposite Output for Keypad Duress and select an output.
4. Click on the Save & Exit button.

▶ *Set Power Failure Delay*

The Power Failure Delay specifies a period of time to ignore power interruptions before triggering a power failure alarm.

If you do not assign an output for a power failure, do not specify a power failure delay time.

Set Power Failure Delay

1. From the main screen, select the Utilities menu > Default Panel Outputs and Protocols.
2. Click on the down arrow under Unit ID, and select the name of the access control unit.

3. In the Panel Feature section, click on the down arrow under Output opposite Output for power failure and select an output, if you have not done so already.
4. In the Minutes text box opposite Power failure delay, enter a value. The maximum is 99 minutes.
5. Click on the Save & Exit button.

► *Set Manufacturer Codes – WSSKP1 Keypads*

Set Manufacturer Codes WSSKP-1 Keypads

Use the Manufacturer Codes to select the card reader protocols. This feature is used only where WSSKP 1 keypads are installed without a reader present. The Manufacturer Codes have the following two fields with their respective codes:

Default Code

003 132 002 204 - Manufacturer Code Defaults

002 204 000 000 - Manufacturer Code Defaults WSSKP-1



The system default protocol is the Manufacturer Code Defaults. Your installer or service vendor will determine the correct protocols. Please do not change the codes.

Reader Access Level Reports

Reader Access Level Reports can summarize door group access levels, and, if selected, the time zones and holiday schedules for each specified door reader. You can include a listing of active cardholders that belong to each door group in the report as well. Select individual or multiple door readers for your report. You can also save the report as an Acrobat PDF document for non-system users. The Reader Access Level Report excludes elevator readers.

Procedures

► *Create a Reader Access Level Report*

1. From the Client main screen, select the Utilities menu and click on Reader Access Level Report.
2. From the Reader Access Level Report, select the readers by clicking in the box to the left.
3. To display cardholders, click the radio button to the left of Include All Active Cards. You can specify how the cards are displayed by selecting Last Name or Card Number by clicking on the down arrow under Sort By Field.

4. To exclude groups with no access, click in the box to the left of Exclude Groups with No Access.
5. Click on the Run Report button.
6. Select either Yes or No in the Group/Reader Report dialog box, depending on whether you wish to include those details in your report.
7. Select either Yes or No in the Time Zone Details dialog box, depending on whether you wish to include those details in your report.
8. View the report in the Keyscan Report Previewer.
9. Use the Back and Forward buttons to scroll through a multi-page report.
10. To change the View, click on the down arrow to the right of the magnifying glass on the toolbar and select a view option from the pop-up menu.
11. To print a report, click on the Printer icon on the far right of the toolbar.
12. From the print dialog box, specify the Printer, the Print range, and Number of copies.
13. Click on the Print button.
14. Click on the Exit buttons until you are returned to the main screen.

► *Save a Reader Access Level Report as a PDF Document*

1. From the Client main screen, select the Utilities menu and click on Reader Access Level Report.
2. From the Reader Access Level Report, select the reader(s) by clicking in the box to the left.
3. To display cardholders, click the radio button to the left of Include All Active Cards. You can specify how the cards are displayed by selecting Last Name or Card Number by clicking on the down arrow under Sort By Field.
4. To exclude groups with No Access, click in the box to the left of Exclude Groups with No Access.
5. Click on the Run Report button.
6. Select either Yes or No in the Group/Reader Report dialog box, depending on whether you wish to include those details in your report.
7. Select either Yes or No in the Time Zone Details dialog box, depending on whether you wish to include those details in your report.
8. From the Keyscan Report Previewer, click on the Export to PDF button.
9. From the Select a PDF Export File dialog box, click on the down arrow to the left of the Save In box and specify a directory.

10. In the File Name box, enter a name for the PDF document.
11. Click on the Save button.
12. Click on the Exit buttons until you are returned to the main screen.

Cumulative Hours Reports

Cumulative Hours Reports can summarize time intervals between card reads where designated readers establish a controlled enter/exit environment. Readers must be configured in the Set Door and Reader Parameters form so as to accurately monitor all entering (IN) and exiting (OUT) activity of all designated cardholders.

The Cumulative Hours Report lists specified cardholders, and based on a date range, lists the date and time of each IN card read, the date and time of each OUT card read, the time interval between each IN & OUT card read, and the total or cumulative time.

The Cumulative Hours Report is only available if you have the optional System VII - Photo Badging module.



The In reader and the Out reader should both have Anti-passback enabled.

Example of Cumulative Hours Setup

The following is a basic example of a controlled enter/exit environment where Company X requests that all hourly employees use an employee side door whenever they enter or leave the building, be it arriving for work, taking lunch, or leaving for home. The employee door is equipped with two readers:

- Reader A is mounted on the exterior door side and set on direction – IN (marks date and time of entry)
- Reader B is mounted on the interior door side and set on direction – OUT (marks date and time of exit)

An employee arrives for work at 8:30 A.M., leaves the building for lunch at 12:15 P.M., returns at 1:00 P.M. and finishes work for the day at 4:45 P.M. A cumulative hours report summarizes the hours as follows:

Card Number	Cardholder	Direction – In	Direction – Out	Total (hh:mm)
001 – 12345	Edward Smith	mm/dd/yy 8:30	mm/dd/yy 12:15	3:45
001 – 12345	Edward Smith	mm/dd/yy 1:00	mm/dd/yy 4:45	3:45
Total = 7:30				

In the above example employees have access to other reader controlled doors,

however when the cumulative hours report is generated, only the employee side door is specified for the report. All other doors are excluded from the report.

Procedures

► Steps to Run a Cumulative Hours Report

1. From the Client main screen, select the Utilities menu and click on Cumulative Hours Report.
2. From the Report Options form, if it is not currently selected, click on the Date Options and Other Settings tab.
3. In the Date Options field, select one of the available options by clicking in the box to the right.
 - Date Range
 - Last # of days
 - One Day
4. Set the Date Settings and Transaction Times for the report.
5. Select the Cardholders, Optional Fields tab.
6. To list all cardholders, click on the Find Cards button, or for specific cardholders, first specify the pertinent search criteria, and then click on the Find Cards button.
7. Select the Devices, Direction tab.
8. Under Door List, by default, all doors for the logged on site are pre-selected. Click in the box to the left of those doors which are not part of the cumulative hours report to de-select them.
9. Click in the box to the left of the doors you use for summarizing the In/Out activity for your report.
10. Select the Date Options and Other Settings tab.
11. Click on the Cumulative Hours Report button.
12. The Keyscan Report Previewer shows a summary of the cumulative hours for all the specified cardholders:
 - To print a report, click on the print icon
 - To produce a PDF version of the report, click on the Export to PDF button
13. To return to the main screen, click on the Exit buttons.

Door and Input Status

The Door and Input Status form allows you to view the current alarm status of access control units in your system. This includes the door status, auxiliary input status, and supervised input status. The following outlines the status conditions. The refresh button polls the access control unit to list the current status. The Door and Input Status form is accessed from the Utilities menu.

Door & Auxiliary Input Status Legend

- Normal = Clear of an alarm condition
- Alarm Activated = An alarm condition exists
- Shunted = Bypassed

Supervised Input – Shunt Status

- Disarmed
- Manual/Auto
- Disarmed Auto
- Disarmed Manual

Supervised Input – Input Status

- Alarm Activated
- Alarm Short
- Alarm Open
- Normal

Time Zone Status

The Time Zone Status form acts as a diagnostic utility and is used to review the current status of all time zones in your system or view the hours of selected time zones. Time zones have two states: ON or OFF. From this form you can also manually toggle individual or all time zones ON or OFF for a selected access control unit.

- If time zones are toggled ON they remain on until the time zones' next scheduled end time.
- If time zones are toggled OFF they remain off until the time zones' next scheduled start time.

The Time Zone Status form is accessed from the Utilities menu.



You cannot edit a time zone from this form. Be aware that toggling a time zone is altering the time event.

Procedure

► *Toggle a Time Zone ON/OFF*

1. From the main screen, select the Utilities menu > Time Zone Status.
2. Click on the down arrow under Unit ID, and select the name of the access control unit.
3. To toggle time zones:
 - To toggle all time zones, select either the Toggle All On button or the Toggle All Off button
 - To toggle an individual time zone, double click on the time zone to toggle it on or off.
4. Click on the Apply Changes button.
5. Select the Exit button to return to the main screen.

Manual AI Shunt and SI Control

The Manual Auxiliary Input Shunt and Supervised Input Control form allows you to view or manually set specific or all auxiliary and supervised inputs.

The inputs are in one of 2 states:

- Normal Status – no manual overrides applied and the point is armed
- Disarmed Status – a user applied override shunt or bypass applied to the point

The Manual Auxiliary Input Shunt and Supervised Input Control form is accessed from the Utilities menu.

Procedures

► *Set Inputs to Normal or Disarmed Status*

Set Individual Inputs – Normal or Disarmed

1. From the main screen, select the Utilities menu > Manual Aux. Input Shunt and Supervised Input Control.
2. If it is not displayed, click on the down arrow under Unit ID and select the access control unit. Wait for the Processing Communication Request box to close.
3. Double click on the specific input. Each double click on the input toggles the setting.
4. Click on the Apply Changes button. Wait for the Processing Communications Request form to update the panels. It closes automatically when communication is completed.
5. Click on the Exit button.

Set All Inputs – Normal or Disarmed

1. From the main screen, select the Utilities menu > Manual Aux. Input Shunt and Supervised Input Control.
2. If it is not displayed, click on the down arrow under Unit ID and select the access control unit. Wait for the Processing Communication Request box to close.
3. Under the appropriate input, Auxiliary or Supervised, click on the Set All to Normal Status or Set All to Disarmed Status.
4. Click on the Apply Changes button. Wait for the Processing Communications Request form to update the panels. It closes automatically when communication is completed.
5. Click on the Exit button.

IOCB1616 Shunt Control Status

The IOCB1616 Shunt Control Status form allows you to view or manually set specific or all inputs on the associated IOCB1616 circuit boards. The following defines the input state as per the status column:

Shunt Status

- Normal Status – no manual overrides apply and this point is armed
- Disarmed Status – a user applied shunt or by-pass applied to the point

Auto Status

The input is set to a time zone.

- Normal Status – time zone is off
- Disarmed Status – Auto – the time zone is on

Input Status

- Normal Status – the input circuit is closed
- Alarm Activated – the input circuit is open



Please note that an input's shunt status overrides its auto status.

The Set All to Normal Status and Set All to Disarm Status only changes the Shunt Status and applies the changes to all IOCB1616 circuit boards connected to the specified under Unit ID.

After changing settings in the software, you must select the Apply Changes button to institute those changes at the circuit board level.

IOCB1616 Output Control Status

The IOCB1616 Shunt Control Status form allows you to view or manually toggle specific or all outputs on the associated IOCB1616 circuit boards.

The Output is in one of the following conditions as indicated in the IOCB Output Status column:

- On
- Off

To toggle an output point, either click in the box to the left under Output # for a specific output or use Toggle All On or Toggle All Off buttons.

Automatic/Manual

- Automatic – no manual condition has been set for the output
- Manual – the user has changed the state and is in control of the output

IOCB Current Status

- indicates the current condition of the output on the IOCB1616

IOCB Automatic Status

- indicates the condition of the output after selecting the Apply Changes button.



After changing settings in the software, you must select the Apply Changes button to institute those changes at the circuit board level.

Manual Output Control

The Manual Output Control form allows you to view or manually toggle individual or all auxiliary outputs to an ON or OFF state providing you do not have an input assigned to an output. The Manual Output Control form is accessed from the Utilities menu.

Procedure

► *Toggle Individual or All Auxiliary Outputs*

To Toggle Individual Outputs

1. From the main screen, select the Utilities menu > Manual Output Control.
2. If it is not listed, click on the down arrow under Unit ID and select the access control unit. Wait for the Processing Communication Request to close.
3. Under the appropriate output, click in the box to the left.

- OFF
 - ON
4. Click on the Apply Changes button. Wait for the Processing Communications Request form to update the panels. It closes automatically when communication is completed.
 5. Click on the Exit button.

To Toggle All Outputs

1. From the main screen, select the Utilities menu > Manual Output Control.
2. If it is not listed, click on the down arrow under Unit ID and select the access control unit. Wait for the Processing Communication Request to close.
3. Click on the Toggle All On or Toggle All Off button.
4. Click on the Apply Changes button. Wait for the Processing Communications Request form to update the panels. It closes automatically when communication is completed.
5. Click on the Exit button

Elevator Floor Control Status

The Elevator Control Status form shows the current status of each elevator floor button and allows you to manually override individual or all elevator floor buttons. Floor buttons are in one of the following 3 states:

SECURED – The floor is secure and a valid card is required to activate the floor button.

UNSECURED – The floor is unsecured and a valid card is not required to activate the floor button. If an elevator button is manually set to unsecured, it remains so until either, it is manually toggled to secured or, if applicable, when its automatic re-lock time starts as set in the Set Elevator Time Zones to Automatically Lock/Unlock Floor Buttons form.

TIMED UNLOCK – The floor is unsecured for a specified period of time. The maximum period is 7 days for a timed unlock. At the conclusion of the timed unlock, the elevator floor button is secured.



Please be aware of a timed unlock applied to an elevator floor button that has been programmed to automatically lock/unlock on a time zone. If the timed unlock expires after the start of an auto unlock period, the floor button remains secured until the next programmed auto unlock start time.

Procedures

► *Manually Toggle Elevator Floor Buttons – Secured or Unsecured*

1. Select Elevator Control Status from the Utilities menu on the main screen.
2. Click on the down arrow under Unit ID, and select the name of the elevator control unit.
3. Do one of the following steps:
 - To Toggle All Floor Buttons - Select either the Toggle All On (Secured) button or the Toggle All Off (Unsecured) button.
 - To Toggle Individual Floors – Left click on elevator floor to turn specific floor buttons ON or OFF.
 - To apply a Timed Unlock, right click on the elevator floor, specify the date and time in the Unlock Floor Until field, and select Apply Timed Unlock.
4. Select the Exit button to return to the main screen.

Reset Anti-Passback

In a controlled enter/exit environment, where the anti-passback option is in effect, the Keyscan system maintains an in or out status for each cardholder. When anti-passback is reset, the card can be used at an IN or OUT reader on its next reader presentation before it is again governed by the IN/OUT anti-passback protocol.

If you were to check the Card In/Out Status report in the Utilities menu, cards are still listed as In or Out based on their last transaction after anti-passback is reset.

You can reset anti-passback for a single card, multiple cards, or all cards.

Procedure

► *Reset Anti-passback*

1. Select Reset Anti-passback from the Utilities menu on the main screen.
2. If you are resetting anti-passback for all cardholders, go to the next step. If you are resetting anti-passback for one or some cardholders, select those cardholders in the list:
 - for a single cardholder, select the cardholder
 - for consecutive cardholders, select the first cardholder, hold down the Shift key and select the last cardholder
 - for non-consecutive cardholders, hold down the Ctrl key and select the cardholders.
3. Click on the Reset button.
4. In the Reset Anti-passback warning box, select either:

- Yes - for resetting highlighted cardholders
 - No - for resetting all cardholders
5. If you selected No in the previous step, in the Reset Anti-passback warning box, select Yes.
 6. Anti-passback is reset and the Reset Anti-passback window closes.

Related Topic

▶ *Set Door and Reader Parameters*

Card In/Out Status

The Card In/Out Status form allows you to view the current status of all or selected cardholders for a specific site. This form is particularly useful for generating a snapshot of who is in or out of the building on sites that have controlled enter/exit portals or determining the last transaction of individuals in a building.

The status of each cardholder is listed by the following headings:

- First Name – the cardholder’s first name
- Last Name – the cardholder’s last name
- Card Number – the batch number and card number assigned to the cardholder
- Direction – the direction of the card based on the reader and door configuration (unknown indicates an
- Count – the remaining number of times a temporary card can be used if it was assigned a limited number of uses.
- Status – the card status field is blank for active cards or archived for archived cards
- Date & Time – the date and time of the cardholder’s last transaction
- Device Name – the location of the cardholder’s last transaction
- Unit ID – the ACU that regulates the named device
- Site ID – the name of the site where the transaction occurred

The information listed under each heading can be manipulated so it is cited as follows:

- Alphabetical listings – A to Z or Z to A
- Numerical listings – lowest to highest or highest to lowest

Procedures

▶ *Display Card Status*

1. Select Card In/Out Status from the Utilities menu on the main screen.
2. If applicable, and you have authority to view multiple sites, click on the down

- arrow to the right of Site Name, and select a site or all sites from the drop down list.
3. Click on the down arrow to the right of Unit ID and select either a specific access control unit or All Panels depending on your search criteria.
 4. Specify dates using one of the following options:
 - Search Last # of Days – click on the down arrow to the right and select the previous number of days where the report starts.
 - Specify From and To dates – select the down arrow to the right of From . Use the arrows to scroll to the month and click on a day in the calendar. Repeat for setting the To date.
 5. To narrow or refine your search even further, use the cardholder information fields to filter your criteria.
 - General Cardholder Information
 - Additional Cardholder Information
 - Optional Cardholder Information
 6. From the Include Card Fields list, select any applicable fields you wish included in your Card In/Out Report.
 7. Click on the Find Cards button. To print a report, continue with the next steps or to return to the main screen, click on the Exit button.
 8. To preview a report that lists cards based on a specific direction, click on the down arrow to the right of Print Direction and select a direction mode from the drop down list:
 - All – prints all listed cards
 - In – prints only In cards
 - Out – prints only Out cards
 - Unknown – prints only Unknown cards
 9. Click on the Print button.
 10. From the Keyscan Report Previewer, click on the printer icon.
 11. From the Print dialog box, select a printer, if necessary, select a Print Range option, and specify the Number of copies.
 12. Click on the OK button.
 13. Click on the Exit button to close the Keyscan Report Previewer.
 14. Click on the Exit button to close the Card In/Out Report and return to the main screen.

► *Manipulate Listings Under a Specific Heading*

You must have performed a search with cardholders listed in the table to manipulate the order.

- Click on the heading in the Title Bar.
- Click on the same heading in the Title Bar to reverse the order of the listings.

Alarm Notification

The Alarm Notification can be set to one of two states:

- ON - Alarm Notification has a check mark
- OFF - Alarm Notification is unchecked

Alarm Notification is accessed from the Utilities menu.

When Alarm Notification is active, an Alarm Warning dialog box opens to inform the system user that an alarm event has been triggered. Alarm Warning dialog boxes open whether the Client is the active application on the desktop or it has been minimized.

Displaying Online Transactions

The Keyscan software adds to an internal log any transactions that have occurred within the last two minutes listing up to a maximum of 100 entries. The system automatically clears the 101st entry. The Online Transactions form allows you to view system activity and sort information by using filters to highlight specific transactions. The Display Online Transactions form is accessed from the Utilities menu or from the Display Online Transactions quick button.

Select the GMT (Greenwich Mean Time) time zone to view current on line transactions for remote panels or sites if they are in a different time zone from the monitoring location. If the remote panels or sites are in the same GMT time zone as the monitoring location, by default, the software sets the appropriate GMT time zone.

Procedures

▶ *Sort Transactions Using Filters*

1. Specify the field to filter by selecting the heading in the title bar of the Online Transactions form.
 - For Transaction Type or Device Name, specify the fields to filter by clicking in the box to the left, then select Exit .
 - For all Unit ID, Batch, Card, First Name, Last Name and Direction, type the filter criteria in the text box, and then select OK. As an example, to filter all cardholders with a last name that starts with the letter C, type C in the text box.
2. To reset a heading that has already been filtered, click on the title bar, then

the Yes button warning box to clear the current filter.

Related Topics

▶ *Set Show Photos*

Show Photos

The Show Photos form displays a photo and the transaction details whenever a cardholder presents a credential at a reader. The Show Photos form has a number of configuration options including a history window. The history window can be set to retain photos of the last 10 active cardholders.

You must be in the Online Transaction form, to access the Show Photos function.



The Show/Hide Photos feature only works if you have the optional System VII Photo Badging software module, and you have inserted images in each cardholder record.

Procedures

▶ *Set Show/Hide Photos*

1. To access the Show Photos function, select the Display Online Transactions quick button > Show Photos button.
2. To set the number of history windows, click on the Photo Settings menu > Change Display Layout and select the number of History Windows on the Show Photos form.
3. To change the alignment of the history windows, click on the Photo Settings menu > Align History Windows and select an option:
 - Left
 - Right
4. If you do not want history windows displayed, click on No History Window.
5. To keep the Show Photos form on top, select the Photo Settings menu > Window Always On Top. The Online Transactions window must be open or minimized. If the Online Transactions window is closed, the Show Photos form closes.
6. To close the Show Photos form, click on the Photo Settings menu > Close Photo Window.

Related Topics

▶ *Display On-line Transactions*

Display Software Connections

The Display Software Connections form lists any PC currently logged into the Keyscan database with any open Keyscan System VII application. The form identifies the name of the PC, the open Keyscan application and the date and time the application established a connection with the database. The Display Software Connections form lists the following open Keyscan applications:

- Keyscan System VII - Client Version x.x.x
- Keyscan System VII - Communication Service Version x.x.x
- Keyscan System VII - Template Editor Version x.x.x

Where multiple sites exist, the Display Software Connections form displays all open Keyscan applications on all sites regardless of the system user's authority levels.

Procedures

To open the Display Software Connections window, from the main screen, select the Utilities menu > Display Software Connections.

Select the OK button to close the Display Software Connections window.



Users must exit the Keyscan application in order to disconnect from the database, otherwise the database will indicate that the user is still operating with an open application.

CCTV

Setting Up CCTV

Setup a CCTV System

The optional System VII CCTV Integration module is designed to integrate with a closed circuit television system. The System VII CCTV module is compatible with the following platforms:

- DVRs (supported manufacturers only)
- RS-232 camera systems

Depending on your specific configuration, before you begin to setup your CCTV system in the System VII software, you must first install any video related software drivers for devices such as a video bus or video capture board. You may require camera or switcher manufacturer's literature for command and communications settings.

DVR Pre-configuration

If you are integrating System VII with DVRs, please observe the following DVR pre-configuration steps.

- Setup a valid IP Address, Gateway & Subnet Mask for each DVR. Make sure that you write down the IP Address for later use in the System VII Client software.
- Use the DVR viewer to connect to each unit.
- Once connected, you must create a new user. This user must have the same user name and password that is used to log on to the System VII software.
- When you have entered and saved the user name and password, return to the System VII Client.



Other factors that may affect operation are as follows: (a) enable web browsing, (b) security levels per camera point, (c) recording on event - Keyscan recommends 24/7 recording.

System VII CCTV Forms

After you have installed any necessary device drivers and/or acquired the necessary IP addresses and passwords as outlined above, setting up CCTV from within System VII involves completing 3 forms as listed below. You will note that the CCTV Action Setup & Email Notification is listed as optional. You can monitor the CCTV cameras without completing this form however, you will not be able to use the powerful automation and report CCTV linking features. Click on the links below for details on each form and step-by-step instructions.

Related CCTV Topics

▶ *CCTV Type Setup - required*

- ▶ *CCTV Command Setup - required*
- ▶ *Show Live Video - confirms CCTV connections*
- ▶ *CCTV Action Setup & Email Notification - optional*

CCTV Type Setup

This form is used to identify the DVR or switcher/matrix manufacturer and input the manufacturer's camera setting commands.

Switcher/Matrix

If you are setting up for a switcher/matrix, you will have to consult with the manufacturer's documentation for camera and display mode setting commands.

DVR

If you are setting up a DVR, you can only set up a supported DVR. You can contact Keyscan or visit www.keyscan.ca for supported DVR brands. When completing the CCTV Type Setup Form, you have to pick the CSV file of the supported DVR manufacturer to load the camera settings. The CSV files are identified as follows:

- *ManufacturerKeyscanDVR.csv*

You must also have obtained an IP address for each DVR and applicable Gateway and Subnet Mask.

Procedure

▶ *Steps To Complete the CCTV Type Setup - DVR*

1. From the main screen, select the System settings menu > CCTV Setup/Email Setup
2. From the CCTV Setup/Email Setup form, select the CCTV Type Setup tab to ensure this is the active form.
3. Click on the Add New CCTV Type button.
4. In the CCTV Type text box, enter the name of the DVR manufacturer.
5. Click on the Save button.
6. Ensure that the DVR manufacturer's name you just entered is listed in the CCTV type text box. If not click on the down arrow to the right and select it from the list.
7. Click on the Import CCTV Command button.
8. From the Keyscan Import CCTV Command File box, select the appropriate DVR driver. Drivers are identified as manufacturerKeyscanDVR.csv files.

9. Select the Open button. The camera commands are automatically inserted in the table.
10. Scroll down the table until you see the [Manufacturer] IP Address field.
11. Double click on the [Manufacturer] IP Address
12. In the Setting Command text box, enter the IP address assigned to the DVR.
13. Click on the Save button.
14. If you have more than 1 DVR of the same brand/manufacturer click on the Add New Setting Description button, otherwise go to step 19.
15. In the Setting Description text box, enter the same description as the IP Address was described in step 12, plus a space and the number 2.
16. In the Setting Command text box, enter the IP Address of the second DVR.
17. Click on the Save button.
18. If you are adding another DVR, repeat steps 14 to 17.
19. When the CCTV Type form is completed, go to the CCTV Command setup form instructions.

► *Steps to Complete the CCTV Type Setup - Switcher/Matrix*

1. From the main screen, select System Settings > CCTV Setup.
2. By default the CCTV Setup/Email Setup opens to the CCTV Type Setup form. Select the CCTV Type Setup tab if it is in view.
3. Click on the Add New CCTV Type button.
4. In the CCTV Type text box, enter the name of the video multiplex manufacturer.
5. Click on the Save button.
6. Under Settings is a list of Display Camera #s from 1 to 16, camera display modes, and camera commands. Double click on Display Camera #1. This assumes you are entering the first camera.
7. Display Camera # 1 is listed in the Setting Description text box. In the Setting Command text box, enter the setting command found in the switcher manufacturer's literature. This assumes that you have connected Display Camera # 1 into port #1 on your switcher. For dealers/service vendors, you may use the Import CCTV Commands to import a CSV file to load camera commands.
8. Click on the Save button.

9. To add another camera or set display and zoom modes, repeat steps 6 & 7.

CCTV Command Setup Form

After you have completed the CCTV Type Setup form, complete the CCTV Command Setup form to set communications.

You must have completed the CCTV Type Setup form before you can complete the procedures below.

Procedures

► *Steps To Complete the CCTV Command Setup Form - DVR*

1. Select the CCTV Command Setup tab.
2. Click on the down arrow to the right of CCTV Type and select the DVR manufacturer entered in the CCTV Type Setup form.
3. Click on the down arrow to the right of Driver Options and select the DVR manufacturer.
4. Click on the Save Default Setup button.

► *Steps To Complete the CCTV Command Setup Form - Switcher Matrix*

1. Click on the CCTV Command Setup tab.
2. Click on the down arrow on the right side of CCTV Type and select the switcher/matrix manufacturer's name from the drop down list.
3. Click on the down arrow on the right side of CCTV Port and select the port number from the drop down list that the switcher is connected to on the client PC.
4. Click on the down arrow under Drive Option and select the switcher or camera driver from the drop down list.
5. Click on the down arrow under CCTV Baud Rate and select the correct setting from the drop down list. Consult with the switcher/matrix manufacturer's literature for specifications.
6. Repeat for CCTV Parity, CCTV Data Bits, and CCTV Bits. Consult with the switcher and camera manufacturer's literature for specifications.
7. Click on the Save Default Setup button.

Show Live Video

The Show Live Video function will confirm that your settings are correct by displaying a live, on-screen video feed. Review Verify Live Video below.

Once you have established video connections are properly interfaced with the

System VII CCTV module, to use Vantage's CCTV camera automation for alarms and email, click on the CCTV Action Setup & Email Notification link on the left and follow the directions. If you are only monitoring the CCTV cameras from the System VII software, you do have to complete CCTV Action Setup & Email Notification. This is an optional feature.

If you can't establish a video connection, see Potential DVR Connection Problems below.

Procedures

► *Verify Live Video*

1. From the Client main screen, click on the Show Live Video quick button. The video feed is shown in the Video Stream window. For DVRs, if you don't have an image, click on the down arrow to the right of DVR Connection and select the appropriate IP address
2. Depending on the CCTV configuration, if there are multiple cameras in the system, select the buttons in the Camera Selection Control panel to view the video feed from each camera. Button numbers correspond to the display camera number assigned in the CCTV Setup form.

Potential DVR Connection Problems

If you don't have a video feed displayed in the System VII Video Control panel, review the following DVR & network configuration issues that may be causing connection difficulties. These are general guidelines to troubleshoot connection problems and do not necessarily apply to all makes of DVRs.

- An invalid address. Verify you have valid IP, Subnet Mask and Gateway addresses.
- The network port is closed because of Firewall Security or in the DVR setup. Ensure DVR remote ports are factory set and not customized and DVR settings, such as web browsing, are enabled at DVR interface.
- DVR is not set for 24/7 camera recording. This produces a blank screen if cameras set for motion recording. Ensure DVR is set to 24/7 recording.
- User password may not have authority to setup the DVR
- The DVR user ID and password are not the same as the System VII user ID and password. Ensure the user ID and passwords are the same for the DVR and the System VII software.
- User ID or password entered incorrectly. Passwords and in some cases user IDs are case sensitive. Ensure user ID and password have been entered correctly.
- You are logged on to the DVR and System VII simultaneously. Log off the DVR and remote connect from the System VII Video Control Panel to the DVR.

Related Topic

▶ *Operate the System VII Video Control Interface*

CCTV Action Setup and Email Notification Form

The CCTV Action Setup and Email Notification form can be used to program the following settings with your CCTV cameras:

- capture still images for specified alarm conditions
- email an alarm message to a recipient address
- email a message with a photo on a selected card transaction

If you do not wish to have your CCTV cameras capture still images for specified alarm conditions, or Email an alarm message to another address, leave this form blank.



The System VII Email Notification only functions when the SMTP Email Settings form has been completed.

Procedures

These procedures apply to DVR and switcher/matrix systems.

▶ *Steps to Set Cameras for Alarm Conditions and Email Notification*

Ensure that you have the appropriate manufacturer selected in the CCTV Type box on the CCTV Command Setup form before proceeding to the steps below..

1. From the CCTV Setup / Email Setup form, click on the CCTV Action Setup and Email Notification tab.
2. From the CCTV Action Setup and Email Notification form, click on the down arrow on the right side of Unit ID and select the ACU model from the drop down list.
3. From the table with the headings # | Device Type | Device Name | Status, double click on the appropriate ACU, door or input the camera monitors.
4. In the DVR IP Address box, enter the IP address if setting actions for cameras connected to a DVR.
5. Click on the down arrow to the right of Camera Number, and select the camera that is monitoring the device.
6. From the Transaction Type table on the left, select the event that will initiate the camera to act on. You may select multiple events.
7. Click on the down arrow on the right side of CCTV Command to Apply field and select the command to be applied when the selected events occur from the preceding step.

8. If applicable, In the Email Address text box, enter an Email address to notify the addressee of the alarm event(s). The Email includes code descriptions as they are listed in the Alarm Event window on the main screen.
9. If applicable, you can enter a command line to shell out to another application that would open on any of the selected alarm events.
10. If you have created maps in the Photo Badge Template Editor, and linked devices to it in the Alarm Response Instructions & Alarm Graphic Locations, click on the down arrow to the right of Load Active Map on Alarm Event if you wish a floor plan to open indicating the location of the alarm.
11. Select the Update CCTV Settings button.
12. To set actions for another camera, repeat steps 2 to 11.
13. Select the Exit button to return to the main screen.

► *Steps to Set Email with Cardholder Selection (CCTV)*

Generally, this function is used with access granted to notify the Email recipient that a cardholder has arrived or entered the premise. After the cardholder presents his or her card at the reader, the system automatically issues an email message with Keyscan System V Message as the subject and the following data:

- Transaction Type / Unit ID / Site ID / Device Name / Card Batch (#) / Card Number / Card(holder) Name / Alarm Date Time

The following outlines the steps to setup Email with Cardholder Selection.

1. From the CCTV Action Setup and Email Notification form, click on the down arrow to the right of Unit ID and select the appropriate access control unit.
2. In the table that lists the # | Device Type | Device Name, double click on the name of the Door.
3. In the Alarm Types panel, click in the box to the left of the Access Granted, or the desired field. You may choose multiple events.
4. Click in the box to the left of Email with Cardholder Selection. If you have cardholder records with photos and the recipient's receiving device is capable of displaying photos, click in the box to the left of Email with Cardholder Pictures to send the cardholder's photo with the email.
5. Click on the Show Email Settings for Cardholder Selection button.
6. Type the recipient's address in the Email Address text box.
7. Type the cardholder's card batch number in the Batch field. (The 3 digit number.)
8. Type the cardholder's card number in the Card Number box. You can enter 5 additional Email addresses with the same or five different cardholders.

9. Click on the Update Email Settings button.
10. To return to the main screen, click on the Exit button.

Operate the CCTV Module

Operate the Video Control Panel

The System VII Video Control Panel provides camera monitoring and control of the CCTV system. Some of the functions may not be available depending on the features of the DVR or switcher/matrix that is interfaced with the System VII CCTV module. Each heading below provides an overview of the functions within that particular panel of the System VII Video Control screen.

The System VII Video Control Panel can remain on the desktop for monitoring when the System VII Client is closed.

Video Stream

- Shows live video based on selected camera(s) in the Camera Selection Control panel and selected screen configuration in the View Control panel
- Window Always On Top ON/OFF - When the System VII Client is open, selecting ON keeps the System VII Video Control Panel on top
- Detail message lists System VII software processes to acquire the video feed from the DVR and indicates Connection Successful or Connection Failed

PTZ Camera Control

- Arrows pan and tilt camera in 8 different directions - left, right, up, down
- Zoom In/Zoom Out adjusts camera field of view
- Pan Speed sets the frames per second rate (higher rate = faster pan speed)
- Tilt Speed sets the frames per second rate (higher rate = faster tilt speed)
- Camera Command Set allows selecting custom DVR presets for returning camera to designated home positions

View Control

- Camera Monitoring buttons - select to view 1 camera, 4 cameras, or 9 cameras in the Video Stream panel
- Display Live returns monitoring to live feed after performing a search
- Details ON/OFF enables or disables viewing DVR video information
- Audio ON/OFF enables or disables audio at System VII Client (Does not disable in DVR. May contravene state or federal laws if audio ON)
- DVR Connection allows switching from DVR to DVR if DVRs are made by the same manufacturer

Video Resolution

- High/Medium/Low sets resolution on System VII Video Control Panel (High offers better image in Video Stream panel, however requires greater PC

resources and network bandwidth. This setting does not have any affect on image quality captured in DVR)

Playback Control

- Date & Time - displays current date and time (yyyy-mm-dd-hh-mm-ss) or sets date and time to retrieve video
- Go to Event - retrieves video from DVR based on settings in the Date & Time field
- Fast Back/Forward/Stop/Fast Forward/Pause buttons are used to control direction of video search

Camera Selection Control

- Selects the active camera for manipulation by the other control functions - the camera number is in bold italic text - 1 - to indicate it is the selected camera in the control panel

Find Video from a Report

When the System VII CCTV module is interfaced with a DVR and you have programmed cameras to respond to specific transaction types, such as Alarm Tripped, you can locate specific video segments by running a Transaction Report. You should be familiar with setting up and running a transaction report before attempting the procedures below.

You must have assigned cameras to transaction types in the CCTV Action Setup & Email Notification form to use this feature.

Procedure

►Steps to Find Video from a Transaction Report

1. From the System VII main screen, select the Transaction Reports quick button.
2. From the Report Options form, ensure the Date Options and Other Settings tab is selected.
3. Click in the box to the left of Transaction Types to clear the list of transaction types. All the check marks are removed.
4. In the Transaction Type list, select the specific type of transactions associated with the camera or cameras.
5. Complete the Date Options and Date Settings based on the time frame of the event.
6. If applicable, select the Cardholders, Optional Fields tab and complete the appropriate fields if cardholders are part of the video search.

7. Select the Devices, Direction tab.
8. De-select all the items in the categories by clicking in the box to the left of each heading. The check marks are removed when disabled. Select the appropriate doors, inputs, outputs, or elevator floors.
9. Select the Run Report button.
10. From the Keyscan System VII Report Previewer, locate the transaction associated with the video segment you are searching for. You can enlarge the report by clicking on the down arrow to the right of the button with the magnifying glass and then selecting a view percentage.
11. Right click on the transaction.
12. From the Show Live Video pop-up, left click inside the box.
13. From the Keyscan System VII Video Control window, enter the date and time of the transaction in the Date & Time field in the Playback Control panel. You may have to drag the Keyscan System VII Video Control window to view the date in the transaction report.
14. If you have more than 1 DVR connected, click on the down arrow to the right of the DVR Connection field and select the IP address of the appropriate DVR.
15. Click on the Go To Event button to retrieve and view the video segment.
16. When you have finished, click on the X in the upper right of the Keyscan System VII Video Control window to close it.
17. Click on the Exit buttons of the open forms until you are returned to the main screen.

Related Topic

▶ *CCTV Action Setup & Email Notification*

▶ *Transaction Reports*

Present3

Present3

Present3 is a card feature whereby presenting an authorized card at a selected reader with 3 consecutive passes either toggles a door lock or toggles a time zone. The benefit is added system flexibility since Present3 allows invoking system controls using a card instead of having to be at a computer with a Client module. Present3 can be used in any of the following applications:

- locking and unlocking doors to secure rooms or areas such as for schools or condominium recreation and leisure facilities etc.
- arming and disarming various points connected to devices such as motion sensors
- locking out other cardholders to prevent false alarms
- implementing a supervisory override to keep staff out
- controlling devices such as lights or HVAC etc.

Present3 modes are per the access control unit. They are not global with CPB-10 connections. Only doors and devices connected to the same access control unit as the target reader are affected.

Assigning who may use Present 3 modes is based on door groups. One or a consecutive range of door groups can be selected.

For cardholders with multiple Door Group Access Level assignments in the General Cardholder Information form, please note the following: Present3 only recognizes the door group assigned under Door Group Access Level A. If this door group is not specified in the Present 3 Group Range, the cardholder cannot use this function.

Using Present3 to toggle a door lock or change a time zone is governed by the door group access level - either 24 hours or during the hours of the assigned time zone.



Keyscan strongly recommends not using the First Person In function with Present3.

Related Topics

▶ *Present3 Modes*

▶ *Using Present3*

▶ *Setting Up Present3*

Present3 Modes

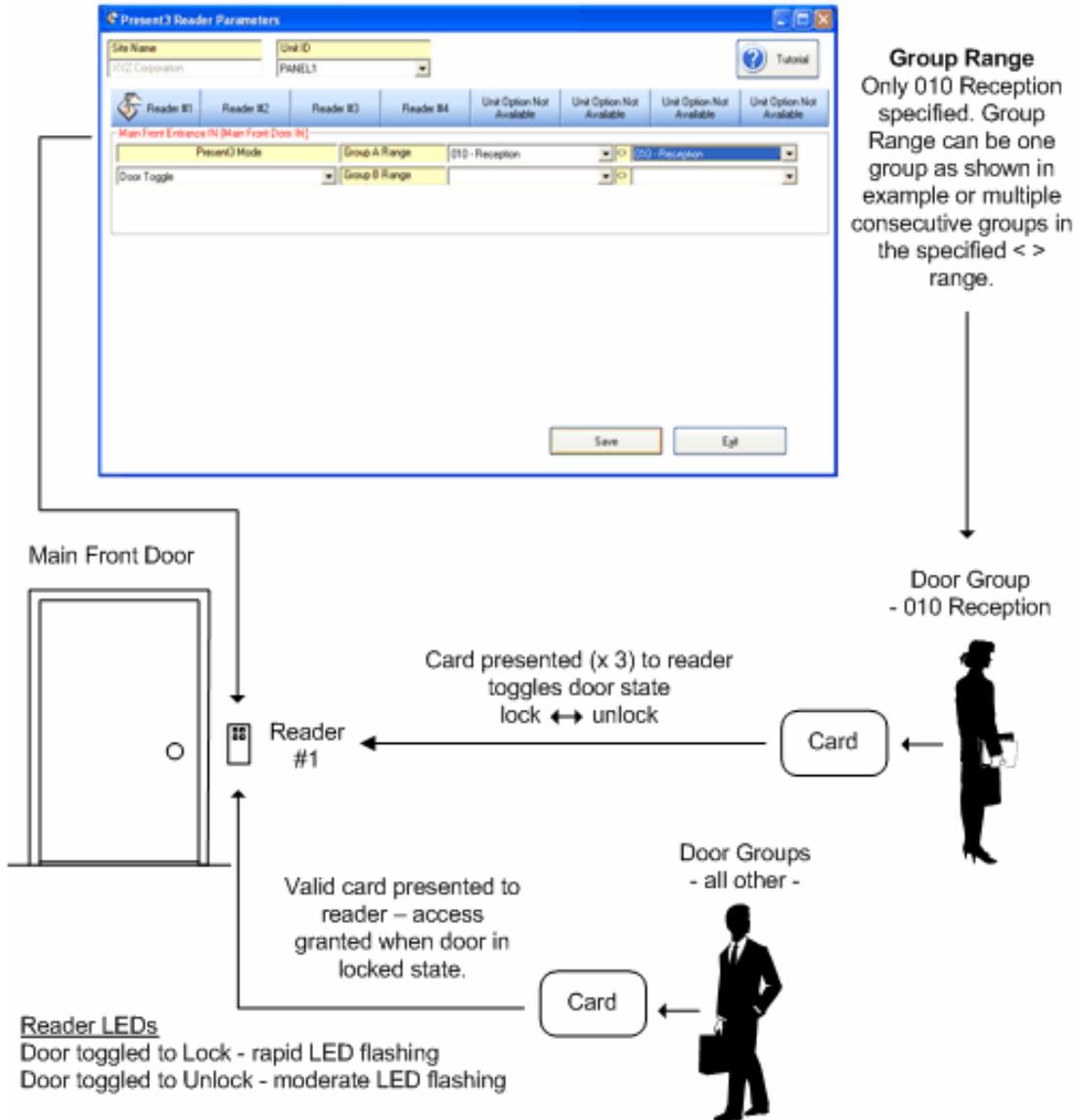
Present 3 has four modes of operation which are defined under the following sub-headings. Diagrams illustrating each Present 3 mode can be accessed by

selecting the green text.

Door Toggle

Door Toggle - toggles the specified reader's door state – lock or unlock. Only cardholders in selected door groups can toggle the door lock. Valid cardholders in other door groups may still access the door with a "single card presentation" when the door has been toggled to its locked state.

► Example of Door Toggle



Time Zone Toggle with Cardholder Lockout

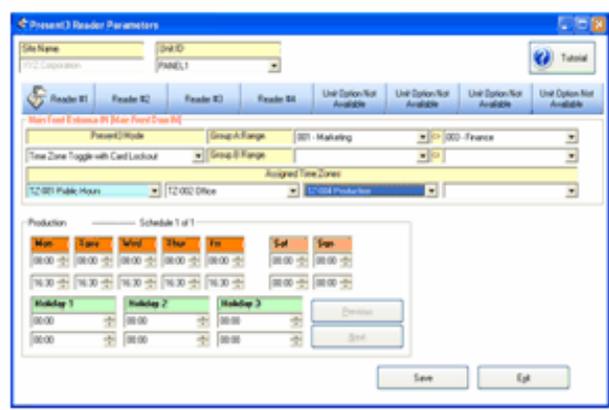
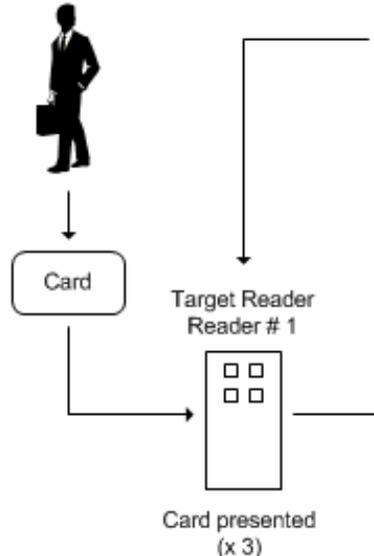
Time Zone Toggle with Cardholder Lockout - toggles specified time zones – ON or OFF – by cardholders in selected door groups at a specified target reader. This

mode affects door group access, doors set on auto unlock/lock, and auxiliary input/shunt and auxiliary output devices that are controlled by the selected time zones.

While Present 3 is in effect and the time zone specified in the left box under Assigned Time Zones in the Present3 Reader Parameters form is toggled OFF, all cardholders in all door groups are denied access with a "single card presentation".

▶ *Example of Time Zone Toggle with Cardholder Lockout*

Door Group Range <>
001 Marketing, 002 Sales, 003 Finance

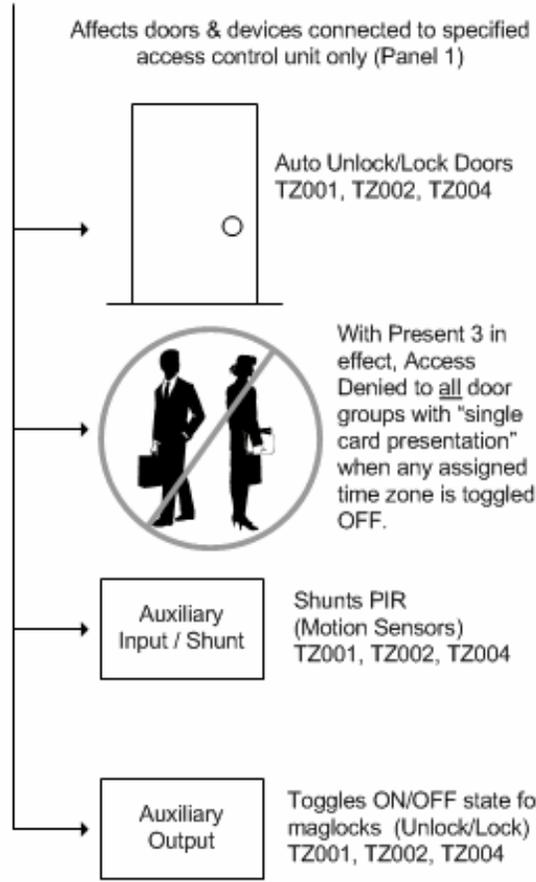


- Toggles Assigned Time Zones ON – OFF
- TZ001 – Public Hours
 - TZ002 – Office
 - TZ004 – Production

Target reader LEDs on Present 3
Time Zone toggled Off - rapid LED flashing
Time Zone toggled On - moderate LED flashing

Present 3 Reader with any Time Zone Toggle
Time Zone programmed or toggled – OFF
repeated cycle – rapid flashing 2 seconds, stops
flashing 5 seconds during OFF period

Group Range can be one group or multiple consecutive groups in the specified Group A or B range.



Time Zone Toggle with Cardholder Lockout and Exit Delay

Time Zone Toggle with Cardholder Lockout and Exit Delay - toggles specified time

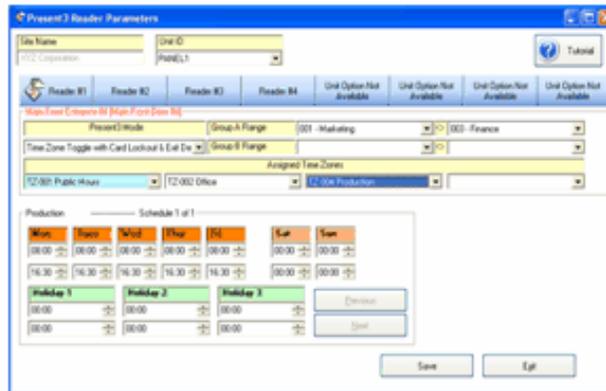
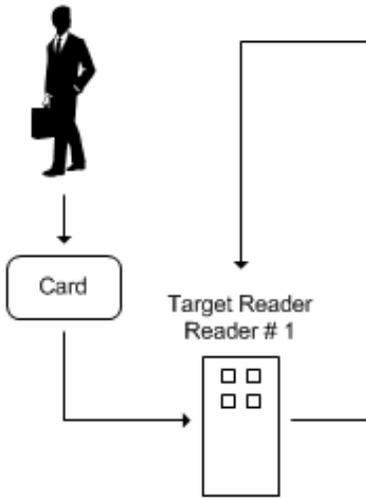
zones – ON or OFF – by cardholders in selected door groups at a specified target reader. This mode affects door group access, doors set on auto unlock/lock, and auxiliary input/shunt and auxiliary output devices that are controlled by the selected time zones.

When the time zone is toggled to its OFF state, the change in state is delayed by the number of seconds assigned in the Door Held Open Time / Exit Delay field in the Set Door & Reader Parameters form. The exit delay can be from 1 – 99 seconds. This mode can be cancelled to stop the time zone from being toggled off after the initial 3 card presentation. To cancel this mode, repeat presenting the card 3 times within the Exit Delay time.

While Present 3 is in effect and the time zone specified in the left box under Assigned Time Zones in the Present3 Reader Parameters form is toggled OFF, all cardholders in all door groups are denied access with a "single card presentation".

► *Example of Time Zone Toggle with Cardholder Lockout and Exit Delay*

Door Group Range < >
001 Marketing, 002 Sales, 003 Finance



Card presented
(x 3)

Toggles Assigned Time Zones ON – OFF
- TZ001 – Public Hours
- TZ002 – Office
- TZ004 – Production

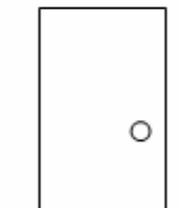
Target reader LEDs on Present 3
Time Zone toggled Off - rapid LED flashing
Time Zone toggled On - moderate LED flashing

Present 3 Reader with any Time Zone Toggle
Time Zone programmed or toggled – OFF
repeated cycle – rapid flashing 2 seconds, stops
flashing 5 seconds during OFF period

Exit Delay
Delays time zone change to OFF by the number
of seconds assigned in the Door Held Open
Time / Exit Delay field in the Set Door & Reader
Parameters form

Group Range can be one
group or multiple
consecutive groups in
the specified < >
range.

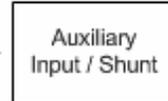
Affects doors & devices connected to specified
access control unit only (PANEL 1)



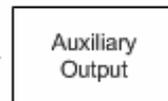
Auto Unlock/Lock Doors
TZ001, TZ002, TZ004



With Present 3 in
effect, Access
Denied to all door
groups with "single
card presentation"
when any assigned
time zone is toggled
OFF.



Auxiliary
Input / Shunt
Shunts PIR
(Motion Sensors)
TZ001, TZ002, TZ004



Auxiliary
Output
Toggles ON/OFF state for
maglocks (Unlock/Lock)
TZ001, TZ002, TZ004

Time Zone Toggle without Cardholder Lockout

Time Zone Toggle without Cardholder Lockout allows toggling specified time zones – ON or OFF – by cardholders in selected door groups at a specified target reader. This mode affects door group access, doors set on auto unlock/lock, and auxiliary input/shunt and auxiliary output devices that are controlled by the selected time zones.

While Present 3 is in effect, cardholders in door groups assigned to selected time zones when toggled OFF are denied access with a "single card presentation" (supervisory override). All other valid cardholders assigned to non-selected time zones are granted access with a "single card presentation".

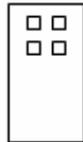
► *Time Zone Toggle without Cardholder Lockout*

Door Group Range <>
009 Managers & 010 Reception

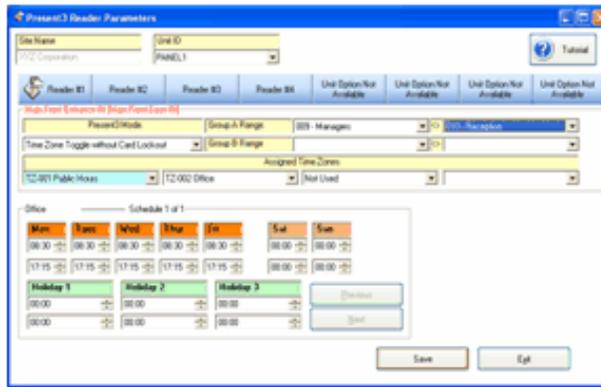


Card

Target Reader
Reader # 1



Card presented
(x 3)



Toggles Assigned Time Zones ON – OFF
- TZ001 – Public Hours
- TZ002 – Office

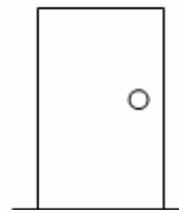
Target reader LEDs on Present 3
Time Zone toggled Off - rapid LED flashing
Time Zone toggled On - moderate LED flashing

Present 3 Reader with any Time Zone Toggle
Time Zone programmed or toggled – OFF
repeated cycle – rapid flashing 2 seconds, stops
flashing 5 seconds during OFF period



Valid cardholders
assigned to other
access levels may enter
door with "single card
presentation" when
TZ001 & TZ002 are
toggled off.

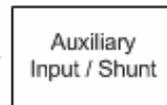
Affects doors & devices connected to specified
access control unit only (PANEL 1)



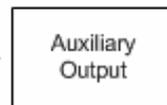
Auto Unlock/Lock Doors
TZ001, TZ002



Door Group Access
Levels
TZ001, TZ002
(Access denied when
time zone toggled off.)



Shunts PIR
(Motion Sensors)
TZ001, TZ002



Toggles ON/OFF state
for maglocks (Unlock/
Lock)
TZ001, TZ002

Not Used

Not Used clears the previous Present 3 mode for the selected reader.

Using Present3

Cardholders in door groups assigned to use Present3, just as its name implies, present their card 3 times in succession at a designated reader. Each successive card presentation must occur within 1.5 seconds of the preceding card presentation. When using the Door Toggle mode or either of the Time Zone Toggle modes, the reader LEDs will flash as listed below indicating that the time zone is being toggled:

- Door Toggled to Lock – rapid LED flashing
- Door Toggled to Unlock – moderate LED flashing
- Time Zone Toggled OFF – rapid LED flashing
- Time Zone Toggled ON – moderate LED flashing
- The Online Transactions form displays the relevant details whenever a door or time zone has been toggled.



Please note the following about any designated Present3 reader assigned a time zone toggle mode. After the time zone is toggled to its OFF state, either by a programmed time zone change or by a Present3 toggle, the reader's LED rapidly flashes for 2 seconds, stops flashing for 5 seconds, and then repeats the cycle. This remains in effect during the OFF period.

Setup Present3

Present3 has four modes of operation. Instructions to setup each mode are listed below under Procedures.

Procedures

► Steps to Setup Door Toggle Mode

1. From the Client main screen, select the Door Maintenance menu > Set Present 3 Reader Parameters.
2. From the Present 3 Reader Parameters form, if the access control unit is other than the one displayed under Unit ID, click on the down arrow and select the access control unit connected to the reader for toggling the door lock.
3. Select the tab of the appropriate reader # along the top of the form.
4. Click on the down arrow under Present 3 Mode and select Door Toggle from the drop down list.
5. Click on the down arrow to the immediate right of Group A Range and, from the drop down list, select the first door group that can toggle the door lock using Present 3. The maximum range is door group 001 to door group 255.

6. Click on the second down arrow of Group A Range (to the right of the < > symbols) and select either the same door group as chosen in the preceding step if only one door group is to use the door toggle mode or select the door group that is the last group in the range of door groups to use the door toggle mode.
7. To create a Group B Range of door groups, repeat the preceding 2 steps, otherwise go to the next step.
8. Click on the Save button.
9. Click on the Exit button.
10. From the Client main screen, click on the Update Changes quick button.
11. From the Panel Updates form, select the Upload button.
12. Click on the OK button, in the Upload Completed confirmation box.

► *Steps to Setup Toggle Time Zone with Cardholder Lockout*

1. From the Client main screen, select the Door Maintenance menu > Set Present 3 Reader Parameters.
2. From the Present 3 Reader Parameters form, if the access control unit is other than the one displayed under Unit ID, click on the down arrow and select the access control unit connected to the reader for toggling the door lock.
3. Select the tab of the appropriate reader # along the top of the form.
4. Click on the down arrow under Present 3 Mode and select Time Zone Toggle with Cardholder Lockout from the drop down list.
5. Click on the down arrow to the immediate right of Group A Range and, from the drop down list, select the first door group that can toggle the time zone(s) using Present 3. The maximum range is door group 001 to door group 255.
6. Click on the second down arrow of Group A Range (to the right of the < > symbols) and select either the same door group as chosen in the preceding step if only one door group is to use the time zone toggle mode or select the door group that is the last group in the range of door groups to use the time zone toggle mode.
7. To create a Group B Range of door groups, repeat the preceding 2 steps, otherwise go to the next step.
8. Under Assigned Time Zones, click on the 1st arrow to the left and select a time zone from the light blue drop down list. This is the primary time zone. You can select 3 additional secondary time zones from the white drop down lists. When the primary time zone is OFF, all cardholders using a single card presentation are denied access regardless of whether the secondary time

zones are off or on.

9. To add more time zones, repeat the preceding step.
10. Click on the Save button.
11. Click on the Exit button.
12. From the Client main screen, click on the Update Changes quick button.
13. From the Panel Updates form, select the Upload button.
14. Click on the OK button, in the Upload Completed confirmation box.

► *Steps to Setup Toggle Time Zone with Cardholder Lockout and Exit Delay*

Follow the steps outlined in Steps to Setup Toggle Time Zone with Cardholder Lockout to setup this mode for Present 3. The Door Held Open Time / Exit Delay field in the Set Door and Reader Parameters form has a default time of 25 seconds. If you wish to change the exit delay time from 25 seconds, follow the instructions below, otherwise the exit delay will be set to 25 seconds.

1. From the Client main screen, select the Door Maintenance menu > Set Door and Reader Parameters.
2. If its not currently displayed, click the down arrow to the right of Unit ID, and select the access control unit.
3. Select the Door Output # tab of the target reader that is to be used to toggle the time zone.
4. Click on the down arrow to the right of Door Held Open Time / Exit Delay and select a time from the drop down list. The values are expressed in seconds.
5. Select the Save button.
6. Select the Exit button.
7. From the Main screen, select the Update Changes quick button.
8. From the Panel Updates form, select the Upload button.
9. Click on the OK button in the Upload Completed confirmation box.

► *Steps to Setup Toggle Time Zone without Cardholder Lockout*

1. From the Client main screen, select the Door Maintenance menu > Set Present 3 Reader Parameters.
2. From the Present 3 Reader Parameters form, if the access control unit is other than the one displayed under Unit ID, click on the down arrow and select the access control unit connected to the reader for toggling the door lock.

3. Select the tab of the appropriate reader # along the top of the form.
4. Click on the down arrow under Present 3 Mode and select Time Zone Toggle without Cardholder Lockout from the drop down list.
5. Click on the down arrow to the immediate right of Group A Range and, from the drop down list, select the first door group that can toggle the time zone(s) using Present 3. The maximum range is door group 001 to door group 255.
6. Click on the second down arrow of Group A Range (to the right of the < > symbols) and select either the same door group as chosen in the preceding step if only one door group is to use the time zone toggle mode or select the door group that is the last group in the range of door groups to use the time zone toggle mode.
7. To create a Group B Range of door groups, repeat the preceding 2 steps, otherwise go to the next step.
8. Under Assigned Time Zones, click on the 1st arrow to the left and select a time zone from the drop down list. (You can select up to 4 different time zones.)
9. To add more time zones, repeat the preceding step.
10. Click on the Save button.
11. Click on the Exit button.
12. From the Client main screen, click on the Update Changes quick button.
13. From the Panel Updates form, select the Upload button.
14. Click on the OK button, in the Upload Completed confirmation box.

► *Steps to Clear an Existing Present 3 Mode*

1. From the Client main screen, select the Door Maintenance menu > Set Present 3 Reader Parameters.
2. From the Present 3 Reader Parameters form, if the access control unit is other than the one displayed under Unit ID, click on the down arrow and select the access control unit connected to the target reader.
3. Select the tab of the appropriate reader # along the top of the form.
4. Click on the down arrow under Present 3 Mode and select Not Used from the drop down list.
5. Click on the Save button.
6. Click on the Exit button.
7. From the Client main screen, click on the Update Changes quick button.

8. From the Panel Updates form, select the Upload button.
9. Click on the OK button, in the Upload Completed confirmation box.

I/O Management

I/O Management

Setting I/O Management parameters requires CA256 input/output control boards. The CA256 circuit boards are for special applications such as locker systems. The I/O Management forms should only be completed by a dealer/installer.

Glossary

Glossary of Terms

Term	Meaning
ACU	An acronym for access control unit, sometimes referred to as a "panel", the ACU is the main circuit board that inter-connects with the door hardware, readers, and the PC with the System VII software. The ACU sends and receives data from the System VII software and makes decisions to grant or deny access.
Archived Cardholder	When archived, the cardholder record remains in the database, however, the card assigned to that cardholder is de-activated. The system denies the cardholder entry to any system controlled doors or elevator floors that he or she would normally have access to until the Archived Cardholder status is disabled.
Archived System User	When archived, the system user's account remains in the database, however, the individual's account is de-activated and that person cannot log on to the software until the archived status is disabled.
Baud Rate	Indicates the number of bits per second transmitted. A baud rate of 9600 transmits 9600 bits per second.
Card	A card, such as a proximity card, is coded with a specific number. The card identifies the individual when it is presented to a reader which determines whether access is granted or denied.
Cardholder	An individual recorded in the system database who has been issued a credential, such as a proximity card, that can be used to access reader controlled doors or other controlled entry points.
CCTV	An acronym for closed circuit television. CCTV systems can be integrated with access control systems.
COM Port	A communication port usually found on the back of the PC that is used to connect with other peripheral devices.
CPU	An acronym for central processing unit which is the central processor that performs most of the calculations when a computer is instructed to do a task.
Door Group	In the software access is based on door groups, not individual cardholders. Cardholders are assigned to specific door groups for determining

	access levels at system controlled doors.
Elevator Group	In the software access is based on elevator groups, not individual cardholders. Cardholders are assigned to specific elevator groups for determining access levels at system controlled elevator floors.
Function Keys	Function keys are located along the top of the keyboard F1 to F12. Within the System VII software, pressing a function key acts as a shortcut to open certain interface screens or perform an action.
GMT	An acronym for Greenwich Mean Time. GMT is used as the primary basis for standard time around the world.
IP Address	The IP address identifies the address of a computer or device on a network.
Keypad	A keypad has a set of keys and is usually mounted in proximity to a door or entry point. To gain access, individuals key in their PIN codes using the keypad.
Master Login Account	A system user status in the software that gives authority to perform specific tasks.
Modem	Modem is an abbreviation for modulator/demodulator. A modem connects the computer to the access control units to transmit data over an analog phone line.
NIC	An acronym for network interface card, it is a circuit board installed inside the computer that allows it to be connected on a network.
Password	A personal access code keyed into the computer. A password is a security feature that enables a system user to log on and have access to the software.
PIN	An acronym for personal identification number. In the access control system, a PIN is a 5 digit number entered on a keypad to gain access.
Pulse	A term used in the software to momentarily unlock a door manually. When a door is pulsed, it is momentarily unlocked for the number of seconds specified in the Door Relay Unlock Time field. After the Door Relay Unlock Time expires, the door re-locks.
RAM	An acronym for random access memory, RAM is the computer memory available to the software programs when they operate.
Reader	A reader is a device that cardholders present their cards to in order to gain access at the controlled

	entry point.
Schedule	In the software a schedule is a user-defined period of time. Schedules reside in a time zone.
Site	Site refers to a description that defines one or more panels that control entry points in a building, part of the building, or some other physical location.
SMTP	An acronym for simple mail transfer protocol. SMTP is a protocol for sending email between servers.
System Administrator	A system user status in the software that gives authority to perform specific tasks.
System User	An individual that has been authorized for administrative tasks or monitoring the access control system.
TCP/IP	An acronym for transmission control protocol/internet protocol. TCP/IP is a set of transmission protocols used on the Internet and networks to transmit data.
Time Zone	A time zone is a user-defined period of time. Time zones can regulate cardholder access, automatically lock/unlock doors, regulate outputs, or arm/disarm auxiliary inputs and supervised inputs.
USB Port	Universal serial bus port is used to communicate with peripheral devices connected to the computer.

Troubleshoot Database Connection Error

Index

2

24 hour access	61
----------------------	----

A

accessibility feature	81
set times	43
add block of cards	120
alarm listings form	115
alarm monitoring	113
alarm notification	199
alarm response comments form	113
alarm types	117
alarm warning	117
anti-passback	43
reset	196
archive cardholders	127
archive system users	169
arm and disarm auxiliary inputs	55
arm and disarm supervised inputs	56
assign time zones to auxiliary outputs	54
assign time zones to readers/keypads	56
assigning outputs to auxiliary/supervised inputs	53
automatically lock/unlock elevator floor buttons	69
automatically unlock/lock doors	48
auxiliary input status	191

C

card in/out status	197
cardholder – reader access level reports	142
cardholder folder location	25
cardholder form	81
CCTV action setup/email notification	209
CCTV command setup	207
CCTV system	204
CCTV type setup	205
communication service setup	105
compressing the database	162
copy card records	129
credential	13
cumulative hours report	189

D

database location form	102
database maintenance options	157
daylight savings	78
default panel outputs protocols	185
delete a system user	169
deleted cardholder report	142
display access level summary	81
display online transactions	199
display software connections	201

door and input status	191
door group access levels	61
example	62
door group name	42
door held open time	43
door lock/unlock status form	148
door operation mode	43
door output # form	43
door relay unlock time	43
door status	191
door time zones form	33
examples	39
DVR	205

E

edit/delete card(s)	126
elevator bank names	65
elevator control status	195
elevator floor names	66
elevator group access levels	72
example	73
elevator group name	64
elevator name	65
elevator time zones	67
elevators	64
assign to banks	66
email alarm notification	97
export records - CSV	135
export records - PDF	134

F

find site contacts	164
find system users	167
first person in	50
example	51
floor button selection time	65
function keys	17

G

glossary	233
Greenwich Mean Time	199

H

holiday 1	33
holiday 2	33
holiday 3	33

I

I/O management	231
import records - CSV	135
import/export cardholder information	135
conventions	137
schedule	140
IOCB1616 parameters	54
IOCB1616 shunt control status	193

K	
Keyscan admin user account.....	151
Keyscan report previewer.....	178
L	
last card transaction	144
log on	22
lost or stolen card	130
M	
machine key serial number	15
manual AI shunt and SI control.....	192
manual output control.....	194
master log in account	91
N	
no access	61
not used since.....	132
O	
optional (cardholder) fields	84
P	
panel upload.....	110
password.....	154
change.....	154
password confirmation	154
PC requirements	14
photo capture.....	85
photo shape setup.....	184
Present3.....	217
modes.....	217
setup.....	225
using.....	225
print cardholder badges	133
print cardholder records.....	132
processing communications request.....	146
purge transactions	160
Q	
quick button	16
R	
reader access level report	142, 187
reader information form.....	43
re-index database	162
reports - access levels	142
reset anti-passback	196
restore database.....	157
S	
schedule CSV imports	140
schedule remote connections - modems.....	29

schedule/email reports	177
scheduled database backups.....	101
schedules	33
search for cardholders.....	122
security levels	92
set alarm response instructions/alarm graphic locations	58
set AO names & AO status	53
set elevator banks to time zones	67
show live video	207
show photos.....	200
signature capture	86
site contacts form.....	28
site information form.....	25
site information search form	24
site setup.....	24
site setup wizard.....	21
site unit setup form	27
SMTP email settings.....	30
software registration	15
standard time	78
supervised input status	191
switcher/matrix	205
system administrator	91
system log.....	181
system user account.....	89
archive.....	169
delete.....	169
security levels	92
types.....	91
user authority levels	92
system user information form.....	89
System VII Client version.....	17

T

temporary card.....	131
temporary card options	83
time zone limited access	61
time zone status.....	191
transaction	13
transaction reports	172
previewer	178
schedule/email	177
types of alarms	117

U

upload access control panels	110
user authority levels.....	92

V

video control panel.....	213
--------------------------	-----

W

wild cards	122
------------------	-----