

Copyright © 2001 - 2003 Keyscan Inc. All rights reserved.

Information in this document is subject to change without notice. The software outlined in this document is provided under license agreement. The software may only be used in accordance with the terms expressed by Keyscan Inc.

No part of this documentation may be reproduced or transmitted in any form or by any means except for the user's benefit of operating the software without the express written permission of Keyscan Inc.

Keyscan Inc.

1099 Kingston Road

Suite 206

Pickering, Ontario L1V 1B5

Canada

Phone: 1-888-539-7226 (Toll Free Canada/USA)

Phone: 905-420-7522

Fax: 905-420-7524

www.keyscan.ca

Table of Contents

Part 1: Introduction	1
Benefits	1
Overview	2
Alarms	3
Features	3
Using Security Cards	3
What's New in This Release	4
Online Help	5
Product Registration	5
Upgrading From System 3 or 3 Plus to System V	6
The Importance of Database Maintenance	6
Part 2: Software Installation & Existing Database Integration	7
Software Overview	7
System Requirements	8
System Configurations	8
Installation Instructions	10
Integrating a System 3 or 3Plus Database to System V	20
Part 3: Setup the System	25
Site Setup Wizard	25
Steps to Setup the System	26
Preliminary Steps to Site Setup	28
Site Setup	31
Site Information Form	32
Site Unit Setup Form	34
Site Contacts Information Form	36
Setting Up Doors for a New Site	38
Create Door Group Names	38
Create Door Names and Reader Outputs	40
Set Door Time Zones	44

Set Auxiliary Output Names & Set Auxiliary Output Status _____	49
Set Auxiliary/Supervised Input Names-Output Assignment _____	50
Assign Time Zones to Doors _____	51
Assign Time Zones to Auxiliary Outputs _____	53
Assign Time Zones to Auxiliary Inputs _____	54
Assign Time Zones to Supervised Inputs _____	55
Assign Time Zones to Readers/Keypads _____	56
Assign Door Group Access Levels _____	58
Set Alarm Response Instructions/Alarm Graphic Locations _____	61
Setting Up Elevator Information _____	63
Add Elevator Group Names _____	63
Set Elevator Bank Names _____	65
Set Elevator Names and Floor Hold Times _____	67
Assign Elevators to Elevator Banks _____	68
Set Elevator Floor Names _____	69
Set Elevator Banks to Time Zones _____	71
Set Elevator Time Zones to Automatically Lock/Unlock Floor Buttons _____	74
Assign Elevator Floors to Group Access Levels _____	76
Setup Holiday Time Zones _____	79
Assign a Holiday to a Holiday Time Zone _____	80
Daylight Savings _____	82
Add New Cardholders _____	84
General Cardholder Information _____	84
Additional Cardholder Information _____	88
Optional Cardholder Information _____	89
Setup System Administrators/Users _____	91
Backup Database _____	97
Uploading the Access Control Panels _____	99
Part 4: Preserving Site Data _____	100
Database Backup _____	100
Site Setup Report _____	100
Exporting Card Holder Records in CSV format _____	101
Part 5: Communication Problems _____	103
Procedure A – Keyscan Software Operation _____	104

Procedure B – Database IP Address _____	105
Procedure C – Network Connections _____	105
Procedure D – Keyscan Software/ACU Communication _____	106
Procedure E – Serial Port Connections _____	106
Procedure F – TCP/IP Connections _____	107
Procedure G – Modem Connections _____	108
Procedure H – Reader/Cards _____	109
Part 6: Database Recovery _____	111
Restore DB Backup Method _____	111
Copy Database Files to MSSQL7/Data Folder Method _____	115
Panel Recovery Method _____	120
Part 7: Communications Manager _____	125
Overview _____	125
Review of Communications Manager Main Screen and Menus _____	126
Communications Manager User Account _____	127
Log on the Communications Manager _____	127
Auto Start the Communications Manager _____	128
When to Reset Auto Start on the Communications Manager _____	129
Conventions for Configuring ACUs on Multiple Communications Managers _____	130
Re-assigning ACUs to an Alternative Communications Manager _____	132
Add a New Panel with Multiple Communications Managers _____	133
Appendix A _____	137
Terminology _____	137
Appendix B _____	139
Program MSS-COMM _____	139
Appendix C _____	149
Setup a CCTV System _____	149
CCTV Type Setup Form _____	149
CCTV Command Setup _____	150
CCTV Action Setup and E-mail Notification _____	151
Show Live Video _____	153
Appendix D _____	155
Alarm Listings _____	155
Index _____	156

Part 1: Introduction

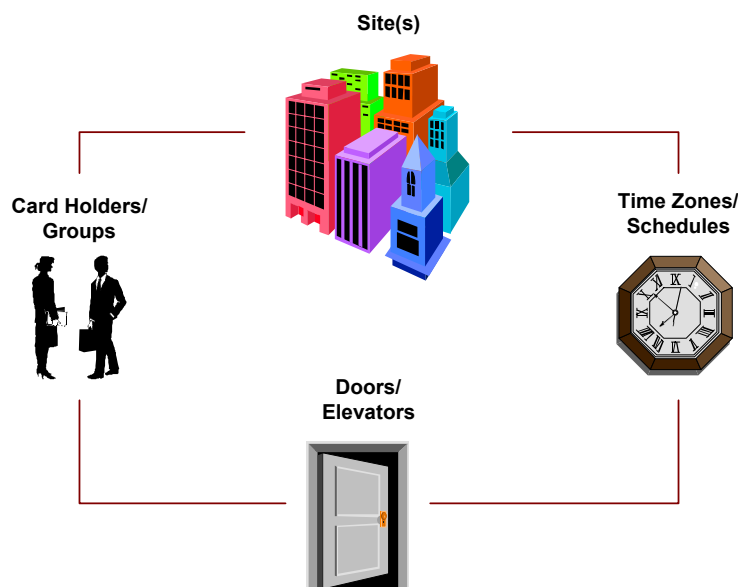
Benefits

In today's world, many organizations operate beyond the traditional schedule of Monday to Friday, 9 to 5. Indeed, whether it's a large corporate office in the heart of a metropolitan area, or a remote building in an isolated rural area, people are coming and going, 24 hours a day, 365 days of the year.

Buildings that rely solely on keys are not necessarily secure. Keys can be easily copied and access is not controlled. Because many companies have their entire financial and operating data on computers, a break-in or unmonitored intrusion could spell the loss or theft of critical information.

Keyscan Access Control Systems give you complete access control and management of your building or site. You can program a multitude of access levels and manipulate them in a variety of ways — any time, for any site. You can give all managers at one location 24-hour access to all doors, while you give the cleaning staff access to just the front door or a certain floor at a certain time. If a cardholder attempts to enter an area after the individual's designated time has expired, the software records that attempt. Reports can also be generated to detail a site's access activity and pinpoint security strengths and weaknesses.

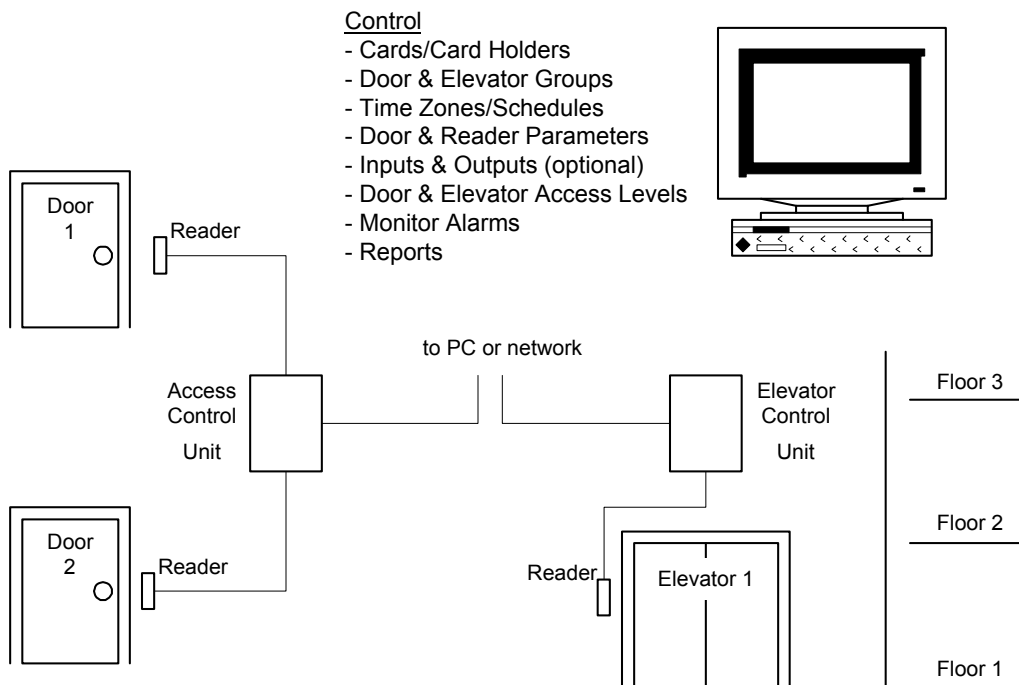
By setting up a comprehensive database of cardholders, access codes, and security clearances, you know exactly who is entering your premises at all times. The software and access control units are configured to work together as a system to monitor every door and entry point in your site around the clock, 365 days a year, and notify you of alarm conditions within seconds.



Overview

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

- Keyscan software
- personal computer
- security card
- card reader and/or keypad
- locking hardware
- access control unit (ACU)
- monitor alarms



keypad can be used alone or in combination with a card reader for even greater security. If used in conjunction with a keypad, card users enter the five digits of their PIN number on the keypad and then present their card at the card reader.

There are four common types of security card technologies:

- Wiegand technology
- Kwik Key data chip
- Proximity card
- Magnetic stripe

Information on these security card technologies is available from your Keyscan representative.

What's New in This Release

We've made some significant improvements to the Keyscan Management System software. In addition to re-designing the graphical user interface in a friendlier format, we've also incorporated the following features:

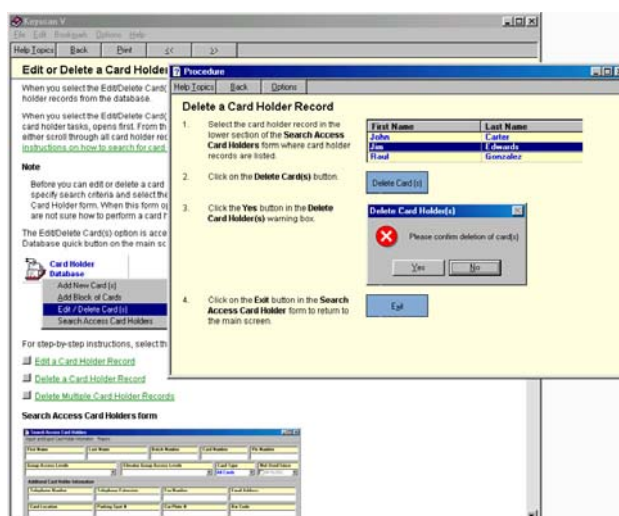
- 32 bit distributed processing
- MSDE database engine with SQL integration
- CCTV integration and control with any RS232 type camera system
- Multi-language capability
- Signature capture feature for photo ID badges
- Auto Email feature sends critical alarm messages or other transactions to PCs, cell phones, or pagers
- PDF format reports for convenient Emailing
- Site Setup Wizard to guide you through the steps to get your system running

Re-designed graphical user interface – main screen



Online Help

This manual is intended only as a guide to install and setup the Keyscan Management System V software, along with a review of some basic troubleshooting techniques and the procedures for database recovery in the event of a computer failure. For more extensive information on operating the Keyscan software, refer to the online help in the Client module. The Keyscan software is also context-sensitive. Pressing F1 on the keyboard opens a help window that explains the purpose of the screen or form currently on display and, where applicable, lists the steps to complete it. The contents of this manual are also included in the online help for convenient reference.



Product Registration

You must register your Keyscan System V software application within thirty (30) days to be an authorized user. Only registered users are eligible for Keyscan technical support. There are four possible packages that you may have to register depending on what you purchased:

- System V Basic Software with 2 Client Licenses (Software Registration tab)
- System V Additional Client Module (Additional Client License tab)
- System V Photobadging Module (Photo Registration tab)
- System V CCTV Module (CCTV Registration tab)



You should refer to your invoice to verify which packages you have purchased before you complete the registration form.

Instructions on how to register are outlined in the Help menu > Product Registration in the Client module. Be sure your company and dealer information is at hand. When you call, a Keyscan representative will request the Machine Key Serial Number posted at the top of the Keyscan System V Registration form, the registration software serial numbers, and your company and dealer information. You will be given Unlock Serial Number(s) to complete your software registration. Unless you receive the Serial Unlock Number(s) the Keyscan software will not function after 30 days.

Upgrading From System 3 or 3 Plus to System V

If you are currently operating with Keyscan Management System 3 or 3 Plus and are upgrading to System V, it is important that after installing the System V software you read Integrating a System 3 or 3Plus Database to System V on page 20. Please follow the steps outlined in this topic to convert your site data to System V before proceeding to do anything else with System V. If you make any entries to System V before completing the steps in Existing Database Integration, you may have to manually re-enter all your site data.

The Importance of Database Maintenance

One of the most important and critical topics in this manual is Backup Database on page 97. We cannot stress enough the importance of backing up your Keyscan data at regularly scheduled intervals and periodically copying the data to a removable storage device such as a CDR or to another network location for safe keeping.

Operating within the Keyscan software is an internal database engine that maintains all site records in a database. Setting up a site can entail a lot of man-hours to input all the data, especially for sites that have hundreds, if not thousands, of cardholders. If the site data is not backed up, in the event of a computer or hard disk failure, all your site information can be lost. Please be sure to read and follow the steps to backup your database. It's time well spent. If you have any questions or difficulties understanding the procedures after reading Backup Database, you can call Keyscan technical support Monday to Friday from 9 a.m. to 5 p.m., EST, at 1-888-539-7226 (Canada/US) or 905-420-7522 for assistance.

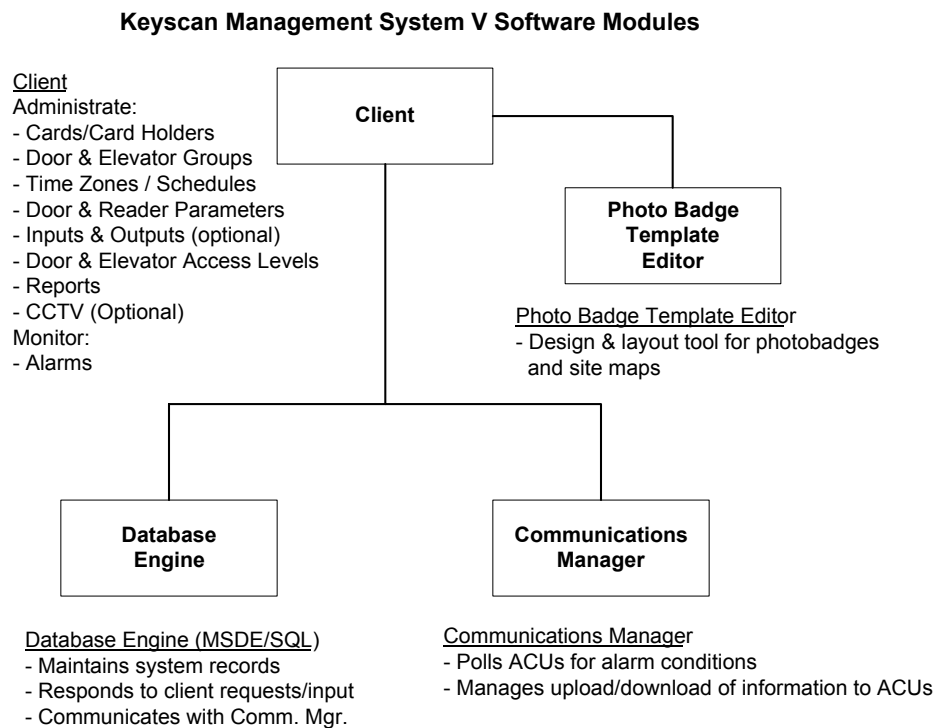
Part 2: Software Installation & Existing Database Integration

Software Overview

The Keyscan Management System V software consists of 4 separate and distinct applications which are referred to as modules. Because all 4 modules are separate but inter-dependant, you must install each one so that the Keyscan V software functions correctly:

- Database Maintenance Module (MSDE Database Engine)
- Keyscan Client (includes the CCTV option)
- Communications Manager
- Photo Badge Template Editor (Optional)

The following illustration outlines the functions of each software module.



System Requirements

The following outlines the system requirements to operate the Keyscan Management System V software application:

- Recommended Central Processing Unit: PIII 800Mhz
- Recommended RAM: 256 megabytes or greater when setting up a single PC operation; 128 megabytes or greater when setting up individual modules on several PCs.
- Hard Disk: Recommended 20 Gigabytes
- USB Port for Photo Badging and Signature Capture (Not supported on NT)
- COM Port: 1 required if direct connect to access control units; 2 required if using CCTV control
- CD-ROM Drive
- Removable Media Storage Device such as a CD Writer for database backup
- Network Interface Card (NIC)
- Operating System: Windows 98, ME, NT, 2000 or XP Professional
- Microsoft Internet Explorer 4.01 Service Pack 2 or later

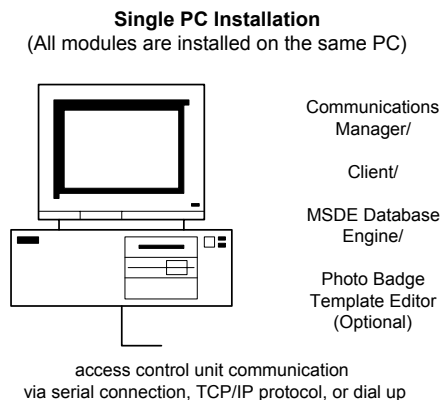
For sites with large cardholder populations and high volumes of transactions, we strongly recommend that you install the Database Maintenance Module (MSDE/SQL) on a dedicated PC. Faster processors and higher RAM provide better system performance.

System Configurations

The Keyscan Management System V software can be installed on a single PC and a network.

Single PC

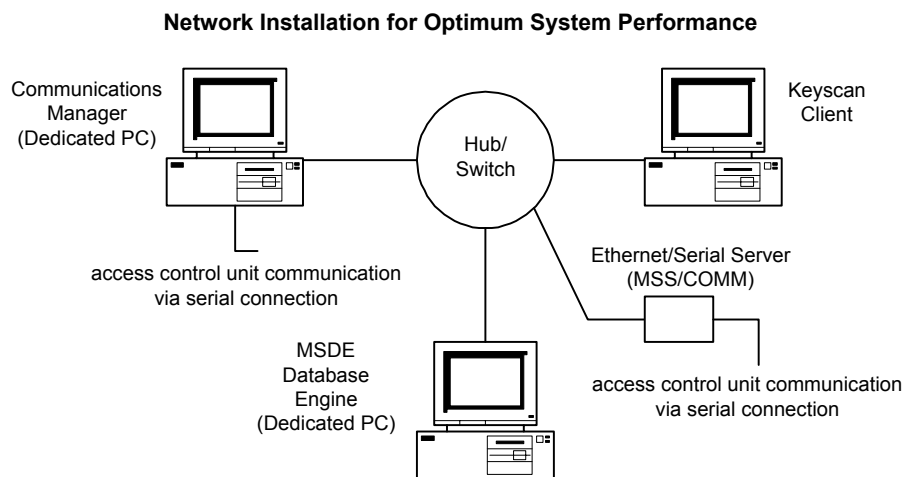
For a single PC installation, all three of the following modules must be installed — the Database Maintenance (MSDE Database Engine) module, the Keyscan Client, and the Communications Manager. You may install the Photobadge Template Editor to create site maps, however, you must register this application to generate badge templates and use the photo verification feature. For optimum system performance on a single PC, a Pentium III 800 MHz or higher processor with 256 megabytes of RAM is recommended.



Networks

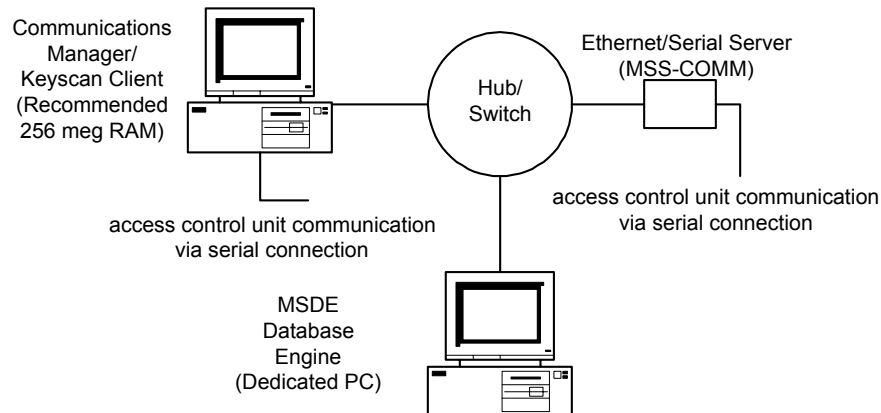
To derive optimum system performance on a network, Keyscan recommends installing the Communications Manager on a dedicated PC and the MSDE Database Engine on a dedicated PC. The Keyscan Client can be installed on multiple PCs. The MSDE database engine's performance declines exponentially as the number of concurrent Client users, users with the Client open simultaneously, increases above the maximum. The Photo Badge Template Editor should be installed at the same location as a Client, however it can be installed anywhere on the network that is accessible to Clients.

Keyscan strongly advises that you do not install the Keyscan software modules on your corporate server. If you are using TCP/IP communication, be sure to check that the IP address is active. To check, type IPCONFIG at the DOS prompt.



As an alternative, if system resources are not available to install the Keyscan V software as recommended, the Client can be installed on the same PC with the Communications Manager shown in the following illustration. However, 256 megabytes of RAM is recommended.

Alternative Network Installation



Installation Instructions

The two modes of installation are as follows:

- Single PC Installation – All the modules are automatically installed on the selected PC that may be either a stand-alone PC or a PC connected to a network.
- Multiple PC Installation – Each module is installed individually on multiple PCs throughout a network. Note, however, that the Database Maintenance, Communication Manager, and Keyscan Client modules must be installed somewhere on the network in order for the system to function.

Follow the appropriate installation instructions as outlined in the succeeding sections. At the conclusion of the installation when you log on to the Keyscan Client module, you will be prompted to register your software. For details about registering, see Product Registration in the online help in the Keyscan Client module.

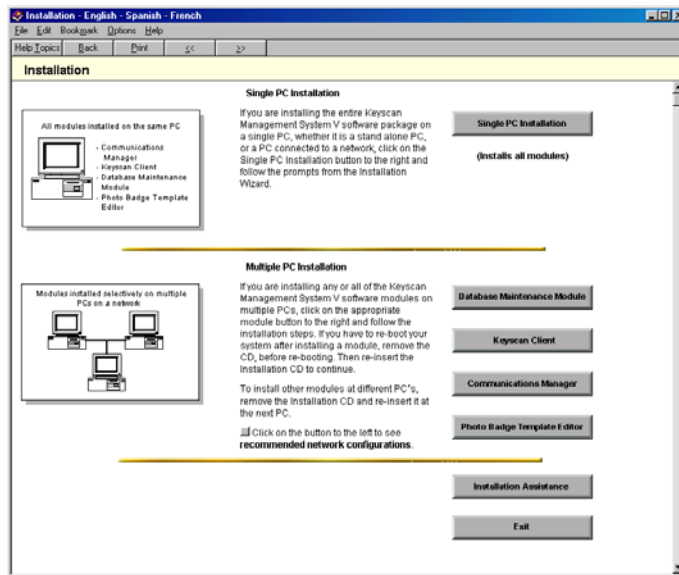
After you have installed the Keyscan software modules and, if at a later date, you need to uninstall any or all of the software modules, please call Keyscan technical support for the proper uninstall procedures. Our toll free number is listed on the card that accompanied the Keyscan Installation CD.

Important

If you are performing a Single PC Installation or a Multiple PC Installation on a system with, Microsoft Windows NT, Windows 2000, or Windows XP Professional, you must have administrator permissions or you will experience problems. Please consult with your IT department.

If your system has Norton Anti-Virus, we advise that you disable 'script blocking'. Please refer to your Norton manual for instructions on disabling this feature.

Installation screen



Installation on a Single PC

Installation on a single PC, by definition, has all four modules installed on one PC, whether the PC is connected directly to the ACU(s) or indirectly to the ACU(s) via a network. For a single PC installation please be sure that your computer has sufficient hard disk space. The KeyScan System V software modules require 500 megabytes plus you must have sufficient additional hard disk capacity to allow for database growth. The size of your facility and the volume of site activity will influence the size of your database and how rapidly it grows.

Note

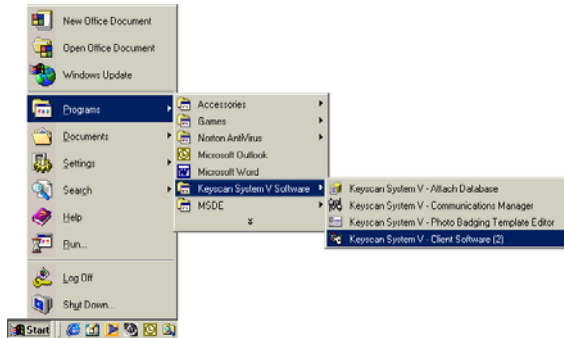
When you select Single PC Installation, the Photobadge Template Editor is automatically installed. If you have not purchased this optional module, you may use the map component to draw site plans and load them into the Alarm Response Instructions \ Alarm Graphic Locations form. You cannot, however, import photobadge templates, use the photo verification feature, or import photos to cardholder records unless you purchase and register this optional module.

Steps for Single PC Installation

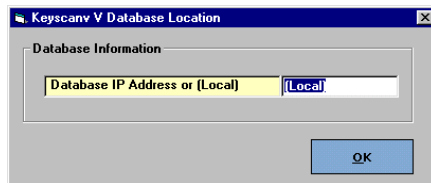
1. Close any applications that are currently open.
2. Insert the KeyScan Management System V CD into the CD-ROM drive. Autorun will open the installation procedures.
3. From the Welcome screen, select a language.
4. Please take a moment to read the information on the Forward screen. Click on the Continue to Installation Page button at the bottom.
5. From the Installation screen, select the Single PC Installation button and follow the on-screen prompts from the Installation Wizard. During the installation, the progress indicator may appear to stall around 95 %. At this juncture the database engine is loading and may take several minutes depending on your computer's processor. Please be patient.



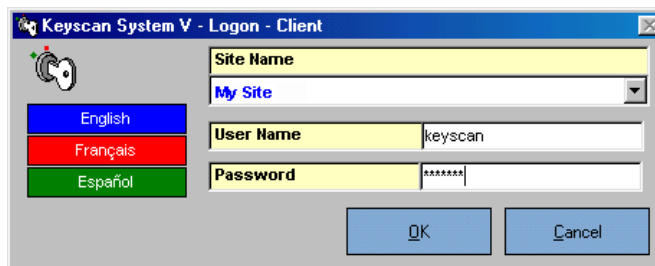
6. After the installation is complete, open the Keyscan Client software. You may have to re-start your computer depending on your version of Windows[®].



7. From the Keyscan V Database Location dialog box, leave the default setting on (Local).



8. Click on the OK button.
9. In the Keyscan System V – Logon – Client dialog box, if appropriate, click on the – English, Français, or Español button to change the program interface to your preferred language, enter *keyscan* in the User Name text box and enter KEYSCAN in the Password text box. The password is case sensitive and must be entered in upper case. If you have an existing database from a previous version of Keyscan software, see Integrating a System 3 or 3Plus Database to System V on page 20. If you intend to start setting up your system go to page 25.



Multiple PC Installation on a Network

Whether you follow our recommended network configuration or choose to configure it differently, we suggest you pre-plan where you intend to install each software module on your network before you start the installation procedures.

Network Installation Events

Database Installation

Select location for Database installation.
↓
Install Database Maintenance.
↓
Activate Database Auto-start service.
↓
Attach Database and confirm path.

Client Installation

Select location for Client installation.
↓
Install Client.
↓
Open Client and specify IP address of database.
↓
Repeat for each Client installation.

Communication Manager Installation

Select location for Communication Manager installation.
↓
Install Communication Manager.

Important

Keyscan strongly advises that you do not install the Keyscan software modules on your corporate server. We recommend that you install the software modules on PCs.

Note

If you have not purchased the Photobadge Template Editor module, you may install it and use the map functions within the application to draw site plans and

load them into the Alarm Response Instructions \ Alarm Graphic Locations form in the Client module. You cannot, however, import photobadge templates, use the photo verification feature, or import photos to cardholder records unless you purchase and register this optional module.

Installing Multiple Communications Managers

Where a large number of panels exist, for faster polling and activity collection, multiple Communications Managers may be installed on multiple PCs.

Multiple Communications Managers may be configured in the following four schemes:

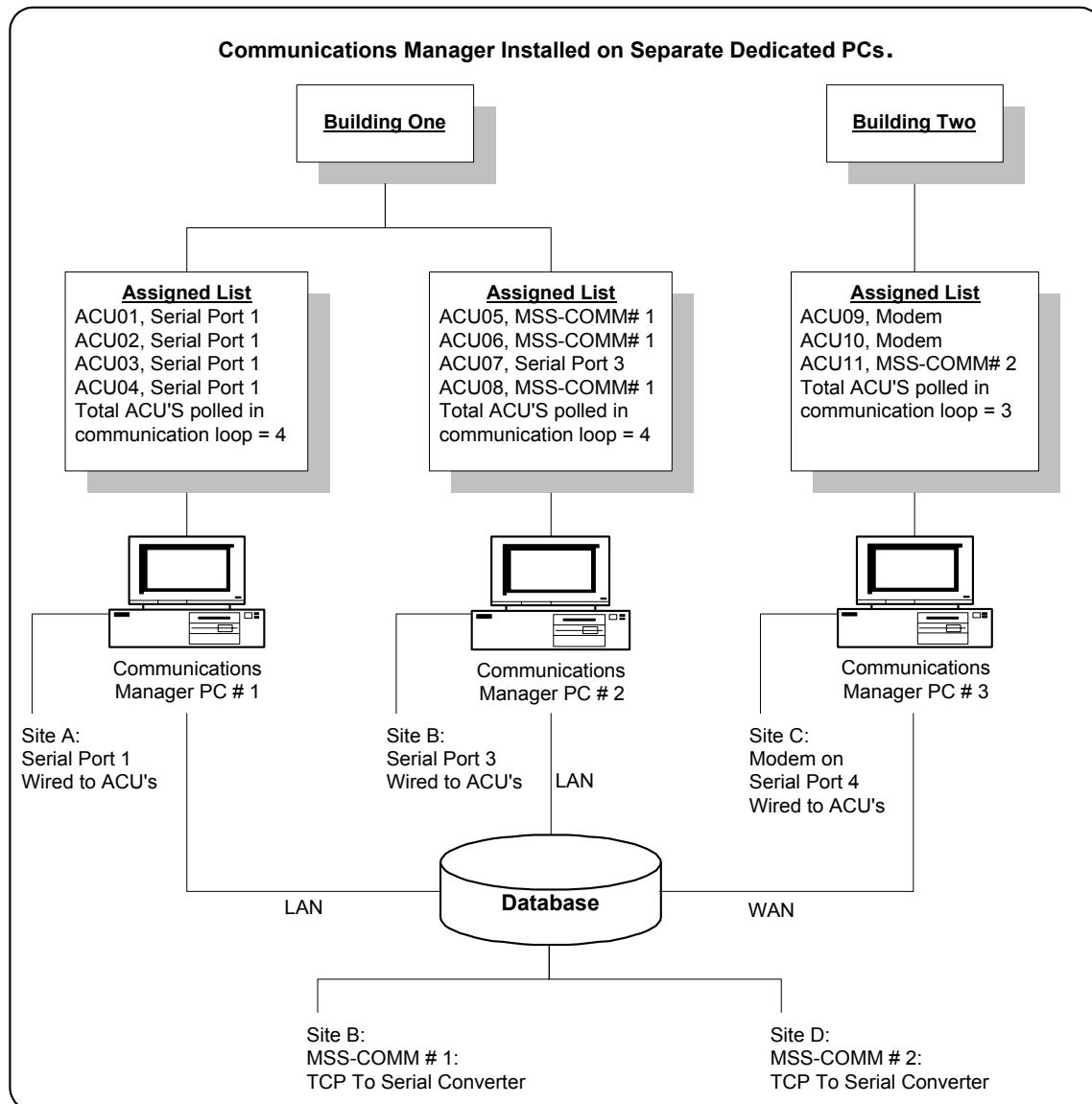
- 1 Communications Manager for all sites
- 1 Communications Manager for each site
- 1 Communications Manager for a group of access control units within 1 site
- 1 Communications Manager for a group of access control units across multiple sites

Communications may be established by MSS-COMM (TCP to Serial Converter), modem, or serial connection within the same Communications Manager.

Important

Do not install more than one Communications Manager on a PC.

The following diagram illustrates a hypothetical installation with multiple Communications Managers using the three communications modes.



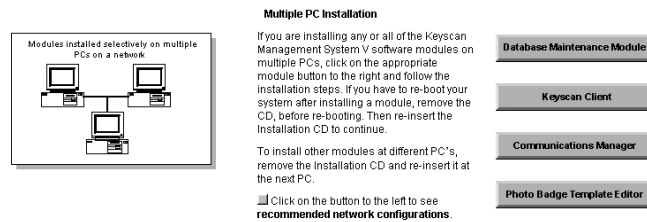
Preliminary Steps for Multiple PC Installation

1. Locate the PC where you intend to install the Database Maintenance module.
2. Close any applications that are currently open.
3. Insert the Keyscan Management System V program CD into the CD-ROM drive.
4. Autorun loads the Installation Procedures.

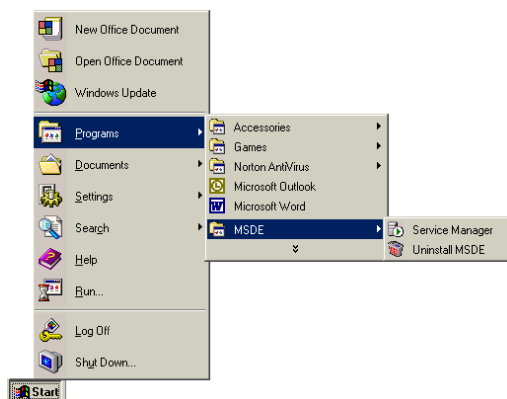
Steps to Install Keyscan V Modules

1. From the Welcome screen, select a language button.
2. Please take a moment to read the information on the Forward screen. Click on the Continue to Installation Page button at the bottom.

3. From the Installation screen, select the Database Maintenance Module button in the Multiple PC Installation section.



4. From the Steps to Install the Database Maintenance Module screen, please read the red text at the top before proceeding. Click on the Install Database Maintenance Module button. This procedure may take several minutes. Follow the prompts from the Installation Wizard.
5. From the bottom left corner of the screen, select the Start button > Programs > MSDE > Service Manager.

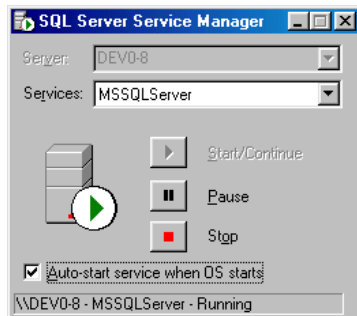


6. From the SQL Server Service Manager dialog box, click in the box to the left of *Auto-start service when OS starts* to activate this function. Activating this field starts the database engine every time the computer boots. Just as an automobile will not operate without the engine running, the Keyscan V software will not function unless the database engine is open and operating.

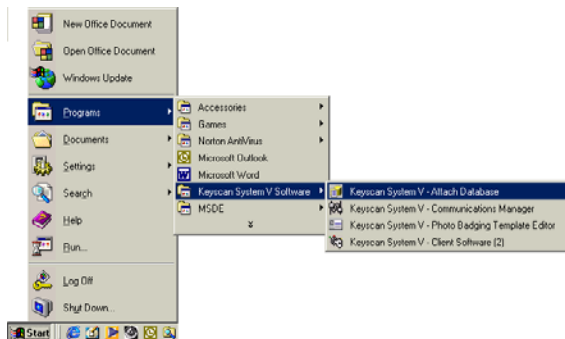


7. If service is *stopped*, indicated by the red button, click on the ► *Start/Continue* button. The SQL Server Service Manager dialog box should appear as the example immediately

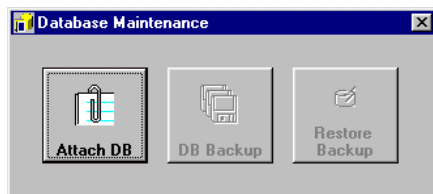
below.



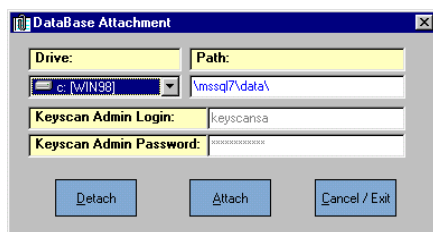
8. Click on the upper right **X** button to close the SQL Server Service Manager dialog box.
9. Select the Start button > Programs > Keyscan System V Software > Keyscan System V - Attach Database.



10. From the Database Maintenance dialog box, select the Attach DB button.



11. Confirm the drive and path are correct in the Database Attachment dialog box, and select the Attach button.



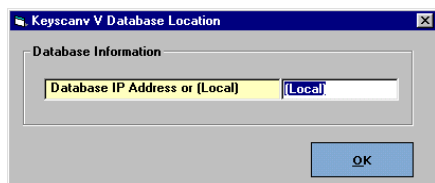
12. From the Auto Start Communication Manager box, select either Yes or No depending on the following conditions:

- Yes – if a Communications Manager is installed on this PC
- No – if a Communications Manager is not installed on this PC

See Communications Manager for procedures on Auto Start.



13. Close both the Database Attachment and Database Maintenance dialog boxes by clicking on the **X** button in the upper right corner.
14. If you intend to install the Client module at another PC, remove the CD from the CD-ROM and relocate to the appropriate PC location and re-insert the Program Installation CD, before you proceed to step 15.
15. From the on-screen Installation Procedures, click on the Keyscan Client button in the Multiple PC Installation section. Follow the on-screen instructions. Also see steps 20 to 23 to specify the IP address for each Client you install.
16. If you intend to install the Communications Manager module at another PC, remove the CD from the CD-ROM and relocate to the appropriate PC location and re-insert the Program Installation CD, before you proceed to step 17.
17. From the on-screen Installation Procedures, click on the Communications Manager button. Follow the on-screen instructions. Also see steps 20 to 23 to specify the IP address for each Communications Manager you install if installed on a separate PCs from any other Keyscan modules.
 - The Communications Manager can be installed on any selected workstation, but it has to be running somewhere on the network when the Keyscan applications are operating.
18. If you intend to install the Photo Badge Template Editor module (optional) at another PC or server, remove the CD from the CD-ROM and relocate to the appropriate PC location and re-insert the Program Installation CD, before you proceed to step 19.
19. From the on-screen Installation Procedures, click on the Photo Badge Template Editor button. This is an optional application. Also see steps 20 to 23 to specify the IP address for the Photo Badge Template Editor if it was installed on a separate PC from any other Keyscan modules.
20. After you have completed installing the Client(s), Communications Manager(s) or the Photo Badge Template Editor(s), click on Start > Programs > Keyscan V > and select the appropriate application. You may have to re-boot your computer before the program opens depending on the version of Windows that operates your system.
21. In the Keyscan V Database Location dialog box, clear (*Local*) from the text box and enter the valid IP Address of the computer where the database was installed. You must do this for each PC where a Keyscan Client, Communications Manager, or Photo Badge Template Editor was installed. If more than one of the preceding modules is installed on the same PC you only have to specify the IP address in one of the modules on that PC.



22. Click on the OK button.
23. In the Log On dialog box, if appropriate, click on the – English, Français, or Español button to change the program interface to your preferred language, enter *keyscan* in the User Name text box and enter KEYSCAN in the Password text box. The password is case sensitive and must be entered in upper case. In the case of the Communication Manager(s) minimize the application to keep it running.



Note

If you have an existing database from a previous Keyscan software version, see Integrating a System 3 or 3Plus Database to System V on page 20, otherwise you may proceed to Part 3: Setup the System on page 25.

Integrating a System 3 or 3Plus Database to System V

It is extremely important to convert and integrate an existing database from a previous Keyscan software version, before you start using the Keyscan Management System V software. The Keyscan Management System V software is bundled with an Import Utility that guides you through the conversion process to integrate your System 3 or 3 Plus Keyscan database into System V. When the conversions are completed, the records for each site in System 3 or System 3Plus are formatted for System V.

Note

Before you begin the process of converting your existing database to the Keyscan System V software, you must map a drive to the old system 3 software's KEYSKAN.INI file. By default this file was located in the C:\SYS34WIN directory. If your Keyscan system is on a network, we strongly suggest you consult with the IT department before mapping a drive.

Preliminary

The Personnel Information form in System 3 and System 3Plus only had a single Name field, which could be a first name, a last name or both names, and 10 user defined fields. In contrast, System V has a First Name field and a Last Name field, 8 system-defined fields, and 10 optional, user-defined fields as seen in the examples below. (The System V Optional Fields form is not shown in the example.)

System 3 & 3Plus

System V – System Defined Fields

Before you start the conversion you may wish to review how the System 3 Personnel Form has been set up, especially the name field. When the conversion utility reaches the personnel segment of the database, it prompts you to specify the how the name field was structured: first name, last name or both names, in order to accurately convert the data from System 3 to the proper name fields in System 5. You also have the option to either, convert the optional System 3/3Plus personnel fields directly to the System V optional fields, or convert them to the System V system-defined fields as shown above on the right, if they match. The conversion utility lists the names of the System 3/3Plus optional fields starting at #2 to #11 as they have been numbered above.

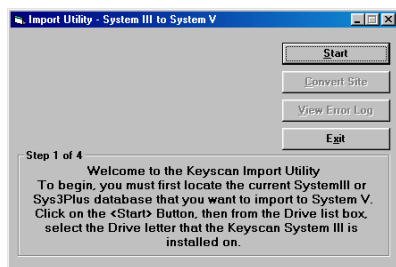
To Convert and Integrate an Existing Database

1. Verify that the MSDE Service Manager is open. At the location where the database was installed, you should see the Service Manager ON icon in the status bar in the bottom right corner of your screen. If you do not see the icon, review the Installation Instructions for networks to activate the Service Manager auto start feature.

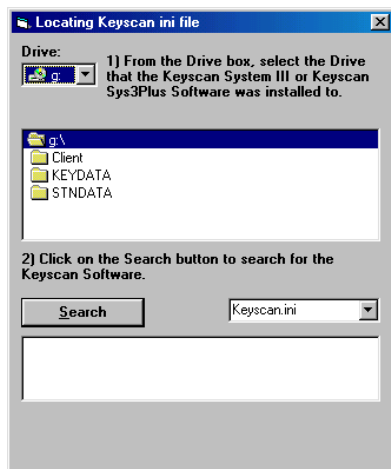


MSDE Service
Manager ON Icon

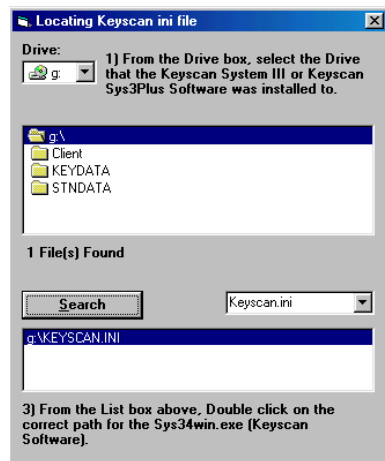
2. The Import Utility – System III to System V is on the Keyscan CD. If you removed the Keyscan CD from the CD-ROM drive, please re-insert the disk. From Windows Explorer, select the CD-ROM drive; locate the Utilities folder, and double click on the file named - SYS3TOSYS5.exe - to open the utility.



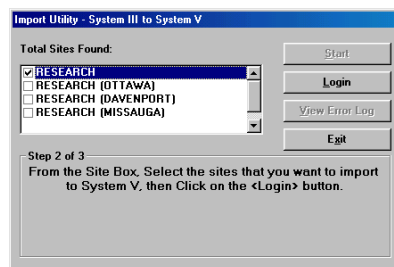
3. Click on the Start button.
4. From the Loading Keyscan .ini file dialog box, click on the down arrow of the Drive box and select the drive where the existing database resides.



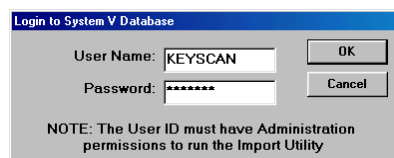
5. Click on the Search button.



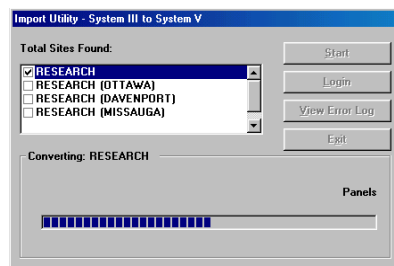
6. Double click on the keyscan.ini file highlighted in blue in the list box below the Search button.
7. Select the names of the sites from the database by clicking in the boxes to the left.



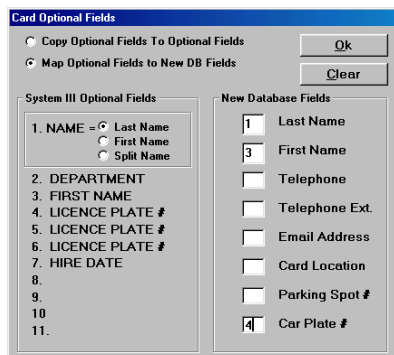
8. Click on the Login button.
9. From the Login to System V Database dialog box, enter *keyscan* in the User Name box, and enter KEYSCAN in the Password box.



10. Click on the OK button. The conversion process starts.

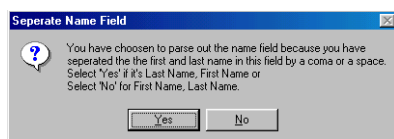


11. When the conversion process reaches the card segment of the database, the utility pauses and the Card Optional Fields dialog box opens. Select one of the radio buttons at the top:
 - Copy Optional Fields to Optional Fields. If this option is selected, the data and the captions in the System III Optional Fields, from #2 to #11, will be copied to the Optional Card Holder Fields in System V.
 - Map Optional Fields to New DB Fields. If this option is selected, the data in System III Optional Fields are copied to the System V captions on the right. In the example below, System III has an optional field 3 - First Name. Because System V (New Database Fields) has a specific First Name field, a value of 3 was entered in the box to the left. The conversion utility copies all field 3 entries from System III to the First Name field in System V.



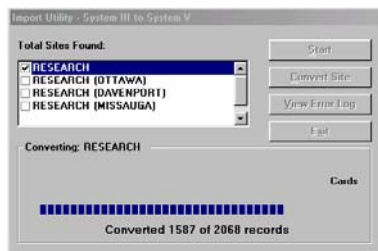
The 'Card Optional Fields' dialog box has two radio buttons at the top: 'Copy Optional Fields To Optional Fields' (unselected) and 'Map Optional Fields to New DB Fields' (selected). Below these are two columns of fields. The left column, 'System III Optional Fields', lists fields 1 through 11. Field 1 is 'NAME =', with sub-options 'Last Name' (selected), 'First Name', and 'Split Name'. Fields 2 through 11 are: 'DEPARTMENT', 'FIRST NAME', 'LICENCE PLATE #', 'LICENCE PLATE #', 'LICENCE PLATE #', 'HIRE DATE', and three empty slots. The right column, 'New Database Fields', lists fields 1 through 4: 'Last Name', 'First Name', 'Telephone', 'Telephone Ext.', 'Email Address', 'Card Location', 'Parking Spot #', and 'Car Plate #'. A value of '3' is entered in the box next to 'First Name'.

12. In the 1. Name = section, select the radio button that depicts the Name convention used in System 3/3Plus.
 - Last Name
 - First Name
 - Split Name (Smith, John = Yes or John, Smith = No in the Separate Name Field dialog box)



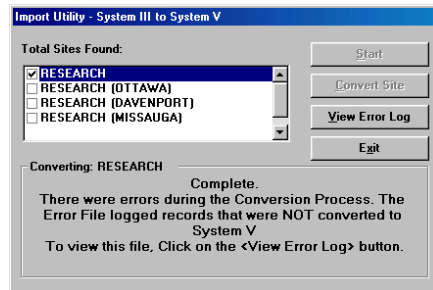
The 'Separate Name Field' dialog box contains a question mark icon and the following text: 'You have chosen to parse out the name field because you have separated the first and last name in this field by a comma or a space. Select 'Yes' if it's Last Name, First Name or Select 'No' for First Name, Last Name.' There are 'Yes' and 'No' buttons at the bottom.

13. If you selected Copy Optional Fields to Optional Fields, proceed to step 14. If you selected Map Optional Fields to New DB Fields, in the New Database Fields section, enter the number in the box that corresponds to the captions on the left listed in System III Optional Fields.
14. Select the OK button. The conversion process continues.

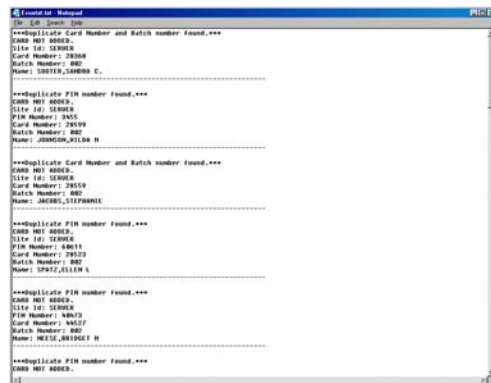


The 'Import Utility - System III to System V' dialog box shows a list of 'Total Sites Found' with 'RESEARCH' selected. Below the list, it says 'Converting: RESEARCH'. At the bottom, a progress bar shows 'Converted 1587 of 2068 records'. Buttons for 'Start', 'Convert Site', 'View Error Log', and 'Exit' are on the right.

15. The Import Utility – System III to System V dialog box will indicate that either the database was converted successfully or it detected mistakes.
 - If the conversion was successful, select the Exit button and proceed to step 17.
 - If there are records with mistakes, select the View Error Log button to review the records that were found to have errors and proceed to step 16.



16. When View Error log is selected, Notepad opens with a listing of errors in the database. Print a copy of the Error Log and make the corrections from the System V Client software module. Select the Quick Buttons menu > Edit/Delete Card Holders.



17. If you are logging on the Keyscan V Client software for the first time, type Keyscan in the User ID text box and KEYSCAN in the Password text box.

Note

If you have converted a System 3 database, when you log on to the newly converted site in System V, you must upload the panel. This only applies to System 3 and not System 3Plus. See Uploading the Access Control Panel on page 99 for the procedures.

Part 3: Setup the System

There are two methods to setup your site, you can use the Site Setup Wizard or you can follow the complete outline in Steps to Setup the System on page 26.

Important

If you have upgraded to Keyscan Management System V software from versions 3.0 or higher, you must open the Import Utility and convert and integrate your existing database before you add site information. See Integrating a System 3 or 3Plus Database to System V on page 20 for step by step procedures.

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 Setup Wizard, it automatically opens the forms for each step in successive order as listed on the illustration of the Site Setup Wizard screen below. Enter the required information and save your data as you progress through each form.

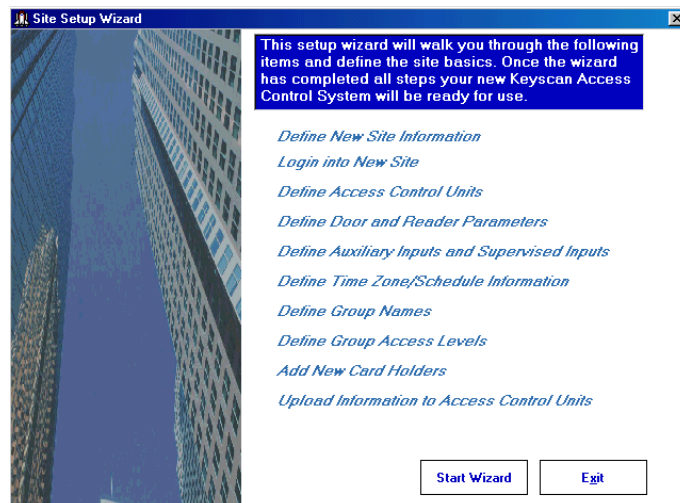
Note

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.

To Open the Setup Wizard

From the Keyscan System V Client's main screen, select the System Settings menu > Site Wizard > Start Wizard button.

Setup Wizard screen



Steps to Setup the System

After installing the Keyscan Management System V software, the next task is to set up your site using the Client software. This consists of 9 general steps as outlined below. Completing the steps involves filling out forms that are accessed from the menus or the quick buttons on the Keyscan V Client's main screen. The configuration of your site determines which steps and forms you complete. As an example, if your site does not have elevators, by-pass this step.

Preliminary

Ensure that both the Communications Manager and MSDE Service Manager are on when you begin to set up your site from the Client module.

1. Create a Site

- Site Information form
- Site Unit Setup form
- Site Contacts Information form

2. Setup Door Information

- Group Information form (create door group names)
- Reader Information/ Door Outputs (set door & reader parameters)
- Door Time Zones form
- Set Auxiliary Output Names & Auxiliary Output Status form
- Set Auxiliary/Supervised Input Names – Output Assignments form
- Assign Time Zone to Automatically Lock/Unlock Doors form
- Assign Time Zones to Automatically Toggle Auxiliary Outputs form
- Assign Time Zones to Auxiliary Inputs form
- Assign Time Zones to Supervised Inputs form
- Reader/Keypad Access Setup and Time Zone Operation form
- Door Group Access Levels form
- Set Alarm Response Instructions / Alarm Graphic Locations form

3. Setup Elevator Information

- Group Information form (create elevator group names)
- Set Elevator Bank Names form
- Set Elevator Names and Floor Hold Times form
- Assign Elevators to Elevator Banks form
- Set Elevator Floor Names form
- Set Elevator Banks to Time Zones form
- Set Elevator Time Zones to Automatically Lock/Unlock Floor Buttons form

- Assign Elevator Floors to Group Access Levels form

4. Setup Holidays

- Setup Holiday Time Zones form
- Assign a Holiday to a Holiday Time Zone form

5. Setup Daylight Savings

- Daylight Savings Setup form

6. Setup New Cardholders

- General Cardholder Information form
- Additional Cardholder Information form
- Optional Cardholder Information form

7. Setup System Administrators

- System User Information form

8. Backup Database

- Full Database Backup form

9. Upload Information to ACUs

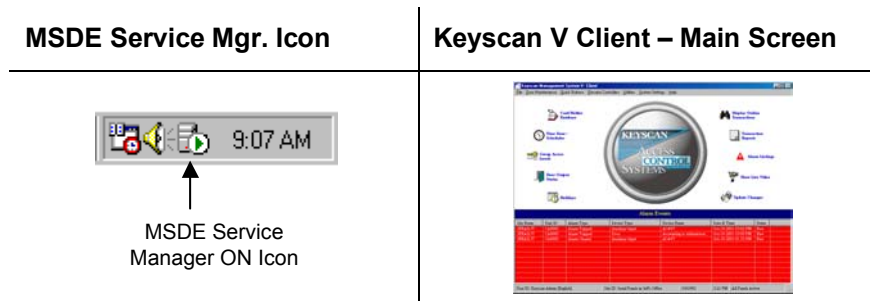
- Panel Updates form

Preliminary Steps to Site Setup

Before setting up your site, the Service Manager, the Communications Manager, and the Keyscan Client must all be open.

If you have completed the installation procedures and you are continuing on from Part 2: Software Installation & Existing Database Integration, the MSDE Service Manager and the Keyscan System V – Client software applications should already be open.

When the MSDE Service Manager is open, its icon is visible at the bottom of the monitor in the status bar of the PC or network location where it was installed. When the Keyscan V Client is open, the screen on the monitor appears as the example seen below.

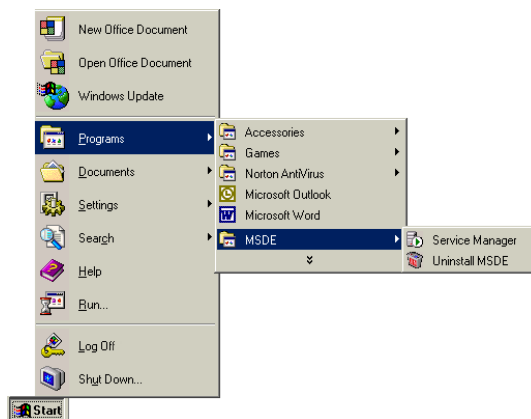


Open the Communications Manager by following the steps on page 29.

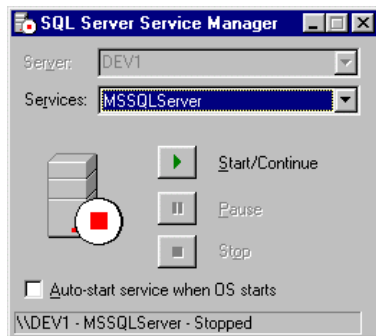
Be sure all three applications – the Service Manager, the Communications Manager, or the Keyscan Client are open, if not, follow the instructions to open the appropriate application.

To Open the MSDE Service Manager

1. Select the Start button > Programs > MSDE > Service Manager.



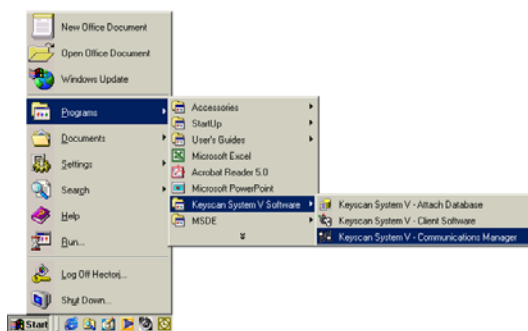
2. If MSSQL Server – Stopped appears in the status bar at the bottom of the SQL Server Service Manager dialog box, click in the box to the left of Auto-start service when OS starts to activate this field.



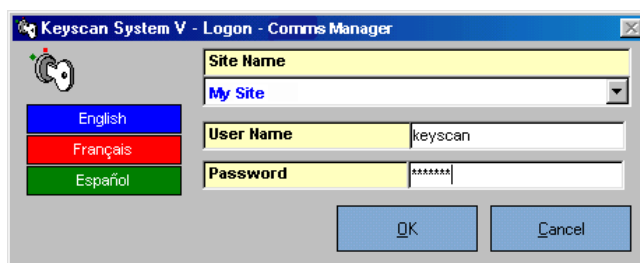
3. Select the Start/Continue button.
4. Click on the X in the upper right corner of the SQL Server Service Manager to close the dialog box.

To Open the Communications Manager

1. Select the Start button > Programs > Keyscan System V Software > Keyscan System V – Communications Manager.



2. In the Logon - Comms Manager dialog box, if appropriate, click on the – English, Français, or Español button to change the program interface to your preferred language, enter *keyscan* in the User Name text box, and enter KEYSCAN in the Password text box. The password is case sensitive and must be entered in upper case.

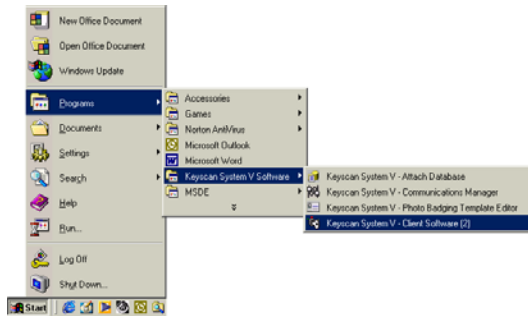


3. Click on the OK button. The Communications Manager screen will minimize after start up.

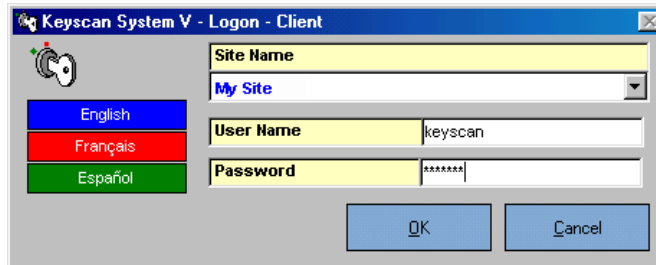
To Open the Keyscan Client

1. Select the Start button > Programs > Keyscan System V Software > Keyscan System V –

Client Software.



2. In the Log On Client dialog box, if appropriate, click on the – English, Français, or Español button to change the program interface to your preferred language, enter *keyscan* in the User Name text box and enter KEYSCAN in the Password text box. The password is case sensitive and must be entered in upper case.



3. The Client main screen opens.

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.

Card Holder Folder Location

On the Site Information form is a field entitled Card Holder Photo Location. The Keyscan Client, the Photo Badge Template Editor, and the CCTV & Video Control module reference the Card Holder Folder Location for all images. This includes photos for cardholder records and ID badges, maps of sites or buildings, signature images, if you have a signature capture device, and images captured on alarms by the CCTV system. Please note, with the exception of site or building maps, you must have the System V Photobadging and Verification and the System V CCTV modules installed to archive and access cardholder photos or alarm images.

By default, images are stored in the \Keyscan\Client Software folder. For either of the following two reasons, you may wish to create a specific directory before you start to complete the Site Information form. Image files can occupy a large volume of hard disk space. You must store them on a drive that has adequate space. On network configurations with multiple Client modules, you must store the images where they are accessible by all users; hence, you may have to create a folder at a location that satisfies this condition.

For a single PC configuration, specify a valid drive and folder. Select a drive accordingly.

- Single PC example – C:\Images

For a network configuration in a multi-user environment, it is important to specify a Card Holder Folder Location. The location you specify must be shareable by all users.

- Network example A – H:\Folder Name (mapped network drive)
- Network example B - \\Server Name\Share Name

In example A, all computers must have the same mapped drive. You may wish to consult with your IT department to set up a Card Holder Photo Location for network configurations.

Important

If you delete a site, including the default site My Site, that was set to Auto Start Communications Server in the Communications Manager, refer to Part 7: Communications Manager. The Auto Start function must be reset to a valid site in the appropriate Communications Manager(s). Otherwise the Communications Manager will malfunction on a re-boot and the Client module will report a communication failure.

To complete the Site Information form

From the Keyscan System V Client's main screen, select System Settings > Site Setup > Add New button from the Site Information Search form. If you previously created a site and are returning to add information, double click on the site name in the yellow table in the Site Search Information form.



1. In the Site Information form, click the cursor inside the Site ID text box and enter an ID name to a maximum of 8 characters. The purpose of a Site ID is to identify the site location where an alarm originates. Use a name that is understandable to other system users.
2. Click in the Site Name text box and enter the name of the site. Generally, this would be the proper name of the company or organization.
3. Complete the remaining site information from Site Location to Fax Number, whichever fields are applicable.
4. The Disable Auto Updates function is intended for sites that employ modems so the ACUs can be updated when a site relatively dormant. To activate this field, click in the box to the left of Disable Auto Updates. If your site communicates with a serial or TCP/IP connection, leave this function inactive. The system automatically uploads card records, time zones, and access levels to the ACUs.
5. To assign the site you are creating as the default site, click in the Default Site check box to activate the field, if it is not already active. The Default Site is the site listed in the Site ID text box when you log on.
6. If you are creating a host site, leave the default setting at No Collection and go to step 8. If you are creating a remote site, 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.
7. In the Host Telephone Number enter the telephone number that the remote site calls.
8. In the Access Control Unit Modem Initialization String, enter the initialization string. Consult your modem manufacturer's literature for the initialization string settings.
9. Specify a Card Holder Folder Location if your card holder records will incorporate photographic image files such as JPEGs or bitmaps.
10. Leave the Last Update and Last Update By fields blank. The software automatically updates these entries based on the date and system user.
11. Select the Panel Setup button to enter information about the Access Control Units and communications settings. See Site Unit Setup Form on page 34.

12. Select the Site Contacts button to register information about who to contact in an emergency. See the Site Contacts Information Form on page 36.
13. After you complete the above two forms, Site Unit Setup (required) and Site Contacts (optional), click on the Save & Exit button to return to the Client main screen.

Site Information form

The site information form has a Print Site setup button at the bottom. After you have completely set up your site, we recommend you return to the Site Setup form and print a hard copy of your site setup and file it for safekeeping. Instructions can be found on page 100.

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.

Note:

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 KEYSCAN.

To complete the Site Unit Setup form

To access the Site Unit Setup form, you must be in the Site Information form. Select the Panel Setup button.



1. Enter the corresponding information into the following four fields:

- Unit ID – Enter a unique Unit ID that distinguishes the ACU from other ACU panels at the site. The maximum is 6 alphanumeric characters.
 - Serial # - Enter the unit serial number which starts with an alpha character, followed by 4 numeric characters.
 - Unit Password (For a remote site setup, it is recommended to change the password from KEYSCAN; for a host site setup, it is recommended to retain the default password KEYSCAN.)
 - Unit Type - Use the down arrow to select the correct model.
2. Select the Active radio button in the upper right corner of the form, if it is not selected.
 3. Click the down arrow on the right side of the Communication Setup field and select the appropriate option for your system and enter the necessary settings:
 - For a Serial Connection – Specify the Baud Rate and Communication Port.
 - For a Network Connection – Specify the IP Address and Subnet Mask. See Appendix B to program the MSS – COMM, if applicable.
 - For a Dial Up Connection – Specify the Auto Dial Telephone Number, the number the host site dials to connect with a remote site, Baud Rate, Communication Port, and Initializing String, if necessary.
 4. If the access control unit has a host number to contact other than that specified on the Site Information form, enter the number in the Host Telephone Number text box, otherwise leave this field blank. This number on the Site Unit Setup form overrides that specified on the Site Information form.
 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 Geographical Time Zone Setting and select the site's correct time zone from the drop down list.
 7. Select the Add Unit button.
 8. If you are entering more than one unit, repeat the above steps, or if you have finished adding ACUs, select the Save & Exit button to return to the Site Information form.

Site Unit Setup form

[illegible]

Site Contacts Information Form

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

To complete the Site Contacts Information form

To access the Site Contact Information form, you must be in the Site Information form. Select the Site Contacts button.



1. Click on the Add New button in the Search Site Contact form to open the Site Contacts Information form.
2. Leave the Site Contact ID blank. This is a system assigned entry.
3. Click in the First Name text box and enter the contact's first name.
4. Complete the remaining fields from Last Name to Email address, whichever information is applicable. Do not use hyphens or brackets in the Telephone Number field.
5. Select the Save & Exit button.
6. To confirm your contact entry, click on the Find Contacts button.
7. To add another contact, click on the Add New button, or select the Exit button to return to the Site Information form.
8. Select the Save & Exit button > Exit button to return to the main screen.

Site Contact Information form

Site Contact Information

Site Contact ID

0

First Name

Edward

Last Name

Smith

User Location

555Main

Site Address

555 Main Street

Telephone Number

(416) 366-8899

Site City

Toronto

Telephone Extension

233

Province / State

Ontario

Fax Number

Country

Canada

Email Address

esmith@abccorp.com

Postal Code / Zip Code

Last Update

2001-12-18 15:52

Last Update By

KEYSCAN

Previous

Next

Save & Exit

Exit

Setting Up Doors for a New Site

Setting up doors for a new site involves naming the doors, establishing door groups, setting inputs and outputs, assigning time zones to doors, and assigning door groups access levels to doors. The topics listed under Setup Door information 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 forms require completion.

Create Door Group Names

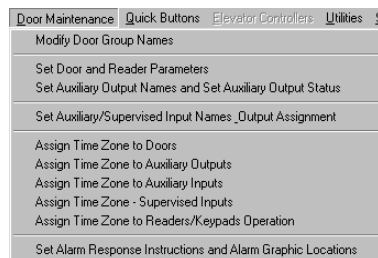
Creating Door Group Names allows you to place cardholders into specific groups based on their security and access levels. When creating a new door group name, it should correspond to descriptions that are generally applied to groups within your organization, as seen in the example of the Search Door Groups form on the following page.

Note

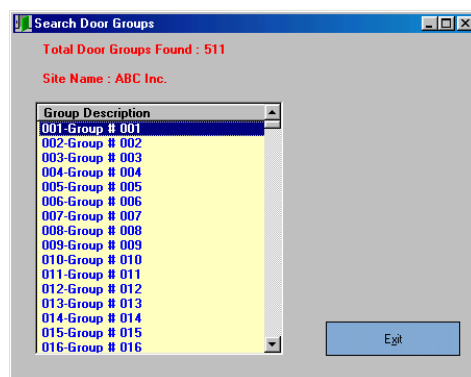
Door groups are listed under the Group Description field. Unassigned or open door groups appear as 001-Group # 1 to 511-Group # 511.

To Create a New Door Group Name

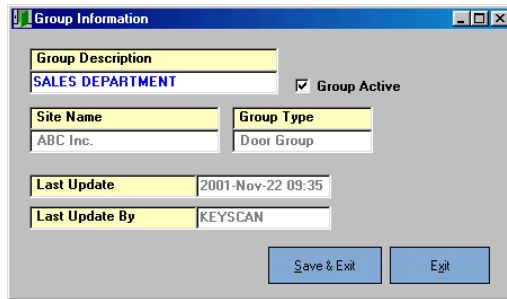
From the Keyscan System V Client's main screen, select Door Maintenance > Modify Door Group Names



1. From the Search Door Groups form, double click on an unassigned door group.



- Click the cursor inside the Group Description text box and type the name of the door group.

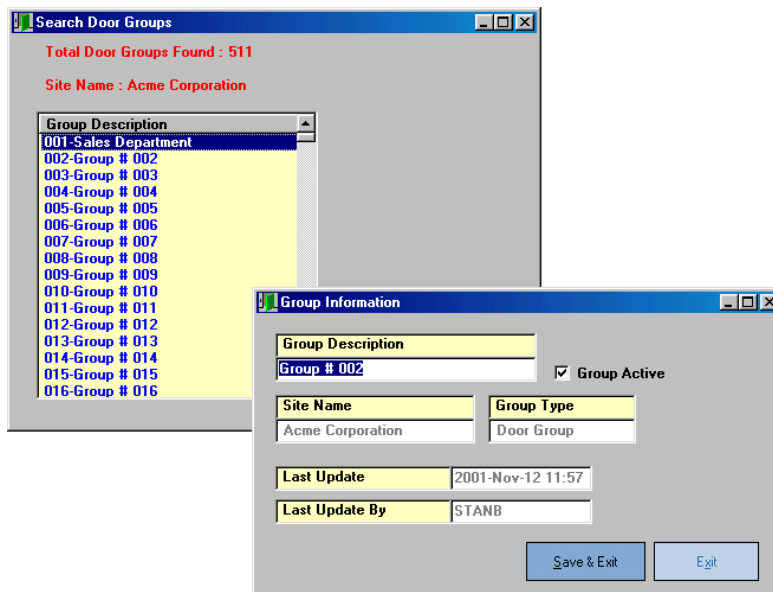


The 'Group Information' dialog box contains the following fields and controls:

- Group Description:** A text box containing 'SALES DEPARTMENT'.
- Group Active:** A checked checkbox.
- Site Name:** A text box containing 'ABC Inc.'.
- Group Type:** A dropdown menu showing 'Door Group'.
- Last Update:** A text box containing '2001-Nov-22 09:35'.
- Last Update By:** A text box containing 'KEYSCAN'.
- Buttons:** 'Save & Exit' and 'Exit'.

- Leave the Group Active field enabled. The box has a check mark.
- Select the Save & Exit button.
- To add another door group name, repeat steps 1 to 4, or to return to the main screen, select the Exit button.

Search Door Groups/Group Information forms



The 'Search Door Groups' dialog box displays the following information:

- Total Door Groups Found:** 511
- Site Name:** Acme Corporation
- Group Description List:**
 - 001-Sales Department
 - 002-Group # 002
 - 003-Group # 003
 - 004-Group # 004
 - 005-Group # 005
 - 006-Group # 006
 - 007-Group # 007
 - 008-Group # 008
 - 009-Group # 009
 - 010-Group # 010
 - 011-Group # 011
 - 012-Group # 012
 - 013-Group # 013
 - 014-Group # 014
 - 015-Group # 015
 - 016-Group # 016

The 'Group Information' dialog box (shown in the foreground) displays the following information for the selected group:

- Group Description:** Group # 002
- Group Active:** A checked checkbox.
- Site Name:** Acme Corporation
- Group Type:** Door Group
- Last Update:** 2001-Nov-12 11:57
- Last Update By:** STANB
- Buttons:** 'Save & Exit' and 'Exit'.

Create Door Names and Reader Outputs

Readers control doors within the Keyscan system. There are two forms to complete – the Reader Information form and the Door Output # form in order to set up the readers at each door.

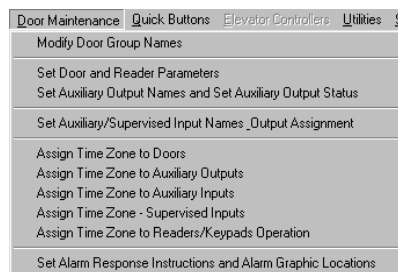
The Reader Information form is used to name the doors that each reader controls. These are referred to as reader port locations. It is best to use clear and descriptive names such as Main Front Door, Employee Door, Shipping Door etc. The Reader Information form is also used to specify the direction of access IN or OUT and, if applicable, to invoke the Anti-Passback option. Anti-Passback prevents one individual from passing his or her card back to another individual for later use. When Anti-Passback is invoked, after a card enters a controlled enter/exit environment, the card must exit, before the system permits the card to enter again.

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. Assigning a door output identifies which door either experienced a forced entry or was held open longer than the allowable specified time limit. The following table outlines ACU models and the maximum doors/door outputs available:

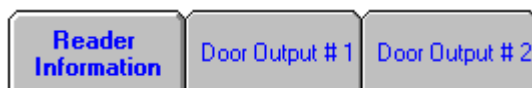
Unit	Doors	Door Outputs
CA – 200	2	2
CA – 4000	4	4
CA – 8000	8	8

To Create Door Names

From the Keyscan System V Client's main screen, select Door Maintenance > Set Door & Reader Parameters.



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



2. If there is more than one access control unit on 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.
3. Click the cursor inside the Reader Port #1 text box and type the name of the door where

the reader is located.

4. Click the down arrow to the right of the Direction field and select one of the two options:
 - In
 - Out
5. To activate the Anti-Passback option, click inside the box.
6. Repeat steps 2 to 5 until each door has been assigned a Reader Port name with the corresponding fields completed.

Set Door and Reader Parameters form – Reader Information

To Assign Door Outputs

1. Select the Door Output # 1 tab. You will now set door outputs for the door that was assigned to Reader Port Name # 1. The name of the door is listed under the Door Name # 1 field. See page 42 for an example of the Door Output # form.

2. 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. (0 toggle = toggles the output state.)
3. 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.
4. Click on the down arrow on the right side of Door Operation Mode and select one of the following door exit options. For an explanation of Door Operation Mode and the three settings, see Note A on the following page.
 - Request to exit. Unlocks door and shunts door contact.
 - Request to exit. Shunts door contact only.

- Free egress. Door held open alarm only.
5. Click on the down arrow on the right side of the Alarm on Forced Entry Output and select an output. See Note B for more information. If you select 000 – No Output Assigned, an alarm warning does not occur if there is a forced entry at this door.
 6. Click on the down arrow on the right side of the Alarm Held Open Timer Output and select an output. See Note C for more information. 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 at this door.
 7. If applicable, click on the down arrow on the right side of the Handicap Door Timer field and select a time, if applicable. The range is 1 to 99 seconds. The Handicap feature is an optional component.
 8. If applicable, click on the down arrow on the right side of the Handicap Door Held Open field and select a time, if applicable. The range is 1 to 99 seconds.
 9. 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.
 10. Click on the Save Doors button when you have completed naming and assigning outputs to your doors.

Set Door and Reader Parameters form – Door Output

Set Door and Reader Parameters

Site Name: Acme Corporation Unit ID: CA200 Total Active Doors: 4

Reader Information | **Door Output # 1** | Door Output # 2 | Door Output # 3 | Door Output # 4 | Unit Option Not Available | Unit Option Not Available | Unit Option Not Available | Unit Option Not Available

Door Name # 1: Front Door

Door Relay Unlock Time: 5 Door Held Open Time: 25

Door Operation Mode: 1- Request to exit. Unlocks door

Alarm on Forced Entry Output: 000 - No Output Assigned Alarm Held Open Timer Output: 000 - No Output Assigned

Handicap Door Timer: 10 Handicap Door Held Open: 25

Reader Name	Antipass	Direction
<input checked="" type="checkbox"/> Front Door	No	In
<input type="checkbox"/> Employee Door	No	In

Save Exit

Note A

A Door Operation Mode must be selected to prevent an alarm event when someone opens a door to **exit** a controlled access area. The three Door Operation Modes are designed for specific door-exit hardware configurations as listed immediately below:

Request to Exit – Unlocks Door and Shunts Contact is selected 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.

Request to Exit – Shunts Door Contact Only is selected 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 is selected 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.

Note B

Assigning output numbers will depend on the configuration of your access control unit and how you wish to set alarm events criteria. As an example, if your system used a CA 200 ACU, then you would have two available outputs, numbered 001 & 002. If your system was monitoring two doors and you wanted to have a forced entry alarm for each door, then door #1 would be assigned output 001 and door #2 would be assigned output 002. Otherwise, if you selected the same output number for both doors, the system would report that there was a forced entry at both doors because the readers were both assigned the same output.

Note C

It is conceivable that you may have assigned all your output #s to an alarm on forced entry. If this condition is true and you want to assign an output number to the Alarm Held Open Timer, then you have the following option. Assign both the Alarm on Forced Entry and Alarm Held Open Timer the same output number at their respective doors. The system will report an alarm event at the door but will not specify which type of event occurred.

Set Door Time Zones

The Set 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. Time zones may have multiple schedules.

- Time zones/schedules are based on a 24-hour clock.
- Maximum combined total of time zones and schedules is 512.
- Maximum range of a time zone is from 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 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.

The table below illustrates some examples of time zone settings that fall within a daily 24-hour clock and time zone settings that overlap midnight.

Time Zone - Within 24 Hour Clock							
Example – Monday to Friday, 9:00 a.m. to Friday 5:00 p.m.							
	Mon	Tues	Wed	Thurs	Fri	Sat	Sun
Start Time	09:00	09:00	09:00	09:00	09:00	00:00	00:00
End Time	17:00	17:00	17:00	17:00	17:00	00:00	00:00

Time Zone – Overlaps Midnight							
Example – Monday to Sunday 5:00 p.m. to 2:00 a.m.							
	Mon	Tues	Wed	Thurs	Fri	Sat	Sun
Start Time	17:00	17:00	17:00	17:00	17:00	17:00	17:00
End Time	02:00	02:00	02:00	02:00	02:00	02:00	02:00

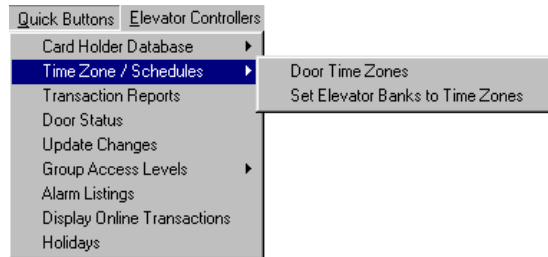
Time Zone – Overlaps Midnight							
Example – Monday to Friday 5:00 p.m. to 2:00 a.m. (Time zone concludes Saturday am)							
	Mon	Tues	Wed	Thurs	Fri	Sat	Sun
Start Time	17:00	17:00	17:00	17:00	17:00	00:00	00:00
End Time	02:00	02:00	02:00	02:00	02:00	02:00	00:00

Note

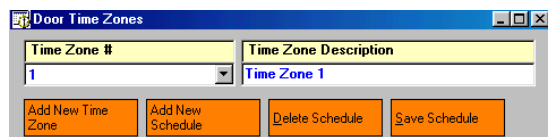
Setting door time zones does not regulate elevators. Elevator time zones are set from the Assign Elevator Banks to Time Zones form.

To Add a Door Time Zone

From the Keyscan System V Client's main screen, select the Quick Buttons menu > Time Zone/Schedules > Door Time Zones



1. Click on the Add New Time Zone button. The program assigns a Time Zone #.



2. Enter a descriptive title in the Time Zone Description text box to identify the time zone.
3. 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.
4. 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.
5. Select the hour in the lower box under Mon and click the up or down arrow at the right to set the end hour.
6. Select the minutes and click the up or down arrow to set the end minutes.
7. Repeat steps 3 to 6 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.
8. Click on the Save Schedule button.
9. To add another time zone, click on the Add New Time Zone button and repeat steps 2 to 8. To return to the main screen, click on the Exit button.

Door Time Zones form set to start at 9:00 a.m. and end at 5:00 p.m. (17:00) Monday through Sunday

The screenshot shows the 'Door Time Zones' window. At the top, 'Time Zone #' is set to 1 and 'Time Zone Description' is 'Time Zone 1'. Below are buttons for 'Add New Time Zone', 'Add New Schedule', 'Delete Schedule', and 'Save Schedule'. A status bar indicates 'Total Time Zones = 3 Total Schedules = 5'. On the left, there are buttons for 'Copy Monday to Friday', 'Copy Monday to Sunday', 'Copy Monday to All', 'Reset All', and 'First Person In'. The main area shows 'Time Zone 1' with 'Schedule 1 of 3'. The schedule table is as follows:

Mon	Tues	Wed	Thur	Fri
09:00	09:00	09:00	09:00	09:00
17:00	17:00	17:00	17:00	17:00
Sat	Sun	Holiday 1		
09:00	09:00	00:00		
17:00	17:00	00:00		
		Holiday 2		
		00:00		
		Holiday 3		
		00:00		
		00:00		

At the bottom, it says 'Time Zone Assigned to: Inputs' and has an 'Exit' button.

Door Time Zone form set to Start at 5:00 p.m. and (17:00) and End at 2:00 a.m. Monday afternoon to Saturday morning

The screenshot shows the 'Door Time Zones' window. At the top, 'Time Zone #' is set to 005 - Factory Afternoon and 'Time Zone Description' is 'Factory Afternoon'. Below are buttons for 'Add New Time Zone', 'Add New Schedule', 'Delete Schedule', and 'Save Schedule'. A status bar indicates 'Total Time Zones = 5 Total Schedules = 9'. On the left, there are buttons for 'Copy Monday to Friday', 'Copy Monday to Sunday', 'Copy Monday to All', 'Reset All', and 'First Person In'. The main area shows 'Factory Afternoon' with 'Schedule 1 of 1'. The schedule table is as follows:

Mon	Tues	Wed	Thur	Fri
17:00	17:00	17:00	17:00	17:00
02:00	02:00	02:00	02:00	02:00
Sat	Sun	Holiday 1		
00:00	00:00	00:00		
02:00	00:00	00:00		
		Holiday 2		
		00:00		
		Holiday 3		
		00:00		
		00:00		

At the bottom, it says 'Time Zone Assigned to: NO DEVICES' and has an 'Exit' button.

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.

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. Be sure the Time Zone # is highlighted in blue.
- Click on the Add New Schedule button.
 - 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.
 - 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.
 - Select the hour in the lower box under Mon and click the up or down arrow at the right to set the end hour.
 - Select the minutes and click the up or down arrow to set the end minutes.
 - Repeat steps 3 to 6 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.
 - Click on the Save Schedule button.
 - To add another schedule, click on the Add New Schedule button and repeat steps 2 to 8. To return to the main screen, click on the Exit button.

First Person In

The First Person In option is a safeguard to keep a door locked after its assigned time zone starts. Until a cardholder from an authorized door group presents his or her card to the reader, the time zone remains locked. This feature restricts cardholders or non-authorized persons from gaining access to your building or an area within the building before the First Person In feature unlocks the time zone.

As an example, Door A's assigned time zone starts at 08:00. Door A leads to a sensitive work area and management does not wish employees entering door A until a supervisor has arrived to oversee the area. To ensure that no one accesses door A until a supervisor is present, Door A would be set for First Person In. Supervisors would be assigned to a different time zone from the employees.

Time Zone	Hours	Door	Door Group	First Person In
Time Zone 1	8:00 – 16:30	Door A	Production Staff	Enabled (✓)
Time Zone 2	8:00 – 16:30	Door A	Supervisors	Disabled ()

Now employees, who have access to door A after 08:00, would be denied entry until a supervisor has used his or her card to unlock the time zone. First Person In is based on time zones; it cannot be set to an individual cardholder.

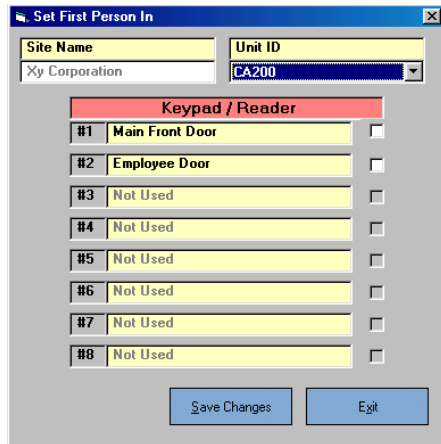
To Set First Person In

- Click on the First Person In button on the Door Time Zones form.
- Click on the down arrow of the Unit ID field and select the appropriate access control unit.
- 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.

4. Click on the Save Changes button to return to the Door Time Zones form.

Set First Person In form



The image shows a software window titled "Set First Person In". At the top, there are two input fields: "Site Name" with the text "Xy Corporation" and "Unit ID" with a dropdown menu showing "CA200". Below these is a section header "Keypad / Reader" in a red box. Under this header is a list of eight items, each with a number in a box, a text field, and a checkbox. The items are: #1 Main Front Door, #2 Employee Door, #3 Not Used, #4 Not Used, #5 Not Used, #6 Not Used, #7 Not Used, and #8 Not Used. At the bottom of the window are two buttons: "Save Changes" and "Exit".

Keypad / Reader		
#1	Main Front Door	<input type="checkbox"/>
#2	Employee Door	<input type="checkbox"/>
#3	Not Used	<input type="checkbox"/>
#4	Not Used	<input type="checkbox"/>
#5	Not Used	<input type="checkbox"/>
#6	Not Used	<input type="checkbox"/>
#7	Not Used	<input type="checkbox"/>
#8	Not Used	<input type="checkbox"/>

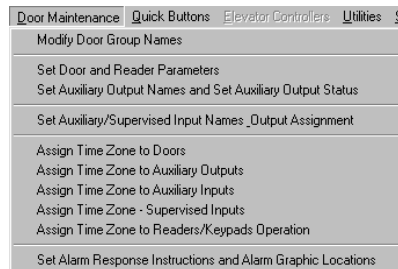
Save Changes Exit

Set Auxiliary Output Names & Set Auxiliary Output Status

The Set Auxiliary Output Names & Set Auxiliary Output Status form is used to directly access control alarms to intrusion devices, lock a door, or some other type of event. Your installer should determine these settings.

To Set Auxiliary Output Names & Set Auxiliary Output Status

From the Keyscan System V Client's main screen, select Door Maintenance > Set Auxiliary Output Names & Set Auxiliary Output Status > No - if the warning message appears.



1. 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 within the site. The total number of auxiliary outputs is listed in the Number of Auxiliary Output field.
2. Double click on the auxiliary output listed in the yellow table to be named.
3. Enter a name in the ON AO Name text box.
4. Enter a name in the OFF AO Name text box.
5. Click on the OK button when you have completed naming the auxiliary outputs.

Set Auxiliary Output Names & Set Auxiliary Output Status form

The screenshot shows the 'Set Auxiliary Output Names & Set Auxiliary Output Status' form. It includes fields for Site Name (Xy Corporation), Unit ID (CA200), and Number of Auxiliary Output (2). Below these is a table titled 'Total Active Auxiliary Outputs: 2' with columns for AO Status, AO #, Auxiliary ON Name, and Auxiliary OFF Name. The table contains two rows: Row 1 has 'Aux. Status ON' checked, AO # 1, ON AO # 01, and OFF AO # 01. Row 2 has 'No Aux. Status' checked, AO # 2, ON AO # 02, and OFF AO # 02. At the bottom, there are input fields for AO #, ON AO Name, and OFF AO Name, with buttons for OK, Cancel, Toggle All On, Toggle All Off, Apply Changes, and Exit.

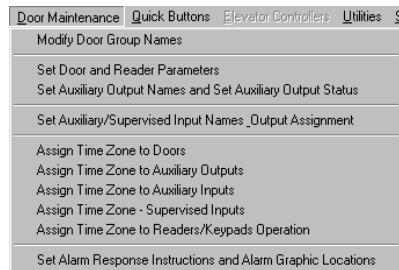
AO Status	AO #	Auxiliary ON Name	Auxiliary OFF Name
<input checked="" type="checkbox"/> Aux. Status ON	1	ON AO # 01	OFF AO # 01
<input checked="" type="checkbox"/> No Aux. Status	2	ON AO # 02	OFF AO # 02

Set Auxiliary/Supervised Input Names-Output Assignment

By assigning outputs to auxiliary/supervised inputs, you assign those inputs to activate outputs in alarm conditions. (Your installer should determine these settings.)

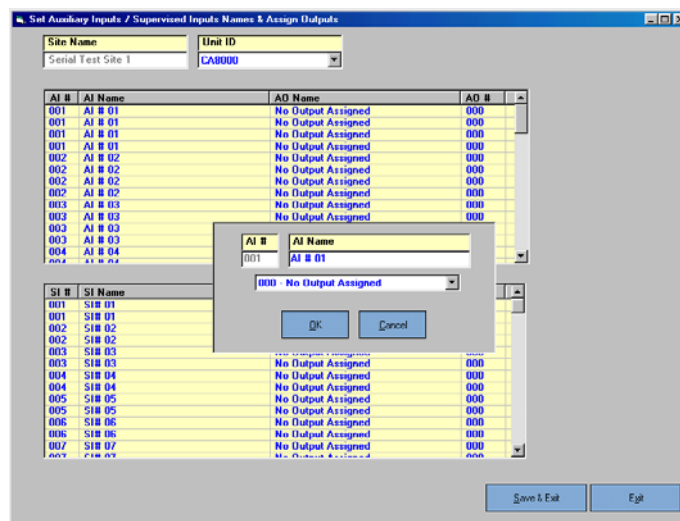
To Set Auxiliary / Supervised Input Names_Output Assignments

From the Keyscan System V Client's main screen, select the Door Maintenance menu > Set Auxiliary / Supervised Input Names_Output Assignments.



1. Click on the down arrow of the Unit ID field and select the unit from the drop down list.
2. Double click on the auxiliary input (AI) or the supervised input (SI) from the appropriate list.
3. Click in the AI Name or SI Name text box and enter the name of the input.
4. 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.
5. Click on the OK button.
6. Click on the Save & Exit button to return to the main screen.

Set Auxiliary / Supervised Input Names & Assign Outputs form



Assign Time Zones to Doors

The Assign Time Zones to 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.

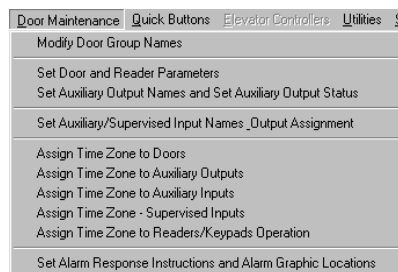
Note

When you assign time zones to automatically unlock doors, it is strongly recommended to use the First Person In option, especially for exterior doors. First Person In stops the time zone from automatically unlocking the door until someone presents a valid card to the reader. An example might be during a severe snowstorm 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 overriding the time zone until a designated card holder arrives at the site. See First Person In on page 47 for more information.

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

To Assign Time Zones to Automatically Lock/Unlock Doors

From the Keyscan System V Client's main screen, select the Door Maintenance menu > Assign Time Zone to Doors



1. In the Access Unit Name field, double click in the yellow table under the door number for the appropriate access control unit. The Door Name and Door Output # fields display your selection.
2. In the Time Zone Selection box, click inside the radio button on the left side of 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.
3. 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.
4. Select the OK button and repeat for any doors that you want automatically unlocking and locking to a time zone.
5. Select Save & Exit to return to the main screen.

Assign Time Zone to Automatically Lock/Unlock Doors form

Assign Time Zone to Automatically Lock/Unlock Doors

Site Name: SERIAL17 Door Name: Front Door Door Output #: 1

Access Unit Name	1	2	3	4	5	6	7	8
CA200	N/A	N/A	---	---	---	---	---	---
CA201	N/A	N/A	---	---	---	---	---	---
CA4000	N/A	N/A	N/A	N/A	---	---	---	---
CA4001	N/A	N/A	N/A	N/A	---	---	---	---
CA8000	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CA8001	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

☐ Not Applicable
☒ Time Zone Limited Access
☐ Shunt Door Contact Only (Door Remains Locked)

17:3 Time Zone 3

OK Cancel Time Zones

Time Zone 3 Schedule 1 of 1

Mon	Tues	Wed	Thur	Fri	Sat	Sun
09:00	09:00	09:00	09:00	09:00	00:00	00:00
17:00	17:00	17:00	17:00	17:00	00:00	00:00
Holiday 1	Holiday 2	Holiday 3				
00:00	00:00	00:00				
00:00	00:00	00:00				

Previous Next

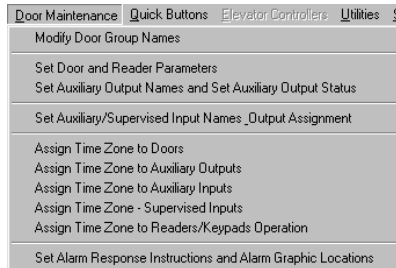
Save & Exit Exit

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.

To Assign Time Zones to Auxiliary Outputs

From the Keyscan System V Client's main screen, select the Door Maintenance menu > Assign Time Zones to Auxiliary Outputs



1. In the yellow table, double click on the appropriate box that lines up with the Access Unit Name and Output Number that is being assigned a time zone.
2. Click in the radio button to activate Time Zone Limited Access.
3. 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.
4. Click on the OK button.
5. After you have completed assigning time zones to auxiliary outputs, click on the Save & Exit button to return to the main screen.

Assign Time Zone to Automatically Toggle Auxiliary Outputs form

Access Unit Name	1	2	3	4	5	6	7	8
CA200	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CA200B	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CA4000	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CA400B	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CA8000	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
CA800B	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

☒ Not Applicable
☐ Time Zone Limited Access

Time Zone Limited Access dropdown menu:
 TZ-1 Time Zone 1
 TZ-2 Time Zone 2
 TZ-3 Time Zone 3
 TZ-4 Time Zone 4

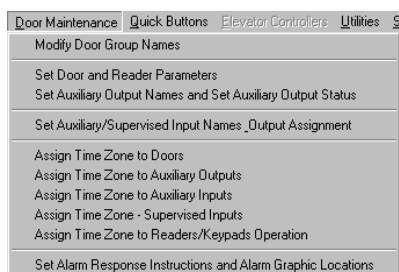
Save & Exit Exit

Assign Time Zones to Auxiliary Inputs

Use the Assign Time Zones to Auxiliary Inputs feature to automatically arm and disarm auxiliary inputs at designated times depending on your site's security requirements.

To Assign Time Zones to Auxiliary Inputs

From the Keyscan System V Client's main screen, select the Door Maintenance menu > Assign Time Zones to Auxiliary Inputs.



1. Click on the down arrow of the Unit ID field, and select the unit name from the drop down list.
2. Select the auxiliary input from the table that lists all the auxiliary inputs available.
3. Click in the radio button to activate Time Zone Limited Access.
4. Click on the down arrow below and to the right of Time Zone Limited Access and select the appropriate time zone for the auxiliary input.
5. Click on the OK button.
6. 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 Auxiliary Inputs form

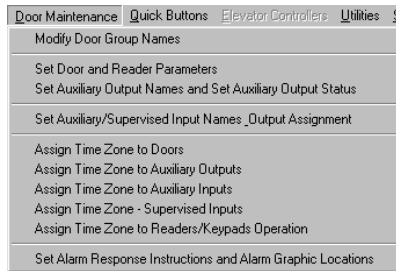
The screenshot shows the 'Assign Time Zone to Auxiliary Inputs' form. It includes a 'Site Name' field with 'TEST1' and a 'Unit ID' dropdown menu with 'CA200'. Below these is a table with columns 'AI #', 'Auxiliary Input Name', and 'Time Zone Assignment'. The table lists auxiliary inputs AI #1 through AI #8, all with 'N/A' in the 'Time Zone Assignment' column. To the right of the table are radio buttons for 'Not Applicable' and 'Time Zone Limited Access'. Below the radio buttons are 'OK', 'Cancel', and 'Edit Time Zones' buttons. At the bottom right, there is a section for 'Time Zone Limited Access' with a dropdown menu and a table for assigning time zones to days of the week (Mon, Tues, Wed, Thurs, Fri, Sat, Sun) and holidays (Holiday 1, Holiday 2, Holiday 3). At the bottom of the form are 'Previous', 'Next', 'Save & Exit', and 'Exit' buttons.

Assign Time Zones to Supervised Inputs

Use the Assign Time Zones to Supervised Inputs feature to automatically arm and disarm supervised inputs at designated times depending on your site's security requirements. Supervised inputs are not available on the CA 200 model.

To Assign Time Zones to Supervised Inputs

From the Keyscan System V Client's main screen, select the Door Maintenance menu > Assign Time Zones - Supervised Inputs.



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

Assign Output to Auxiliary Inputs & Supervised Inputs form

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 reader and a keypad. If the door has only one of the two, either a reader or a keypad, you can bypass this step.

By default, the system sets the Access Setup Mode, the Access Zone ON, and the Access Zone OFF fields to Card or Keypad.

The three reader/keypad setup modes are outlined below:

- Card or Keypad (Only 1 of the two is used to access the door.)
- Card Only (Only a card reader is used to access the door.)
- Card and Keypad (A card reader and a keypad are used to access the door.)

When the door's time zone is ON, one of the following three conditions would be in effect:

- If Access Zone ON is set to Card or Keypad, valid card holders 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 card holders present their card to the reader to access the door.
- If Access Zone ON is set to Card and Keypad, valid card holders present their card to the reader and enter their Personal Identification Number on the keypad to access the door.

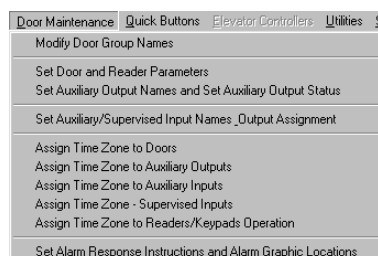
The same holds true for Access Zone OFF, whichever card/keypad option is selected.

Note

If your system uses either a 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 model reader/keypads, the individual presses the star (*) key first, then enters his or her 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.)

To Set Readers/Keypads

From the Keyscan System V Client's main screen, select the Door Maintenance menu > Assign Time Zones to Readers/Keypads Operations.



1. Click on the down arrow below the Unit ID field and select the appropriate access control unit from the drop down list.
2. Click on the down arrow below the Access Mode Setup field for the door you are assigning reader/keypad access to and select one of the available options from the drop down list.
3. Under the Time 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.
4. Click inside the radio button on the left side of Time Zone Limited Access field to activate this option.
5. Click on the down arrow, located above the Edit Time Zones button, and select the time zone from the drop down list. A copy of the time zone is exhibited at the bottom.
6. Select OK.
7. Click on the down arrow below the Access Zone ON field and select one of the available options from the drop down list.
8. Click on the down arrow below the Access Zone OFF field and select one of the available options from the drop down list.
9. To assign reader/keypad access to another door, repeat the above steps.
10. Select Save & Exit after you have completed assigning reader/keypad access to the doors in the system.

Reader/Keypad Access Settings and Time Zone Operation form

The screenshot shows the 'Reader/Keypad Access Setup and Time Zone Operation' window. At the top, 'Site Name' is 'SERAILIT' and 'Unit ID' is 'CA200'. Below is a table for door configuration:

Keycard / Reader	Access Mode Setup	Time	Access: Zone ON	Access: Zone OFF
#1 Front Door	Card and Keypad	TZ-2	Card and Keypad	Card and Keypad
#2 Employee Door	Card and Keypad	TZ-1	Card and Keypad	Card and Keypad
#3 Not Used				
#4 Not Used				
#5 Not Used				
#6 Not Used				
#7 Not Used				
#8 Not Used				

A modal dialog for 'Time Zone 1' is open, showing 'Time Zone Limited Access' selected. Below the dialog, the 'Time Zone 1' schedule is shown for 'Schedule 1 of 1'.

Mon	Tues	Wed	Thur	Fri	Sat	Sun
08:00	08:00	08:00	08:00	08:00	08:00	08:00
16:45	16:45	16:45	16:45	16:45	16:45	16:45
Holiday 1	Holiday 2	Holiday 3				
00:00	00:00	00:00				

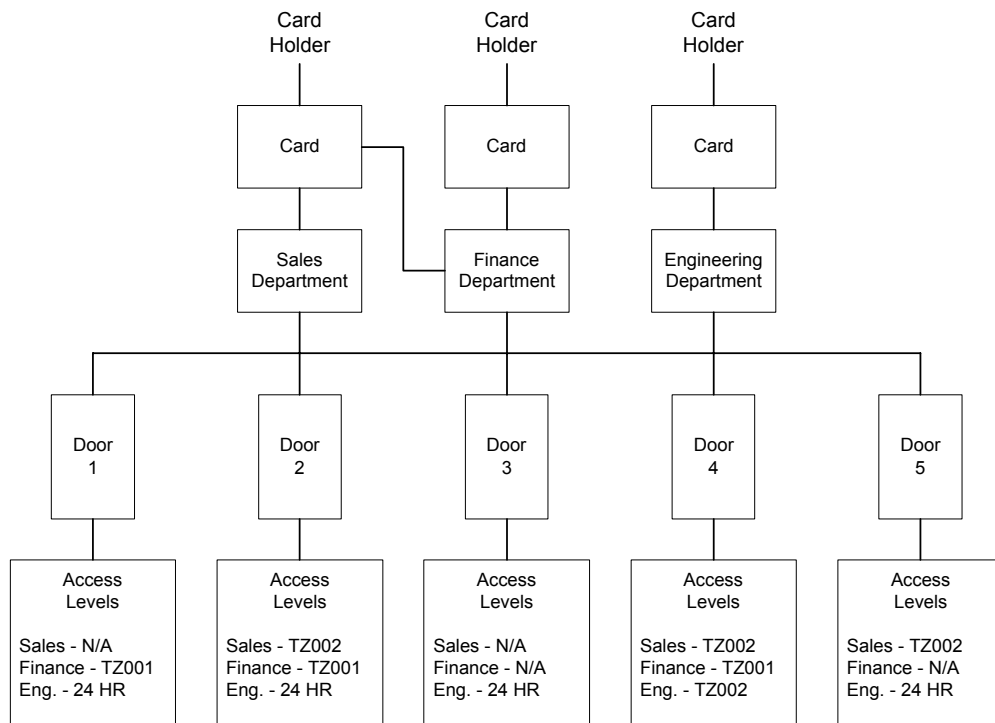
Buttons at the bottom include 'Previous', 'Next', 'Save & Exit', and 'Exit'.

Assign Door Group Access Levels

The Door Group Access Levels form is 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 following diagram illustrates an example site where there are 3 different door groups: Sales Department, Finance Department, and Engineering Department. Five doors are controlled by an ACU. Door group access levels are summarized under each door. You will note that door groups have either: 24 hour access, no access, or limited access based on a time zone.

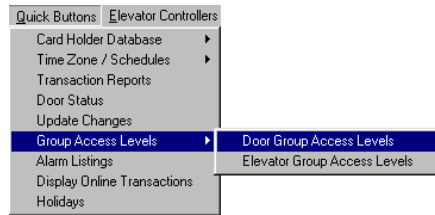


The Door Group Access Levels form is laid out in a table format. The door group names are listed in a column on the left, the reader (door) numbers are listed in a row along the top, and the access levels are set out in a grid in the body of the table.

Door Group Name	1	2	3	4	5
001 - Sales Dept	N/A	TZ-002	N/A	TZ-002	TZ-002
002 - Finance Dept	TZ-001	TZ-001	N/A	TZ-001	N/A
003 - Engineering Dept	24 HR	24 HR	24 HR	TZ-002	24 HR

To Assign Door Group Access Levels to Doors

From the Keyscan System V Client's main screen, select Quick Buttons > Group Access Levels > Door Group Access Levels.



- Click on the down arrow under Reader Selection, and select the door from the drop down list. By default, all door groups for the selected door are highlighted in black. 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 and the 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 multiple doors, click on the upper left grid location and hold and drag the mouse to the lower right grid location.



- Select one of the radio buttons to determine the access level:

- 24 Hour Access (If 24 Hour Access is selected, see step 4.)
- No Access (If No Access is selected, see step 4.)
- Time Zone Limited Access (If Time Zone Limited Access is selected, see step 3.)

- 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.

4. Select OK.
5. Repeat the above steps until all door groups have been assigned an access level for each door.
6. Select the Save & Exit button.

Door Group Access Levels form

The screenshot displays the 'Door Group Access Levels' form. At the top, there are fields for 'Site Name' (SERIAL1), 'Reader Selection' (CA200 - Front Entrance Door), 'Reader Direction' (In), and 'Unit ID' (CA200). Below these is a table with columns for 'Door Group Name' and 10 time zones (TZ-001 to TZ-010). The table lists various door groups such as '001 - SALES STAFF', '002 - MANAGEMENT ACCESS', '003 - RESEARCH & DEVELOPMENT', '004 - ADMINISTRATION', '005 - WAREHOUSE STAFF', '006 - SALES SUPPORT GROUP', '007 - HUMAN RESOURCES', '008 - CORPORATE VISITORS', '009 - ELECTRICAL CONTRACTORS', '010 - SECURITY STAFF', '011 - VISITORS SHORT TERM', and '012 - VENDORS'. A modal window is open for 'TZ 001 Time Zone 1', showing a schedule grid with columns for days of the week and time slots. The grid includes options for '24 Hour Access', 'No Access', and 'Time Zone Limited Access'. Below the grid are buttons for 'Previous' and 'Next'. At the bottom of the modal are 'Save & Exit' and 'Exit' buttons.

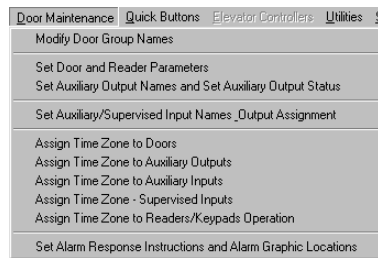
Set Alarm Response Instructions/Alarm Graphic Locations

The Set Alarm Response Instructions & Alarm Graphic Locations is an important form that provides critical contact and location information in the event of an emergency. During system monitoring, if an alarm condition is triggered, it is listed on the lower half of the Client main screen in the Alarm Events section.

The person monitoring the system would double click on the alarm event listed, which opens the Set Alarm Response Instructions & Alarm Graphic Locations form, and the proper authorities can be alerted.

To Set Alarm Response Instructions & Alarm Graphic Locations

From the Keyscan System V Client's main screen, select the Door Maintenance menu > Set Alarm Response Instructions & Alarm Graphic Locations.



1. Click on the down arrow for the Unit ID, Input Name, Connection Number field and select the door name from the drop down list.
2. In the Location text box, enter a brief description of the door's location.
3. In the Instructions, enter brief instructions to be carried out in the event of an emergency.
4. Click on the down arrow for the Alarm Contacts field and select a name from the drop down list. The names listed were input from the Site Contacts form under System Settings > Site Setup > Site Information.
5. Click on the down arrow for the Emergency Contacts field and select a name from the drop down list.
6. To incorporate floor plans or building schematics, click on the Load Picture button (Optional). *
7. From the Select Alarm Bitmap dialog box, navigate to the directory and select the diagram file.
8. Click on the Open button.
9. Click on the Save & Exit button.

* Note

Floor plans or building schematics must be created by the Maps application of the Keyscan Photo Badge Template Editor before they can be incorporated in the Set Alarm Response Instructions & Alarm Graphic Locations form. The Photo

Badge Template Editor saves files in a file format called MAP files, a type of bitmap.

Set Alarm Response Instructions & Alarm Graphic Locations form

The screenshot shows a software window titled "Set Alarm Response Instructions & Alarm Graphic Locations". It contains several input fields and buttons. At the top, there is a dropdown menu for "Unit ID, Input Name, Connection Number" with "CA200 Staff West Entrance" selected. Below this is a "Location" dropdown menu with "North West Corner of Building Langford Rd" selected. To the right of the location is a text area for "Instructions" containing the text: "During office hours call Jim Smith. After hours Acme Security is dispatched to location". Below the location dropdown are two columns of dropdown menus labeled "Alarm Contacts" and "Emergency Contacts", each with three empty slots. At the bottom left, there is a text field for a file path: "C:\Program Files\Keyscan\Client Software\ABC_Floor.map", and a "Load Picture" button. At the bottom right, there are four buttons: "Show Map", "Clear", "Save & Exit", and "Exit".

Set Alarm Response Instructions & Alarm Graphic Locations form with map loaded

This screenshot shows the same software window as the previous one, but with a map loaded. The map is a floor plan diagram with several rooms labeled: "Lobby Door", "Showroom", "Shop Door", "Employee Side Door", and "Parts Room". The map is enclosed in a blue border. The "Instructions" text area and the "Alarm Contacts" and "Emergency Contacts" dropdowns are still visible. The "Show Map" button at the bottom left is now labeled "Hide Map". The "Clear", "Save & Exit", and "Exit" buttons remain at the bottom right.

Setting Up Elevator Information

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

The card holder presents his or her card to the reader and presses a floor button. If the card holder has clearance within the specified time zone for the floor that was selected, the system allows access to the floor. If the card holder does not have clearance, the floor button is locked out and the elevator remains stationary.

Note

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 step.

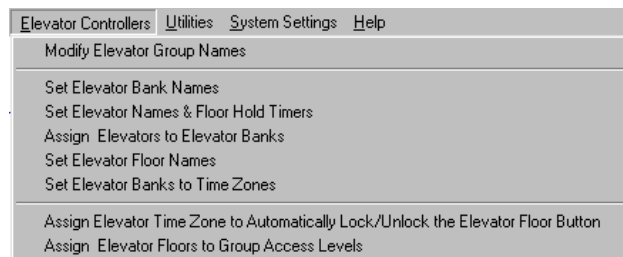
Unassigned elevator groups appear as 001-Group # 1 etc. You may create up to 511 different elevator groups.

Add Elevator Group Names

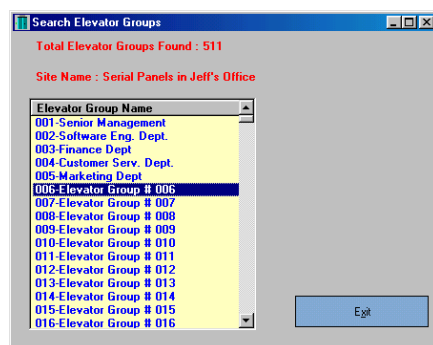
Creating Elevator Group Names allows you to place cardholders into specific groups based on their security and access levels. When creating a new elevator group name, it should correspond to descriptions that are generally applied to groups within your organization, as well as how you may have named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

To Add Elevator Group Names

From the Keyscan System V Client's main screen, select Elevator Controllers > Modify Elevator Group Names.



1. Double click on an open elevator group from the Search Elevator Groups form.



2. From the Group Information form, click the cursor inside the Group Description text box and type the name of the elevator group.

Group Information

Group Description
Elevator Group # 006

☒ Group Active

Site Name
Serial Panels in Jeff's Office

Group Type
Elevator Group

Last Update
2001-Oct-10 12:50

Last Update By
KEYSCAN

Save & Exit Exit

3. Select the Group Active box to activate the elevator group if it is inactive. The box has a check mark to indicate this field is active.
4. Select Save & Exit.
5. To add another elevator group name, repeat the above steps, or select the Exit button to return to the main screen.

Search Elevator Groups form and Group Information form

Search Elevator Groups

Total Elevator Groups Found : 511

Site Name : Serial Panels in Jeff's Office

Elevator Group Name
001-Senior Management
002-Software Eng. Dept.
003-Finance Dept
004-Customer Serv.
005-Marketing Dept
006-Elevator Group
007-Elevator Group
008-Elevator Group
009-Elevator Group
010-Elevator Group
011-Elevator Group
012-Elevator Group
013-Elevator Group
014-Elevator Group
015-Elevator Group
016-Elevator Group

Group Information

Group Description
Sales Department

☒ Group Active

Site Name
Serial Panels in Jeff's Office

Group Type
Elevator Group

Last Update
2001-Oct-10 12:50

Last Update By
KEYSCAN

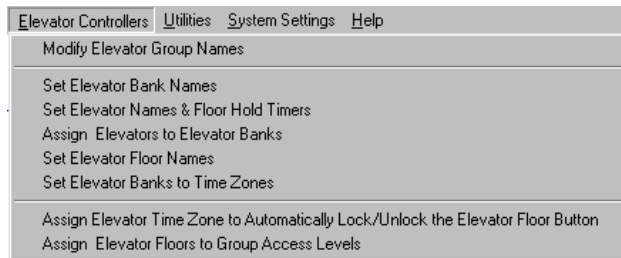
Save & Exit Exit

Set Elevator Bank Names

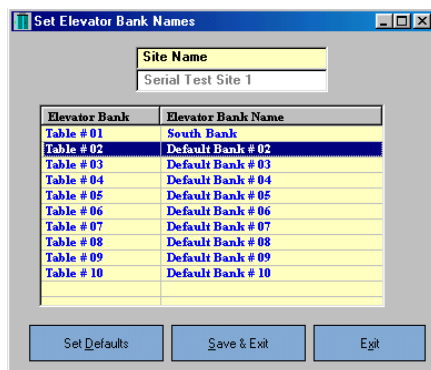
The Set Elevator Bank Names option allows you to assign a name to a specific bank of elevators. Because elevators have access to identical floor numbers or may be in the same tower, creating bank names differentiates one group of elevators from another.

To Set Elevator Bank Names

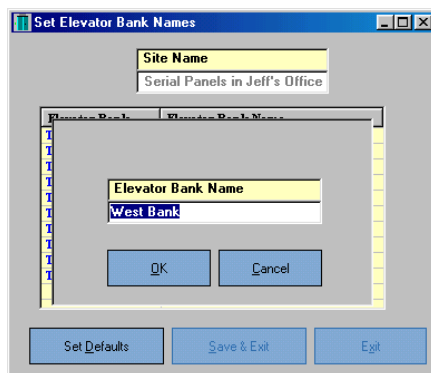
From the Keyscan System V Client's main screen, select Elevator Controllers > Set Elevator Bank Names.



1. Double click on an open elevator bank name from the Set Elevator Bank Names form.



2. Click the cursor inside the Elevator Bank Name text box and type the name of the elevator group. The maximum number of elevator banks is 10.



3. Click on the OK button.

4. Repeat the preceding steps to add another elevator bank name, or click on the Save & Exit button to return to the main screen.

Set Elevator Bank Names form

Elevator Bank	Elevator Bank Name
Table # 01	South Bank
Table # 02	West Bank
Table # 03	Default Bank # 03
Table # 04	Default Bank # 04
Table # 05	Default Bank # 05
Table # 06	Default Bank # 06
Table # 07	Default Bank # 07
Table # 08	Default Bank # 08
Table # 09	Default Bank # 09
Table # 10	Default Bank # 10

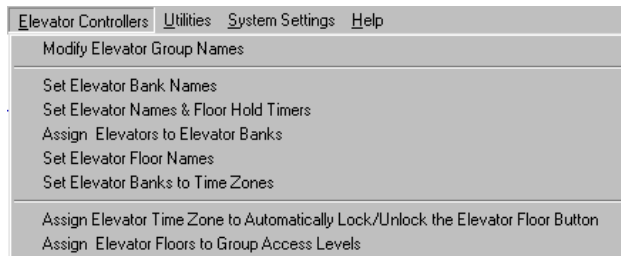
Set Defaults Save & Exit Exit

Set Elevator Names and Floor Hold Times

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

To Set Elevator Names and Floor Hold Times

From the Keyscan System V Client's main screen, select Elevator Controllers > Set Elevator Names and Floor Hold Times.



1. Click on the down arrow on the right side of the Unit ID field and select the elevator control unit for the elevator from the drop down list.
2. Click in the Elevator Name # text box and enter a name for the elevator.
3. Click in the Floor Button Selection Time's left text box and enter a value. This value is automatically multiplied by 5 seconds to set the floor button hold time.
4. Click on the Save & Exit button. (In the right box under Floor Button Selection Time, the form lists the number of seconds the floor buttons are active based on the value entered in step 3 multiplied by 5 seconds.)

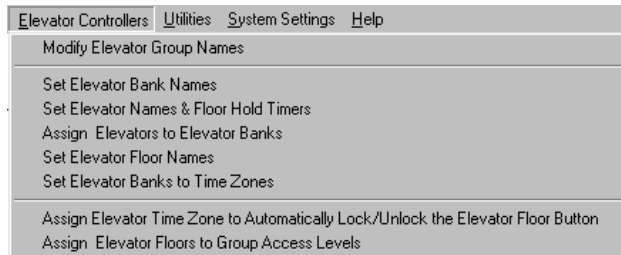
Set Elevator Names form

Assign Elevators to Elevator Banks

After you have completed naming the elevator banks and naming the elevators, you assign elevators to elevator banks.

To Assign Elevators to Elevator Banks

From the Keyscan System V Client's main screen, select Elevator Controllers > Assign Elevators to Elevator Banks.



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

Assign Elevators to Elevator Banks form

Elevator Name	Elevator Bank
#1 Car W1	West Bank
#2	
#3	
#4	
#5	
#6	
#7	
#8	
#9	
#10	

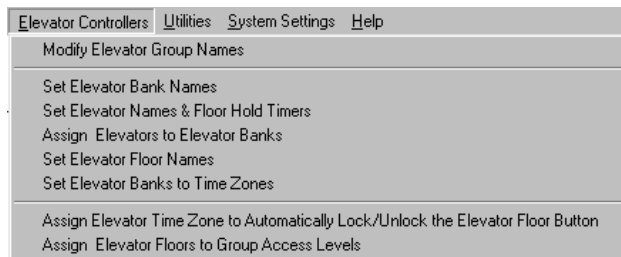
Save & Exit Exit

Set Elevator Floor Names

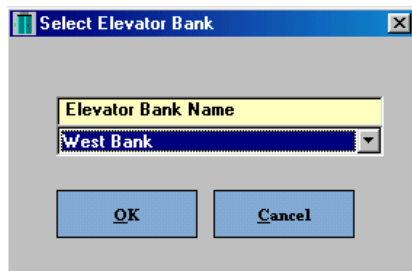
The Set Elevator Floor Names form is used to name elevator floors.

To Set Elevator Floor Names

From the Keyscan System V Client's main screen, select Elevator Controllers > Set Elevator Floor Names.



1. Click the down arrow at the right under the Elevator Bank Name and select the elevator bank from the drop down list.



2. Click on the OK button.
3. Double click on an open floor # from the Floor Name list in the lower part of the Set Elevator Floor Names form.
4. Click in the Floor Name text box and enter a name for the floor.
5. Click on the Update button. The floor name is added to the list.
6. Repeat the above steps until you are finished naming floors.
7. Click on the Exit button to return to the main screen.

Set Elevator Floor Names form

Site Name: Serial Panels in Jeff's Office

Elevator Bank Name: West Bank

Relay #: 06

Floor Name: Floor # 06

Update

Total Floors: 16

Relay #	Floor Name
01	Main/Lobby
02	Finance
03	Software Eng
04	Laboratory
05	Exec Suites
06	Floor # 06
07	Floor # 07
08	Floor # 08
09	Floor # 09
10	Floor # 10
11	Floor # 11
12	Floor # 12
13	Floor # 13
14	Floor # 14

Exit

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. 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 combined total of time zones and schedules is 512.
- Maximum range of a time zone is from 00:01 to 23:59.

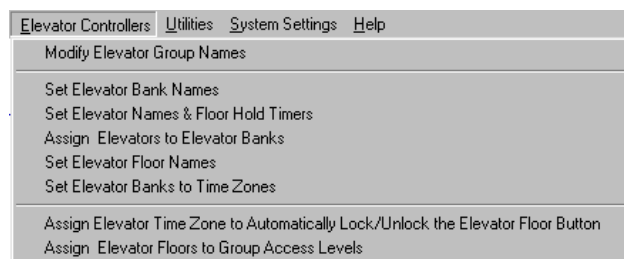
The default setting of 00:00 in the Keyscan software represents No Time. It does not represent midnight. If either the start time or the end time is assigned 00:00 the following conditions result:

- If the start time is set to 00:00 – No Access. The time zone is not enabled.
- If the end time is set to 00:00 – 24 Hour Access. The time zone is not disabled.

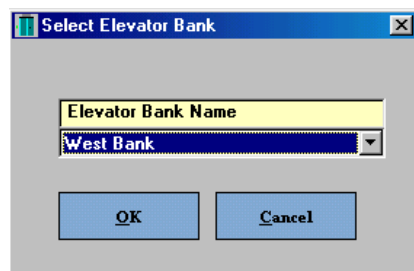
Setting elevator time zones does not regulate door time zones. Door time zones are set from Quick Buttons > Time Zone / Schedules > Door Time Zones.

To Set Elevator Banks to Time Zones

From the Keyscan System V Client's main screen, select Elevator Controllers > Set Elevator Banks to Time Zones.



1. From the Select Elevator Bank form, click on the down arrow at the right under the Elevator Bank Name field and select the elevator bank from the drop down list.



2. Click on the OK button.
3. From the Set Elevator Banks to Time Zones form, click on the Add New Time Zone button. The program assigns an Elevator Time Zone #.

4. Enter a descriptive title in the Elevator Time Zone Description text box to identify the time zone.
5. 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.
6. 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.
7. Select the hour in the lower box under Mon and click the up or down arrow at the right to set the end hour.
8. Select the minutes and click the up or down arrow to set the end minutes.
9. Repeat steps 5 to 8 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.
10. Click on the Save Schedule button.
11. Click on the Add New Time Zone button and repeat steps 3 to 10 to add another time zone, or click on the Exit button to return to the main screen.

Set Elevator Banks to Time Zones form

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.

To Add a New Schedule

1. Click on the down arrow of the Elevator Time Zone # and select the time zone from the drop down list. Be sure the Elevator Time Zone # is highlighted in blue.

2. Click on the Add New Schedule button.
3. 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.
4. 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.
5. Select the hour in the lower box under Mon and click the up or down arrow at the right to set the end hour.
6. Select the minutes and click the up or down arrow to set the end minutes.
7. Repeat steps 3 to 6 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.
8. Click on the Save Schedule button.
9. Click on the Add New Schedule button and repeat steps 2 to 8 to add another schedule, or click on the Exit button to return to the main screen.

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:

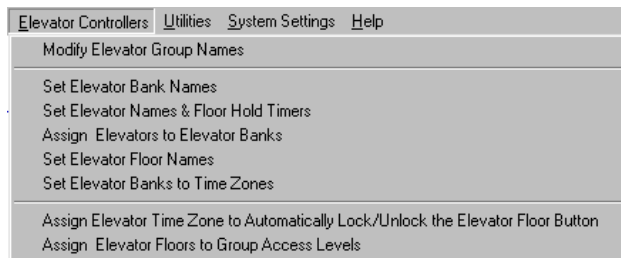
- No Access Without Valid Card – If this option is selected, the elevator floor button is locked out until a valid card is presented to the reader. The floor is not accessible to persons without a valid card. This is the default setting, represented by N/A.
- Time Zone Limited Access – If this option 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 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 the default setting N/A - No Access Without Valid Card.

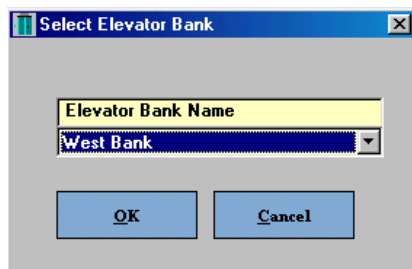
If access to all floors is restricted to valid cardholders, you can bypass this step.

To Assign Elevator Time Zones to Automatically Lock/Unlock Floor Buttons

From the Keyscan System V Client's main screen, select Elevator Controllers > Assign Elevator Time Zone to Automatically Lock/Unlock Elevator Floor Buttons.



1. Click on the down arrow at the right under the Elevator Bank name field in the Select Elevator Bank dialog box and select the elevator bank from the drop down list.



2. Click on the OK button.
3. From the yellow table on the left side of the Assign Elevator Time Zone to Automatically Lock/Unlock Elevator Floor Buttons form, select the floor.

4. 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.
5. 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.
6. Click on the OK button.
7. Repeat the above steps for each floor.
8. Click on the Save & Exit button to return to the main screen.

Assign Elevator Time Zone to Automatically Lock/Unlock form

The screenshot shows a software window titled "Assign Elevator Time Zone to Automatically Lock/Unlock the Elevator Floor Button". It contains the following elements:

- Site Name:** SERAILJT
- Unit ID:** EC2000
- Floor List Table:**

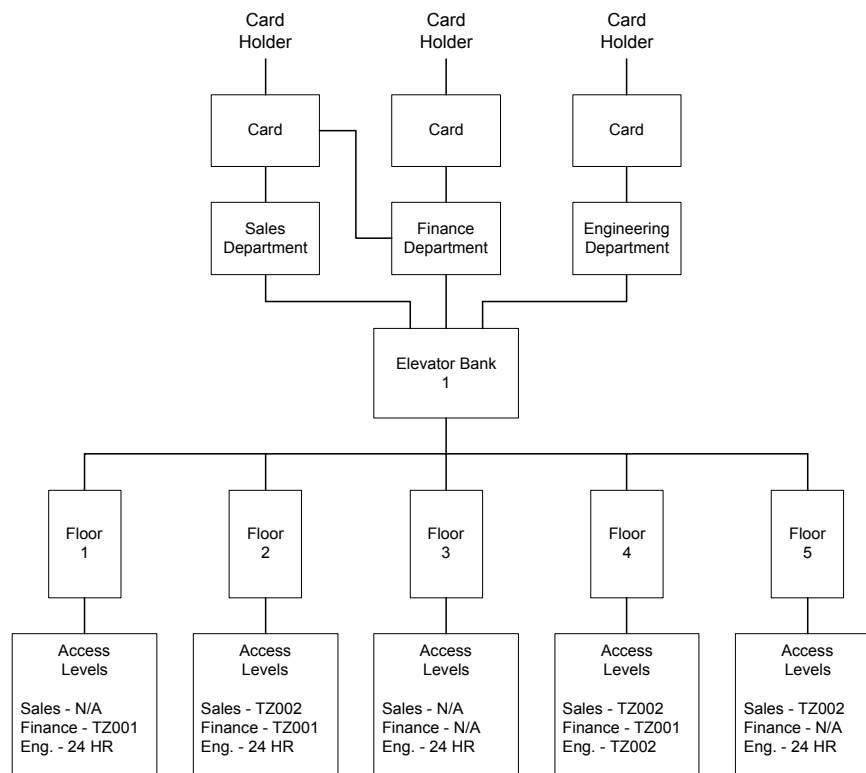
Floor #	Floor Name	Time Zone Assignment
Floor # 01	Main Lobby	TZ-1
Floor # 02	Reception	N/A
Floor # 03	Software Eng.	N/A
Floor # 04	Laboratory	N/A
Floor # 05	Exec Suites	TZ-1
Floor # 06	Cafeteria	TZ-1
Floor # 07	Floor # 07	N/A
Floor # 08	Floor # 08	N/A
Floor # 09	Floor # 09	N/A
Floor # 10	Floor # 10	N/A
Floor # 11	Floor # 11	N/A
Floor # 12	Floor # 12	N/A
Floor # 13	Floor # 13	N/A
Floor # 14	Floor # 14	N/A
Floor # 15	Floor # 15	N/A
Floor # 16	Floor # 16	N/A
- Access Options:**
 - ☐ No Access Without Valid Card
 - ☒ Time Zone Limited Access
- Time Zone Selection:** TZ-1 Public Hours (with OK, Cancel, and Edit Time Zones buttons)
- Public Hours Schedule:**
 - Mon:** 09:00 to 18:00
 - Tues:** 09:00 to 18:00
 - Wed:** 09:00 to 18:00
 - Thur:** 09:00 to 18:00
 - Fri:** 09:00 to 18:00
 - Sat:** 00:00 to 00:00
 - Sun:** 00:00 to 00:00
 - Holiday 1:** 00:00 to 00:00
 - Holiday 2:** 00:00 to 00:00
 - Holiday 3:** 00:00 to 00:00
- Navigation:** Previous, Next, Save & Exit, Exit buttons.

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 following diagram illustrates an example site where there are 3 different elevator groups: Sales Department, Finance Department, and Engineering Department. An ECU controls an elevator bank in a building with 5 floors. Elevator group access levels are summarized below the floor numbers. You will note that elevator groups have either: 24 hour access, no access, or limited access based on a time zone.

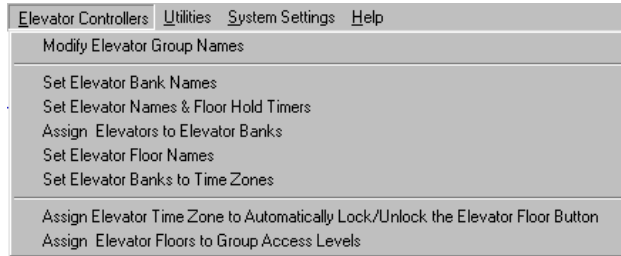


The Assign Elevator Floors to Group Access Levels form is laid out in a table format. The elevator group names are listed in a column on the far left, the floor numbers are listed in a row along the top, and the access levels set in a grid format in the body of the table.

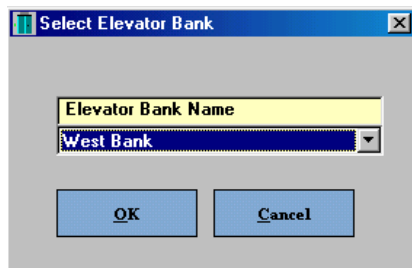
Elevator Group Name	1	2	3	4	5
001 - Sales Dept	N/A	TZ-002	N/A	TZ-002	TZ-002
002 - Finance Dept	TZ-001	TZ-001	N/A	TZ-001	N/A
003 - Engineering Dept	24 HR	24 HR	24 HR	TZ-002	24 HR

To Assign Elevator Floors to Group Access Levels

From the Keyscan System V Client's main screen, select Elevator Controllers > Assign Elevator Floors to Group Access Levels.



1. From the Select Elevator Bank form, click on the down arrow to the right of Elevator Bank Name and select the elevator bank from the drop down list.



2. Click on the OK button.
3. Double click on the grid location in the body of the table for the elevator group/floor # that is to be assigned an access level. Access levels can be assigned by 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 the same access level to all elevator groups for one floor, click on the floor number listed in the blue row at the top of the table.

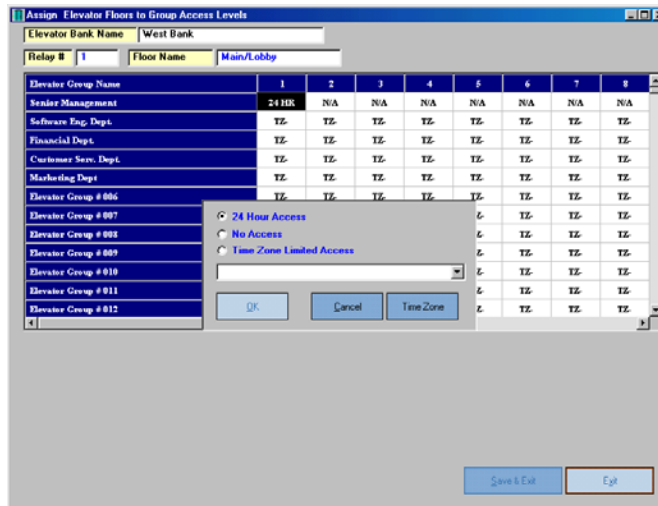


- To assign the same access level to multiple elevator groups for multiple floors, click on the upper left grid location and hold and drag the mouse to the lower right grid location.



- 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 6.)
 - No Access (If No Access was selected, go step 6.)
 - Time Zone Limited Access (If Time Zone Limited Access was selected, go step 5.)
- 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.
- Select the OK button.
- Repeat the above steps until all elevator groups have been assigned an access level for each floor.
- Select the Save & Exit button.

Assign Elevator Floors to Group Access Levels form



Setup Holiday Time Zones

Setting the system for various types of holidays involves two procedures: The first procedure is to set the hours of the holiday time zone. The second procedure is to assign the holiday time zone to a calendar date.

Holiday Time Zone

A holiday time zone resides within a door or elevator time zone. You may have up to three holiday time zones: Holiday 1, Holiday 2, and Holiday 3 within a door or elevator time zone.

As an example, on certain statutory holidays you wish to limit access to the building from 12:00 noon to 3:00 P.M., while on other statutory holidays there is no access to the building. The two holiday time zones would be set as listed below.

- Holiday 1: 12:00 to 15:00 (12:00 Noon to 3:00 P.M.)
- Holiday 2: 00:00 to 00:00 (default setting)

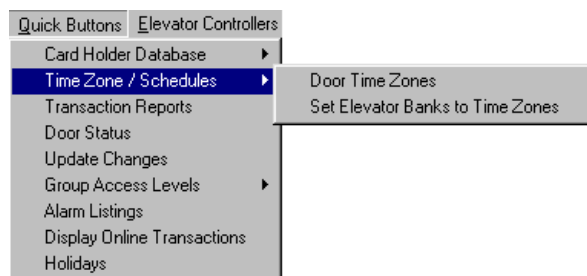
On occasions where there is to be no access during a Holiday Time Zone that coincides with a Door Time Zone overlapping midnight, you must specify an end time for the Holiday Time Zone. As an example, if a shift ended at 1 a.m. and you did not want anyone to access the building after the conclusion of the shift, the holiday time zone would be set as follows:

- Holiday: 00:00 to 01:00 (1 a.m. to start of next valid door time zone)

To Setup Holiday Time Zones

From the Keyscan System V Client's main screen, select Quick Buttons > Time Zone/Schedules

- If you are setting holiday time zones for doors, select Door Time Zones
- If you are setting holiday time zones for elevators, select Set Elevator Banks to Time Zones



1. Click on the down arrow on the right side of the Time Zone # field and select the time zone from the drop down list to which the holiday hours will be applied.
2. Select the hour in the upper box, in either Holiday 1, 2, or 3 and click the up or down arrow at the right to set the start hour.
3. Select the minutes and click the up or down arrow to set the start minutes. You should still be in the upper box.
4. Select the hour in the lower box and click the up or down arrow at the right to set the end hour.

5. Select the minutes and click the up or down arrow to set the end minutes.
6. Click on the Save Schedule button.
7. Click on the Exit button.

Time Zone form

Assign a Holiday to a Holiday Time Zone

After establishing holiday time zones, you assign the holiday time zone to a calendar date, which could be for statutory holidays, vacations, facility shutdown days, etc.

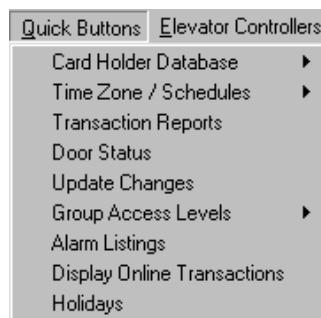
Note

You must review and revise holiday dates at least once a year. This ensures the system dates are reset to calendar dates over the next 12 months.

A holiday time zone overrides a door and elevator time zone.

To Assign a Holiday to a Holiday Time Zone

From the Keyscan System V Client's main screen, select Quick Buttons > Holidays.



1. Click on the arrows at the top of the calendar to scroll to the desired month and year.
2. Double click on the date of the holiday on the calendar to open the Holiday Detail Information dialog box.
3. Enter the name of the holiday in the Holiday Description text box.
4. 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
5. Click on the OK button.
 - To remove or undo a holiday, double click on the entry in the Holidays Added to Database table.
6. Click on the Save & Exit button.

Holidays form

The screenshot shows the 'Holidays' form with the following components:

- Site Name:** ABC Corporation
- Calendar:** May 2002. Today is 4/17/02.
- Holidays Added to Database Table:**

Date	Holiday Description	Type
01/01/2002	New Years Day	1
- Holiday Detail Information Dialog Box:**
 - Holiday Description:** Victoria Day
 - Type:** 1
 - Buttons:** OK, Cancel
- Total Number of Holidays:** 1
- Buttons:** Print Listing, Clear All, Save & Exit, Exit

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.

Note

It is strongly recommended that you review and revise daylight savings dates at least once a year. This ensures the daylight savings dates are re-programmed for the next year.

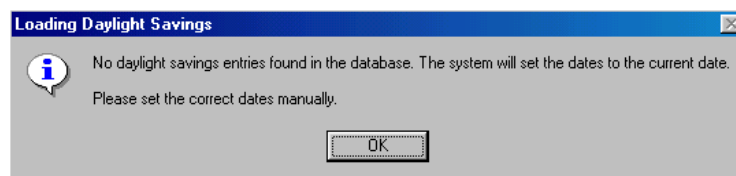
To Set Daylight Savings

From the Keyscan System V Client's main screen, select System Settings > Daylight Savings.



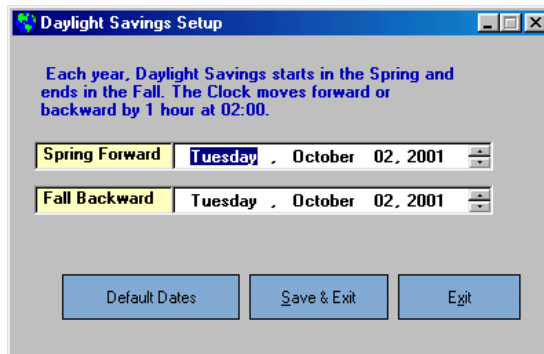
Note

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.



1. Select the Year in the Spring Forward field and click on the up or down arrows to advance to the correct year.
2. Select the Month in the Spring Forward field and click on the up or down arrows to advance to the correct month.
3. Select the Day in the Spring Forward field and click on the up or down arrows to advance to the correct day.
4. Repeat the above steps to set the date for the Fall Backward field.
5. Click on the Save & Exit button.

Daylight Savings Setup form



The image shows a Windows-style dialog box titled "Daylight Savings Setup". It contains a text area with instructions: "Each year, Daylight Savings starts in the Spring and ends in the Fall. The Clock moves forward or backward by 1 hour at 02:00." Below this are two date selection fields. The first field is labeled "Spring Forward" and shows "Tuesday, October 02, 2001". The second field is labeled "Fall Backward" and also shows "Tuesday, October 02, 2001". At the bottom are three buttons: "Default Dates", "Save & Exit", and "Exit".

Daylight Savings Setup

Each year, Daylight Savings starts in the Spring and ends in the Fall. The Clock moves forward or backward by 1 hour at 02:00.

Spring Forward Tuesday, October 02, 2001

Fall Backward Tuesday, October 02, 2001

Default Dates Save & Exit Exit

Add New Cardholders

Each person that is assigned a card to access your building or site is referred to as a card holder. Adding cards/card holders to the database requires completing three forms from the Add New Cards function found in the Quick Buttons menu:

- General Card Holder Information
- Additional Card Holder Information
- Optional Card Holder Information

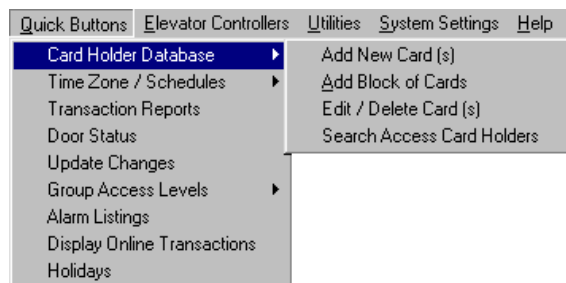
After completing all your card holder records, you can export the records as a CSV file. This is an added precaution to safeguard these records. For procedures, see Exporting Card Holder Records in CSV format on page 101. More extensive information on this topic is available in the Client software. Select the Help menu > Contents > Operating the System > Cardholders > Import/Export Cardholder Information.

General Cardholder Information

The General Card Holder Information form serves to identify the card holder and associate that person to a specific card and door/elevator group. If your system uses either an Indala or HID reader/keypad, please refer to the Note in the Assign Time Zones to Readers/Keypads topic on page 56.

To Add a New Card - General Card Holder Information

From the Keyscan System V Client's main screen, select the Quick Buttons menu > Card Holder Database > Add New Card(s). Select the General Card Holder Information tab at the top, if the form is not in view.



1. Click in the First Name text box and enter the card holders first name. The maximum is 30 characters.
2. Click in the Last Name text box and enter the card holders last name. The maximum is 30 characters.
3. Click in the Batch Number text box and enter the batch number. The batch number is the first three digits on the back of the assigned card. The batch number may also be referred to as the site code or the facility code.
4. Click in the Card Number text box and enter the card number. The card number follows the hyphen after the batch number.

5. The system assigns a 5 digit Personal Identification Number in the PIN number text box. The card holder enters this number when 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 number and proceed to the next step.
6. 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.
7. If the card is temporary, perform steps 8 to 11, otherwise leave the Temporary Card Options inactive, and proceed to step 12.
8. Click inside the Card Limited check box. A tick mark indicates the field is active.
9. If applicable, in the Card Limited to Number of Uses text box enter the maximum number of times the card can be used. If there is no restriction on the number of times the card can be used, leave the Card Limited to Number of Uses text box blank.
10. Under Date Valid From, the current date is displayed. If the start of the temporary date range is other than the current date, click on the down arrow to the right to open the calendar. At the top of the calendar, click on the arrows to scroll to the desired month and year. Select the day on the calendar.
11. Repeat the above step to complete the Date Valid To field.
12. If you're entering more than 1 card with the same batch number, you can activate Batch Mode ON by clicking in the box. This allows entering multiple card holders without having to exit after each card holder is entered in the database.
13. If the card holder is to have access to Multiple Sites, activate this field. You can complete the other card holder information forms by clicking on the tabs, then return to the General Card Holder Information form and click on the Save & Exit button to save the card holder record to the current site. You will notice the Site Name box is active. Click on the down arrow to the right of Site Name and select the name of the next site the card holder is to have access to. If you use PIN numbers, you will have to assign a new PIN number for each site, and if the Door Groups and Elevator Groups are different at various sites, you will have to specify a new Door Group Access Level and Elevator Group Access Level for the card holder.
14. If the card holder has a disability and requires a greater amount of time to gain access to a door, click the Accessibility Feature button to set it ON. When this individual's card is presented to a door, the reader acknowledges the card's disability status and invokes the Handicap Door Timer setting and Handicap Door Held Open Timer setting if your system has this optional feature. These settings are specified in the Set Door and Reader Parameters form. This is an optional feature and may not be included with your system.
15. Leave the Archived Card Holder inactive. This field is used to de-activate a card but maintain a record of the card holder in the database.
16. To insert a photo of the card holder, see Photo Capture on page 86.
17. By-pass the Last Update and Last Update By fields; they are system entries.

18. After the General Card Holder Information form is completed, you have the following choices:
- To save the card holder information in the database and return to the main screen, select Save & Exit.
 - To add another cardholder to the database, if the Batch Entry Mode On is active, select the Save button at the bottom of the form and repeat the steps to complete another form.
 - To abort the card holder information process, select Exit > No to return to the main menu.
 - To complete the Additional Card Holder Information form and/or the Optional Card Holder Information form, select the corresponding tab and complete the required information, then return to the General Card Holder Information form and select the Save & Exit button.

General Card Holder Information form

Photo Capture

You must have purchased and registered the optional Photo Badge Template Editor to capture photos and insert them in the card holder records and print photobadges. If you do not have this optional module, the Capture Photo button and the Print Photo Badge button are not present on the Card Holder General Information form. If your software includes the optional Photo Badge Template Editor, there are two methods to insert an image on the General Information form: from an existing image of the card holder or from a live video capture of the card holder. You must have a video camera connected to your PC to capture a live video image of the card holder.

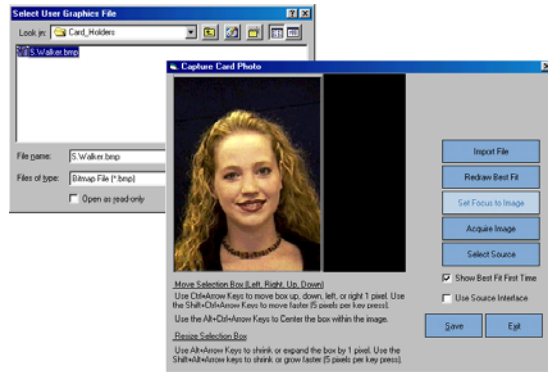
To Insert an Existing Image

1. 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 card holder.
4. Click on the Open button.
5. From the Capture Card Photo form, click on the Save button to import the file into the

General Card Holder Information form.

- Click on the Save & Exit button on the General Card Holder Information form to save the card holder's photo with his or her record.

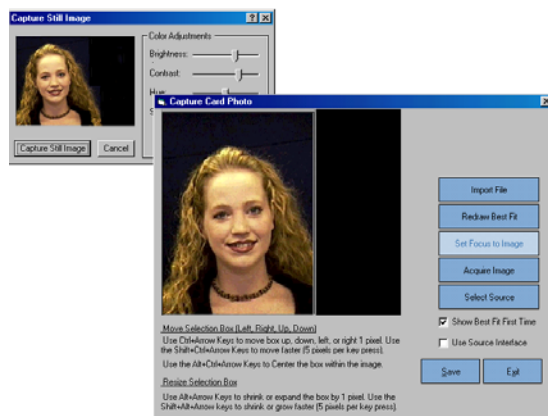
Select User Graphics File dialog box and Capture Card Photo form



To Capture a Live Video Image

- Click on the Capture Photo button.
- From the Capture Card Photo form, click on the Acquire Image button.
- With the Capture Still Image form open, position the card holder in front of the camera to obtain the desired image. Use the Color Adjustment bars to make image corrections and click on the Capture Still Image button.
- In the Capture Card Photo form, the two vertical lines in the image window represent the left and right borders when the image is inserted in the General Card Holder Information form. If the image is satisfactory, click on the Save button to import the image into the General Card Holder Information form, otherwise repeat steps 2 and 3 to acquire a satisfactory image.
- Click on the Save & Exit button on the General Card Holder Information form to save the card holder's photo with his or her file.

Capture Still Image form and Capture Card Photo form



Additional Cardholder Information

The Additional Card Holder Information form lists supplemental information about the card holder, such as telephone number, Email address etc. Completing these fields is optional.

Note

You must have purchased the Photo Badge Template Editor to use the Capture Signature feature, which is found on the Additional Cardholder Information form. A capture signature device and a USB port are also required. As this feature is optional, it may not be viewable as illustrated in the example of the Additional Cardholder information form shown in this manual.

To Complete the Additional Card Holder Information Form

Select the Additional Card Holder Information tab at the top of the Card Holder Information form.



1. Click the cursor in the appropriate text boxes and type the required information.
2. After the Additional Card Holder Information form is completed, you have the following choices:
 - To save the cardholder information in the database and return to the main screen, select Save & Exit.
 - To add another cardholder to the database, if Batch Entry Mode On is active, select the General Card Holder Information tab, select the Save button at the bottom of the form and complete another form.
 - To abort the card holder information process, select Exit > No to return to the main menu.
 - To complete the Optional Card Holder Information form, select the corresponding tab title and complete the required information.

Additional Card Holder Information form

To Capture a Signature

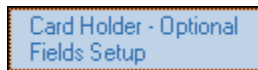
1. Click on the Capture Signature button.
2. With the signature capture device's pen, have the signatory sign his or her name on the glass face of the signature capture device. The signature is transferred to the Card Holder Signature box on the Additional Cardholder Information form.
3. If the signature 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 form.

Optional Cardholder Information

The Optional Card Holder Information form lists supplemental information about card holders not covered by the other two Card Holder Information forms. The fields in the Optional Card Holder Information form are initially blank until you define them.

To Define Fields in the Optional Card Holder Information Form

Select the Additional Card Holder Information tab at the top of the Card Holder form. Click on the Card Holder – Optional Fields Setup button from the Optional Card Holder Information form.



1. Click in the Optional Field Name # 1 text box on the right side of the Card Holder Optional Fields form and type a caption.
2. Repeat for each subsequent field that you wish to define.
3. Click on the Save & Exit button to save the entries and return to the Optional Card Holder Information form.

Card Holder – Optional Fields form

Optional Field Name	Value
Optional Field Name #1	Membership Type
Optional Field Name #2	Emergency Contact
Optional Field Name #3	
Optional Field Name #4	
Optional Field Name #5	
Optional Field Name #6	
Optional Field Name #7	
Optional Field Name #8	
Optional Field Name #9	
Optional Field Name #10	

Last Update	
Last Update By	

To Complete the Optional Card Holder Information Form

1. Click the cursor in the appropriate text boxes and type the required information.
2. After the Additional Card Holder Information form is completed, you have the following choices:
 - To save the cardholder information in the database and return to the main screen, select Save & Exit.
 - To add another cardholder to the database, if the Batch Entry Mode On is active, select the General Card Holder Information tab, select the Save button at the bottom of the form and complete another form.
 - To abort the card holder information process, select Exit > No to return to the main menu.
 - To return to the General Card Holder Information form, select the corresponding tab title.

Optional Card Holder Information form

The screenshot shows a software window titled "Card Holder" with three tabs: "General Card Holder Information", "Additional Card Holder Information", and "Optional Card Holder Information". The "Optional Card Holder Information" tab is active, displaying a form with the following fields:

- Membership Type
- Emergency Contact
- Seven additional empty text input fields.

Below the input fields is a button labeled "Card Holder - Optional Fields Setup". At the bottom of the window is a toolbar with the following buttons: "Print Card Holder Information", "Print Photo Badge", "Capture Photo", "Previous", "Next", "Save & Exit", and "Exit". The status bar at the very bottom displays "System Status", "Keyscan Default", "10/1/01", and "9:23 AM".

Setup System Administrators/Users

Each individual who will administrate the system must be given a user account, which is created in the System User Information form. This prevents unauthorized persons from accessing the Keyscan software and regulates individual user rights to protect the integrity of your access control system.

From within the form, you identify the individual, assign a unique User Name and Password for logging on, set the program interface language – English, French, or Spanish, and specify user authority levels.

With respect to assigning user authority levels for each individual, 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. It is important to understand the conventions of a System User and User Authority Levels when you are creating a user account.

System Users

Each individual who has an account to access the Keyscan software is considered a System User. There are, however, three system user designations. The following highlights the functional differences between those three designations.

<u>System User with</u> Master Login Account	<u>System User with</u> System Administrator	<u>System User</u>
Create new sites Delete sites Add users to any site	Display/Clear/Delete system log events Display/Search/Print PIN card numbers Reset User Passwords Add a system administrator to the current site Import Cards (CSV files)	Excluded from the Master Login Account and System Administrator rights

Additional Notes on System Users

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 for all sites 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.

- 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.

User Authority Levels – Master Login Account

If an individual has a Master Login Account designation, the illustration below shows the User Authority Levels fields that have to be selected, in addition to any other desired system functions.

Master Login Account	User Authority Levels												
Functions	Selected Fields												
Create new sites	<table><tr><th>Available</th><th>Authority Description</th></tr><tr><td><input checked="" type="checkbox"/></td><td>System Users</td></tr><tr><td><input checked="" type="checkbox"/></td><td>Add Site</td></tr><tr><td><input checked="" type="checkbox"/></td><td>View Site</td></tr><tr><td><input checked="" type="checkbox"/></td><td>Edit Site</td></tr><tr><td><input checked="" type="checkbox"/></td><td>Delete Site</td></tr></table>	Available	Authority Description	<input checked="" type="checkbox"/>	System Users	<input checked="" type="checkbox"/>	Add Site	<input checked="" type="checkbox"/>	View Site	<input checked="" type="checkbox"/>	Edit Site	<input checked="" type="checkbox"/>	Delete Site
Available		Authority Description											
<input checked="" type="checkbox"/>		System Users											
<input checked="" type="checkbox"/>		Add Site											
<input checked="" type="checkbox"/>		View Site											
<input checked="" type="checkbox"/>	Edit Site												
<input checked="" type="checkbox"/>	Delete Site												
Delete sites													
Add users to any site													

User Authority Levels – System Administrator

Similarly, for a system user with a System Administrator designation, you must select the corresponding functions in the User Authority Levels panel, plus any other desired functions.

System Administrator	User Authority Levels
Functions	Selected Fields
Display/Clear/Delete system log events	View System Log Entries
Display/Search/Print PIN card numbers	View Cards – General Card Holder Information
Reset system user password	System Users
Add a system administrator to the current site	Perform Printing Tasks
Import Cards (CSV files)	

User Authority Levels – System User

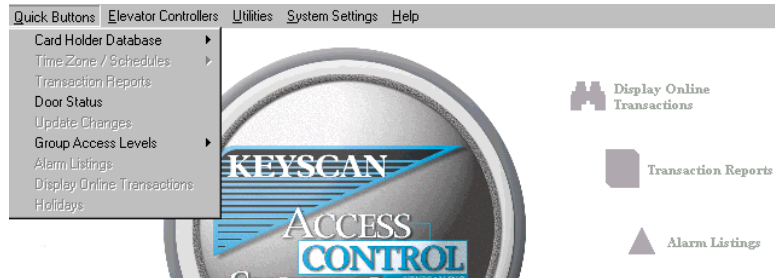
For Individuals deemed solely as System Users, leave the Master Login Account and System Administrator options inactive. As an example, if a system user is only permitted to view, add, or modify card holder information on one site, all the fields in the User Authority Levels panel would be left inactive, with the exception of the following:

- Add Cards
- View Cards – General Card Holder Information
- View Cards – Additional Card Holder Information
- View Cards – Optional Card Holder Information

- Edit Cards
- Delete Cards

When the system user logs on to the system, only the designated functions are accessible; the remaining functions are locked out as indicated by the dimmed menus and the grayed quick buttons.

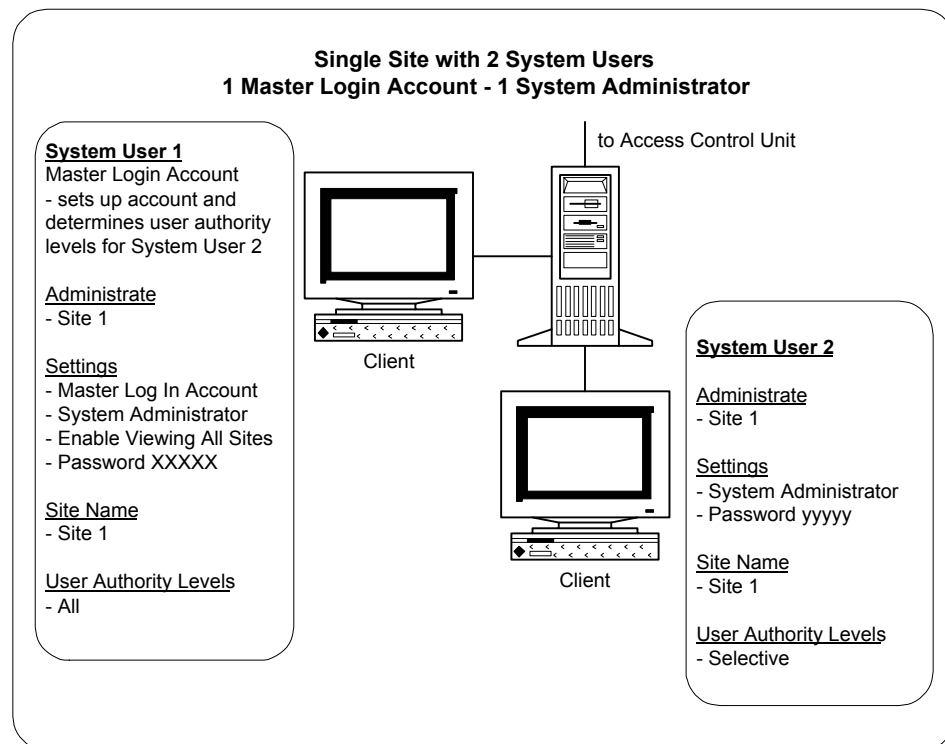
Example of menu with locked out functions and disabled quick buttons



Single Site – System User 1 Master Login Account with access to all functions

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.

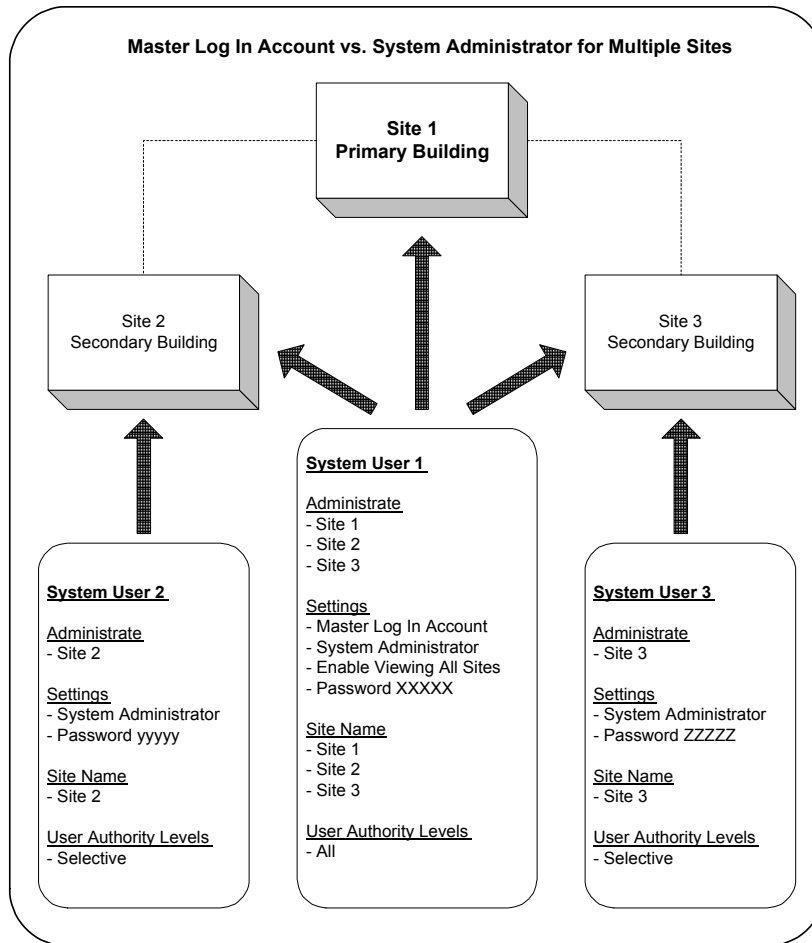
System User 2, in this example, is a Human Resources administrator and has to add, edit, or delete card holder records, review log events and have the option to add another system user. In this case System User 1 would activate the System Administrator option and set the corresponding User Authority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



Multiple Sites – User 1 Master Login Account with access to all sites

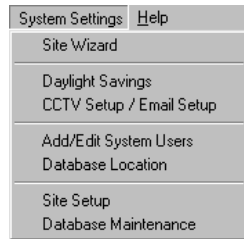
In this example of a three-site setup, System User 1, who is located at Site 1, is responsible for operating and maintaining the entire access control system at all three sites. This person would have System Administrator and Master Login Account designations. To have access to all sites, System User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



To Setup System Users

From the Keyscan System V Client's main screen, select System Settings > Add/Edit System Users.



1. From the Find System Users dialog box, click on the Add New button to open the System Users Information form.
 - To add a new system user to another site you must have a Master Login Account designation.
 - To add a new system user to the logged on site, you must have a System Administrator or Master Login Account designation.
2. 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.
3. Enter the person's first name in the First Name text box.
4. Complete the remaining text boxes from Last Name to Email Address, whichever are applicable.
5. 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 this form.
 - Password Expires On is a system setting. The software prompts the system user every 60 days to renew his or her password.
 - When the system user logs on for the first time he or she will be prompted to confirm the new password. The password is typed in both the Password and Confirm Password text boxes.
6. Click the down arrow on the right side of Language. From the drop down list, select an interface language for that individual as listed below:
 - English
 - Français
 - Español
7. Click the down arrow on the right side of Site Name. Select the appropriate site for the system user from the drop down list.
8. If the person is to have access to the Master Login Account, click in the box to the left to activate this field.

9. If the system user is to have a System Administrator designation, click in the box to activate this field. The box has a tick mark when active.
 - For individuals deemed as System Users, leave the System Administrator and Master Login Account designations inactive.
10. 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.
11. Under the User Authority Levels, activate the appropriate fields for the system user by clicking inside the field's box. If the system user is to have access to all fields, click on the Select All Levels button at the bottom of the form.
 - 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 Keyscan Client and Communications Manager cannot be closed. Please remember that if the Communications Manager and Database Module are closed the system will not operate.
12. Select the Save & Exit button after completing the System User Information form.

System User Information form

System User Information

User Name:

First Name:

Last Name:

User Location:

Telephone Number:

Telephone Extension:

Fax Number:

Email Address:

Password:

Password Expires On:

Language: Site Name:

☐ System Administrator ☐ Archived User

☐ Master Login Account

☐ Enable Viewing of All Sites Transactions

Last Update:

Last Update By:

User Authority Levels

Available	Authority Description
<input checked="" type="checkbox"/>	Add Cards
<input checked="" type="checkbox"/>	View Cards - General Card Holder Information
<input checked="" type="checkbox"/>	View Cards - Additional Card Holder Information
<input checked="" type="checkbox"/>	View Cards - Optional Card Holder Information
<input checked="" type="checkbox"/>	Edit Cards
<input checked="" type="checkbox"/>	Delete Cards
<input checked="" type="checkbox"/>	Change Optional Card Fields
<input checked="" type="checkbox"/>	Time Zone Control - View
<input checked="" type="checkbox"/>	Time Zone Control - Modify
<input checked="" type="checkbox"/>	Run Saved Reports
<input checked="" type="checkbox"/>	Run/Modify Reports
<input checked="" type="checkbox"/>	Door Status - View
<input checked="" type="checkbox"/>	Door Status - Modify
<input checked="" type="checkbox"/>	Elevator Status - View
<input checked="" type="checkbox"/>	Elevator Status - Modify
<input checked="" type="checkbox"/>	Update Database
<input checked="" type="checkbox"/>	System Users
<input checked="" type="checkbox"/>	Add Site
<input checked="" type="checkbox"/>	View Site
<input checked="" type="checkbox"/>	Edit Site
<input checked="" type="checkbox"/>	Delete Site
<input checked="" type="checkbox"/>	Database Maintenance
<input checked="" type="checkbox"/>	Alarms Listings
<input checked="" type="checkbox"/>	Enter Online Transaction Mode

Backup Database

It is extremely important to make backup copies of your database. You can program the software to make backup copies of the database at regularly scheduled intervals. It is not necessary that the Keyscan Client application be open when the scheduled backup occurs. This procedure only backs up Keyscan data; it does not backup cardholder photos, site maps, signature images, or alarm event images. You must back up these files separately.

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 to safeguard your site data.

Note

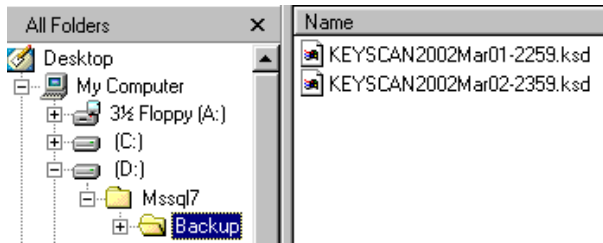
Before you can back up your database, you must have a folder where you will store the backup database file. For your convenience, we have created a backup folder in the Database module located in the following directory: Drive (\\):\\Mssql7\\Backup. If you create a folder in another directory, it must be in a valid folder on the PC where the database engine was installed.

On a Multiple PC setup where the Database Module and the Keyscan Client(s) were installed on separate PCs, it is important to understand the following convention: the database is backed up on the PC or server where the Database module was installed. It is not backed up on the Client PC. Therefore, when you specify the backup folder location from the Client, it must be the drive\\folder location on the PC with the Database module. If you have more than one Client, you only have to setup the automatic backup procedure once from any Client.

To Automatically Backup the Database at Specified Intervals

1. If you elect to use the default backup folder – Drive (\\):\\Mssql7\\Backup, go to step 2, otherwise create a backup folder on the PC with the Database module. Example - D:\\Folder Name. You may wish to write the drive and folder name on a piece of paper.
2. From the Keyscan Client's main screen, select System Settings > Database Maintenance > Yes (to close the Database Maintenance Warning box, if it opens.)
3. Click on the Database Backup button in the Database Setup form and perform either step 4 or 5 depending on your configuration.
4. If the **Database module and the Client are on different PCs**, from the Full Database backup form, in the Backup File Location textbox, type the drive and folder name, and create a name for the backup file with the extension *.ksd*. We suggest naming your backup file KEYSCAN. Example – D:\\Folder Name\\KEYSCAN.ksd.
5. If the **Database module and Client are on the same PC**, click on the Browse button on the Full Database Backup form and from the Save As dialog box, navigate to the backup folder. Specify a name for the backup file; we suggest KEYSCAN. Click on the Save button.
6. Under Backup Schedule, in the Backup Time box, select the 00 representing hours. Use the up and down arrows to advance the time to the designated hour. Then select the 00 representing the minutes. Use the up and down arrows to advance the time to the designated minutes.

7. In the Select the Day(s) of the Week, select the days when the database is backed up. Each successive time the database is backed up the Keyscan software creates a new backup file with a date suffix following the name.



8. Click on the Save Schedule button.
9. Click on the Exit button to return to the main screen.

Full Database Backup form

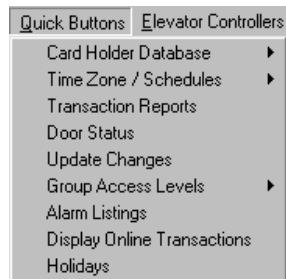
A screenshot of the 'Full Database Backup' dialog box. The title bar says 'Full Database Backup'. The main area has a 'Backup File Location:' label followed by a text box containing 'E:\Mssql7\BACKUP\abc_corp.bak.ksd' and a 'Browse' button. Below this is a red text warning: 'It is extremely important to make backup copies of your database. You can program the software to make backup copies of the database at regularly scheduled intervals. The system will backup the contents of the database, but DOES NOT backup your Cardholder Photos, Badging Templates or Maps. You must separately backup these files/folders using your choice of system backup software. We strongly recommend that you copy your backup database files to another medium such as a writable CD to safeguard your site data.' Below the warning is a 'Backup Schedule' section with a 'Backup Time:' label and a time picker set to '00:00'. Underneath is the text 'Select the day(s) of the week below:' followed by seven checkboxes for 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday', 'Saturday', and 'Sunday'. At the bottom are three buttons: 'Save Schedule', 'Backup Now', and 'Exit'. A status bar at the very bottom says 'Last Backup: 3/12/02'.

Uploading the Access Control Panels

After you have completed entering the site information, card holders, door groups, elevator groups, time zones/schedules, group access levels, door and reader parameters, auxiliary and supervised inputs, the final step is to upload the data to the access control units.

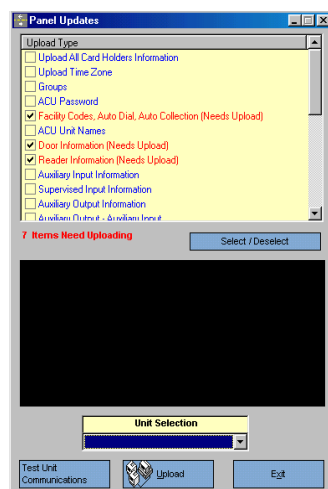
To Upload the Access Control Units

From the Keyscan System V Client's main screen, select the Quick Buttons menu > Update Changes.



1. 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.
2. From the Upload Type window, select the appropriate items to be updated. 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.
3. Select the Upload button. Wait for the message in the black box indicating the access control panels have been updated.
4. Select the Exit button.

Panel Updates form



Part 4: Preserving Site Data

Depending on how large your site is, you may have invested considerable time entering all the site information to get your access control system up and running. In light of this, there are steps we advise you take to safeguard the information in you site database.

Database Backup

If you have not yet done so, **we strongly urge that you follow the procedures reviewed under Backup Database** on page 97. If you employ the Database Backup at regular intervals and you periodically make a copy of your backed up database to another medium or network location, the following procedures are strictly added precautions to preserve your site data. Database files are electronic, however, and they can be corrupted or impregnated with a virus. Printing a Site Setup Report and Exporting Card Holder Records in CSV format only takes a few minutes. Chances are you'll never need them, but they could save you a great deal of time if you lose your database.

Site Setup Report

Printing a Site Setup Report helps safeguard your site information. Be sure to update the report whenever you make changes to the database.

Note

When you print a site setup report, only the site data for the site you are currently logged on is printed. Repeat the print procedures for each site.

Steps to Print a Site Setup Report

From the Keyscan System V Client's main screen, select System Settings > Site Setup.



1. From the Site Information Search form, double click on the site name in the yellow table in the Site Search Information form.
2. From the Site Information form, click on the Print Site Setup button.
3. From the Keyscan Print Previewer, click on the print button, which is an icon of a printer on the right side of the Previewer's tool bar.

4. From the Print dialog box, select the appropriate printer settings.
5. Click on the OK button.

Keyscan Report Previewer

The screenshot shows a window titled "Keyscan Report Previewer" with a "Site Setup Report" for the date 11/27/02. The report contains the following information:

Site ID: 555MAIN
 Site Name: ABC Corporation
 Site Location: Toronto
 Site Address: 555 Main Street
 Toronto, Ontario M1F 2N5
 Canada
 Site Telephone: (416) 366-0099
 Site Fax: No
 Site Default: No
 Site Contact: Edward Smith
 Notify Contact: (416) 366-0099

Number of Units: 3

#	Unit Type	Unit ID	Serial Number	Password
01	CA-4000	ACU1	R1234	KEYSCAN
05	CA-200	ACU2	R1235	KEYSCAN
06	EC-1000	ECU1	R2334	KEYSCAN

Facility Code:
 System Users:
 User Name: User Language: User Status:

At the bottom of the window, there are buttons for "Export to PDF" and "Exit".

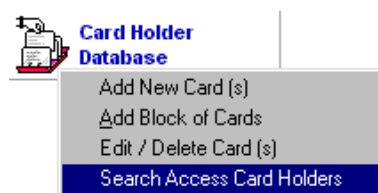
Exporting Card Holder Records in CSV format

Exporting card holder records in CSV file format offers an additional form of backing up this segment of your site data. Generally, entering card holder records requires the most time in setting up a site. For large sites with hundreds or thousands of card holders, re-entering the records, should the information be lost, can involve a substantial time investment. Having a CSV file gives added protection of safeguarding site information and allows you to import your card holder records in a matter of minutes. For more information on Importing and Exporting card holder records, select the Client software Help menu > Contents > Operating the System > Cardholders > Import/Export Card Holder Information. The following steps outline the procedures to export card holder records in CSV format. Periodically, you should update your CSV file as your card holder records change.

Note

When you export card holder records, only the card holder records for the site you are currently logged on are exported. If you have more than one site, you must repeat the export procedures for each site.

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



1. From the Search Access Card Holder form, click on the Find All Cards button to list all

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 > Export Card Holder Information.
3. 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. Your selections should reflect the fields used in the Card Holder Information forms when you entered your card holder records. You can also use the Select All button to automatically select all data fields. You cannot deselect the General Card Holder Information fields. They must be included in the data export.
4. Click on the Export Card Holder Information button.
5. From the Export File dialog box, locate a directory by clicking on the down arrow to the right of the Save In box.
6. Enter a file name in the File Name text box.
7. Click on the Save button.
8. From the Card Holders Export Completed box, click on the OK button.
9. Click on the Exit button to return to the Search Access Card Holders form.
10. Click on the Exit button to return to the main screen.

Export Card Holder Information form

Import and Export Card Holder Information

General Card Holder Information

- ☒ Card Number (Required)
- ☒ Batch (Required)
- ☒ First Name (Required for Import)
- ☒ Last Name (Required for Import)
- ☒ Door Group Access Levels A (Required for Import)
- ☐ Door Group Access Levels B
- ☒ Elevator Group Access Levels A (Required for Import)
- ☐ Elevator Group Access Levels B
- ☐ Archived Card Holder
- ☐ Card Limited
- ☐ Date Valid From:
- ☐ Date Valid To:
- ☐ Photo Location
- ☐ Photo Name

Additional Card Holder Information

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

Optional Card Holder Information

- ☐ Optional Field Name # 1 - Address
- ☐ Optional Field Name # 2 - City
- ☐ Optional Field Name # 3 - Province/State
- ☐ Optional Field Name # 4 - Postal/Zip Code
- ☐ Optional Field Name # 5
- ☐ Optional Field Name # 6
- ☐ Optional Field Name # 7
- ☐ Optional Field Name # 8
- ☐ Optional Field Name # 9
- ☐ Optional Field Name # 10

☐ Update Card Holder Information

Part 5: Communication Problems

This section is a guide to investigate and correct some of the common problems that cause system communication failures.

- a Keyscan software module won't open
- the Keyscan Client module reports a Communications Status Failed message
- the Keyscan Client module reports a DB Connection Lost message
- the Keyscan Client module reports Unit Marked Inactive
- the system does not acknowledge a card at a reader

Generally, the communication problems identified above may be the result of one or a combination of the following causes. The table below lists potential causes of communications problems and the procedures to identify and correct them. If the access control system is connected to a network, you may require the assistance of an IT administrator.



Potential Causes	See Procedure
The Communications Manager or the Database Maintenance module is not running.	A, B
The Keyscan Client software cannot communicate with the Database Maintenance module on a network (multiple PC installation).	C
The Communications Manager cannot communicate with the Database Maintenance module on a network (multiple PC installation).	C
The Communications Manager cannot connect with the access control units via the TCP to Serial Box (MSS-COMM) connection.	C, D, F
The Communications Manager cannot connect with the access control units via the serial connection.	E
The Communications Manager cannot connect with the access control units via the modem connection.	G
The system does not register a card presented at a door reader.	H

Note

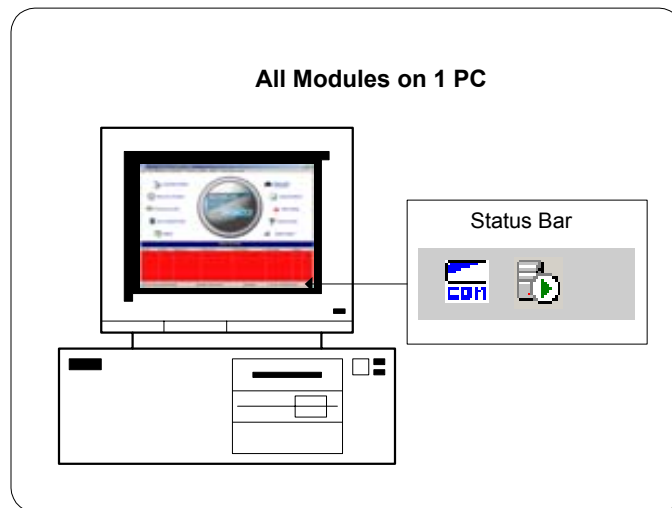
Procedures E & F involve opening the access control panels. Only qualified individuals should perform these procedures, otherwise serious damage to the equipment may result.

Procedure A – Keyscan Software Operation

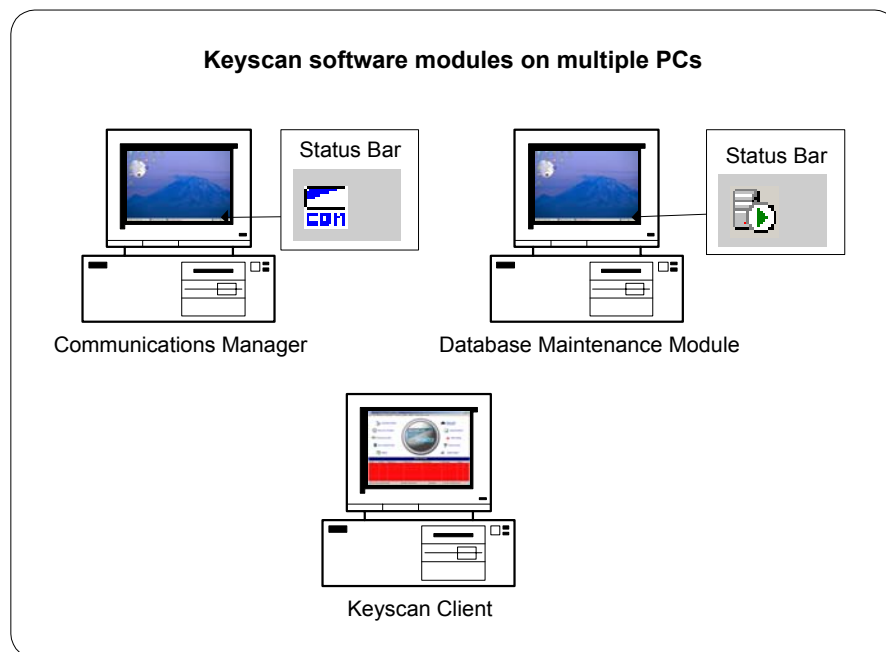
Verify the Communications Manager and Database Maintenance module are running

The Database Maintenance module  and the Communications Manager(s)  must be running on the PC(s) where they have been installed, otherwise the system will not operate. Both modules normally run in a minimized state. Their icons are in the status bar when running as illustrated in the following diagrams for single or multiple PC installations. If either module is closed, you must open it. See page 28 for start up procedures.

Single PC with all Keyscan modules



Multiple PC Installation



Procedure B – Database IP Address

Verify IP Address of Database Maintenance module

1. Get the IP address of the PC that has the Database Maintenance Module.
2. Go to the PC with the Keyscan Client or Communications Manager that is not opening.
3. Right click on Start, and select Explore.
4. Navigate to the Program Files folder > Keyscan > Keyscan Client or Communications Manager, whichever module is not opening.
5. Double click on the KeyScanVSettings.exe file.
6. Select a language button from the Language Selection box. English is the default language.
7. Click on the OK button.
8. Check the IP address specified in the Database Location text box to the actual IP address of the PC with the Database Maintenance module.
9. Enter the correct IP address.
10. Click on the Save Settings button.
11. Try re-opening the Keyscan application.

Procedure C – Network Connections

Verify Network Connections with Keyscan Client or Communications Manager

1. Get the IP address and the name assigned to the PC that has the Database Maintenance module.
2. Go to the PC that is failing to communicate with the Database Maintenance module.
3. Depending on the version of Windows, follow the appropriate instructions:
 - Windows 95, 98, or ME – Select Start > Programs > Accessories > MS-DOS Prompt > Type IPCONFIG at the command prompt
 - Windows 2000 or XP Pro – Select Start > All Programs > Accessories > Command Prompt > Type IPCONFIG at the command prompt
4. At the DOS prompt, type *ping -a* followed by the IP address of the PC with the Database Maintenance module as shown in the following example.

```
C:\WINDOWS>ping -a 123.123.123.123
```

- If the response is Request timed out, there is no connection to the PC with the Database Maintenance module or if the computer name is different, consult with the IT administrator.
- If the response is Reply from... with the correct IP address and the correct computer name of

the PC with the database, the two modules are properly connected.

Procedure D – Keyscan Software/ACU Communication

Verify ACU communication from the Keyscan Client module

1. From a PC with the Keyscan Client, log on to the appropriate site.
2. From the Client main screen, click on the Update Changes icon.
3. From the Panel Updates form, click on the down arrow to the right of Unit Selection and select the unit from the drop down list.
4. Click on the Test Unit Communications button.
 - If the result is Successfully Tested, the ACU is communicating with the Keyscan Client.
 - If the result is Invalid Password, the ACU password does not match the site information password. Check the password that was entered on the Site Unit Setup form in the Keyscan Client. If the password is set to the factory default KEYSCAN, clear the memory of the ACU and re-upload.
 - If the result is No Response, then:
 - (a) check to see if all devices are powered up using a voltmeter;
 - (b) check to see if port transmission is working – com port, modem or Ethernet (TCP/IP);
 - (c) check for typical sounds associated with a modem – the dial up sound or the answering exchange sound. Test the phone line using an analog phone to be sure the phone line is operating;
 - (d) check whether the serial port is active. Use Device Manager in Windows. See Loop Back Test for Serial Ports to verify the serial port is working.

Note

Procedure D may also be performed at a Communications Manager.

Procedure E – Serial Port Connections

Loop Back Test for Serial Ports

Performing a loop back test will determine if your serial port is operating correctly.

To perform the loop back test

1. Go to the location of the access control unit and remove the TD & RD wires from the main circuit board or CPB-10 that are wired back to the computer. These conductors transmit and receive ASCII data.
2. Short the wires together.
3. Go to the PC with the Communications Manager.
4. Log on to the Communications Manager. Be sure to select the appropriate site.
5. Click on the Unit Diagnostic button.

6. Select the Select Communications menu > Switch Unit > appropriate ACU (must have com port assignment).
7. Press any letter on the keyboard. The letter pressed on the keyboard should echo back to the monitor. If this didn't happen, the com port isn't available or the wiring is suspect. If the letter echoed back to the monitor, proceed to the next step.
8. Return to the ACU.
9. Un-short the TD and RD wires and leave them disconnected.
10. Return to the PC with the Communications Manager and press a letter on the keyboard. If an echo occurs, either you have a conflict with another device or a faulty com port. Type AT and press Enter on the keyboard. If OK is displayed on the screen, you have a conflict with the modem on the same port. If there was no echo on the screen, the result indicates there is no conflict with a modem. Contact the provider of the PC for further hardware support.
11. Return to the ACU and re-connect the TD and RD wires to their proper terminals.

Procedure F – TCP/IP Connections

Test for TCP to Serial Box (MSS-COMM) Connection

1. Turn off the appropriate Communications Managers.
2. Go to a PC that has Telnet enabled.
3. Click on the Start button and select Run.
4. In the Run window's text box, type TELNET and the IP address of the MSS-COMM unit.
5. Click on the OK button.
6. Leave the Telnet window open.
7. Click on the Start button again and select Run.
8. In the Run window's text box, type TELNET, the IP address of the MSS-COMM unit, followed by 3001.
9. Click on the OK button. You should now have two Telnet session windows open.
10. From the first Telnet window, at the prompt, type your user ID for the MSS-COMM unit.
11. At the prompt, type SHOW PORT and press Enter. Under Physical Port 1, you will see either Job Service or Idle.
 - Job Service – the PC port is connected to the MSS-COMM unit & the current session indicates the IP address of the connected PC. Proceed to the next step.
 - Idle – the PC port is not connected to the MSS-COMM unit. Check with the IT administrator.
12. Record the value beside and Bytes Output.
13. Click inside the second Telnet (3001) window to make it the active window on the

desktop.

14. Type some random characters on the keyboard.
15. Click inside the first Telnet window to make it the active window again. At the prompt, type SHOW PORT, and press Enter.
16. Compare the values of Bytes Output that you recorded versus that which is now listed in the first Telnet window. It should show an increased value.
 - The MSS-COMM unit tracks what it transmits and receives as Input Bytes and Output Bytes sent serially.
17. Go to the location of the access control unit and remove the TD & RD wires from the main circuit board or CPB-10 that are wired back to the computer. These conductors transmit and receive ASCII data.
18. Short the wires together.
19. Return to the PC with Telnet and select the second Telnet (3001) window to make it the active window.
20. Press any letter on the keyboard. The letter pressed on the keyboard should echo back to the monitor.
 - Echo – the MSS-COMM is functioning. Investigate the ACU hardware.
 - No Echo – investigate the serial cable.
21. Return to the ACU and re-connect the TD & RD wires.

Procedure G – Modem Connections

Test for Modem Connection

1. Go to the PC with the appropriate Communications Manager.
2. Log on to the Communications Manager
3. Select the Utilities menu and enable Communication Port Status. The text of the Communication Port Status reported in the transaction window should be green.
4. Click anywhere within the Communication Manager's transaction window to stop transaction reporting.
 - If message – Com # Port Open (Modem), indicated in green, the port is available to the Communications Manager. Go to the next step.
 - If message – Unexpected Com Port Error, consult with the PC provider.
5. Click on the Unit Diagnostic button.
6. From the Unit Diagnostic window, select the Select Communications menu > Switch Unit > appropriate ACU (must have com port assignment).
7. Type AT and press Enter on the keyboard. The window displays OK.

8. Type ATDT and the phone number of the remote ACU and press enter on the keyboard. One of the following messages is displayed in the window.
 - No Carrier – Host modem has no line out. Consult with phone provider.
 - Busy – Line is busy. Retry last step. If problem continues, consult with phone provider.
 - Connect 9600 – Modem is communicating. Investigate ACU hardware.
 - Connect ### (lists another baud rate other than 9600) – Modem compatibility problem. Contact Keyscan technical support.

Procedure H – Reader/Cards

Test a Reader or a Card

Card does not read at the reader. Generally the most common error is an incorrect batch number or card number entry. (The batch number may also be referred to as the site code or facility code.)

To Test a Card/Reader from the Client software

1. Go to the reader and scan the card a minimum of six times. An Invalid Code alarm is not generated until after the 5th pass of the card over the reader.
2. Return to the PC with the Keyscan Client software. Be sure you have logged on to the appropriate site.
3. From the Client main screen, click on the Display Online Transactions quick button. If there is an Invalid Code message, then the potential problem could be an incorrect card batch/number entry, the card is not on file, or the card has been archived.
4. Close the Online Transaction form.
5. From the Client main screen, click on the Cardholder Database quick button > Edit/Delete Card(s).
6. From the Search Access Card Holders form, enter the cardholders first and last name in the appropriate fields.
7. Click on the Find Card(s) button. Check the card information and make any necessary corrections. Be sure to save the changes, if you altered the card holder record.
8. Return to the reader and re-scan the card to ensure it works. If the card information was correct and it still does not read at the reader, continue to the next step.
9. Return to the PC with the Keyscan Client and click on the Update Changes quick button.
10. From the Panel Updates form, click on the down arrow to the right of Unit Selection and from the drop down list, select the ACU that controls the reader.
11. Click on the View Reader Diagnostics button.
12. Go to the reader and scan the card.
13. Return to the PC with the Keyscan Client. If the reader is working, the batch and card numbers are listed in the black window of the Panel Updates form. If this is the case re-

check the card information. If there is no card information listed in the black window, the reader or the wiring may be faulty. Call your service vendor.

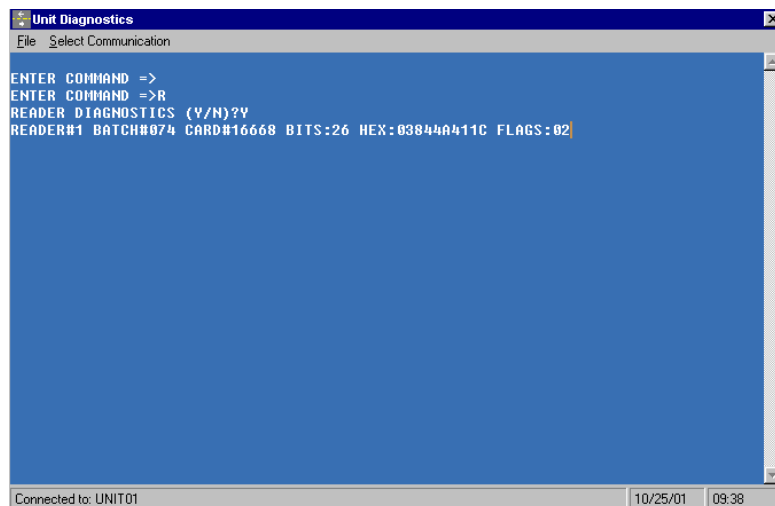
14. Press the escape (Esc) key then click on the Exit button of the Panel Updates form to return to the Client main screen.

To Test a Reader/Card from the Communications Manager

This procedure is an alternative method for dealers to test cards or readers from a Communications Manager.

1. Log on to the Communication Manager. Be sure to select the appropriate site.
2. Click on the Unit Diagnostic button.
3. From the Unit Diagnostic form, click on the Select Communication menu and select the appropriate access control unit.
4. From the Enter Command prompt, type R. This opens the Reader Diagnostic utility.
5. Press Enter. Leave the Reader Diagnostic window open.
6. Return to the reader and present the card to the reader.
7. Return to the Communications Manager PC. If the reader is working, the Reader Diagnostic utility will have recorded the Batch # and the Card #. If this is the case recheck the card information.
8. If there is no data recorded by the Reader Diagnostic utility, then it is most probable that the reader or wiring is faulty. Call your service vendor.

Example of Unit Diagnostic window



Part 6: Database Recovery

In the event that you have replaced or changed the computer with the Keyscan Database Maintenance (MSDE) module, one of the following three methods is available to restore your site data after you have re-installed the Database Maintenance module.

- Restore DB Backup method
- Copy Database Files to MSSQL7/Data Folder method
- Panel Recovery (Disaster Recovery) method

You must have a backup copy of your site database to employ either the Restore DB Backup or the Copy Database Files to MSSQL7 methods. Use the Panel Recovery method if you do not have a backup copy of your database. This method recovers site data directly from the access control units, however, not all site data is recovered.

Before you undertake any of these three procedures, please call Keyscan technical support Monday to Friday, 9 a.m. to 5 p.m., Eastern Standard Time, to verify your System V software version is up-to-date. Our technical support staff can also assist you with the procedures, if needed.


Restore DB Backup Method

The Restore DB Backup allows you to re-load your site data after re-installing the Database Maintenance module. If you did not make a backup copy of your database, you cannot use the Restore DB Backup method.

Networks

If your system operates on a network and you have re-installed the Database Maintenance 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. The Database Location form is accessed from the System Settings menu. You should consult with an IT administrator prior to conducting the following procedures.

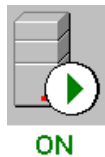
Preliminary Steps



1. At the appropriate PC location(s), close the Keyscan Client Software module(s) by selecting the File menu > Exit command.
2. At the appropriate PC location(s), close the Communication Manager(s). If the Communication Manager is minimized, double click on the COM icon  in the status bar, enter your User ID and Password, click on the OK button, and then click on the Exit button to close the Communication Manager. You should not see the Communication Manager icon in the lower right corner of the status bar when the Communication Manager is off.

3. Close the Photobadge Template Editor(s) by selecting the File menu > Exit command.

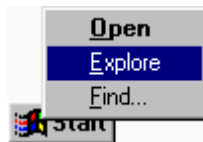
Steps to Restore Database

1. Locate the computer with the Database Maintenance module.
2. Ensure that the SQL Server Service Manager is ON as illustrated below. The SQL Server Service Manager icon is located in the lower right corner of the monitor.

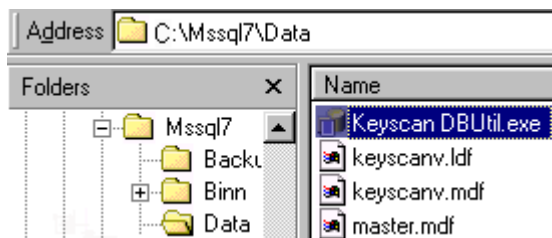


If the SQL Server Service Manager is off , double click on the SQL Server Service Manager icon; click on the Start/Continue button; wait until the Service Manager starts; click on the  button in the upper right corner to close the SQL Server Service Manager form.

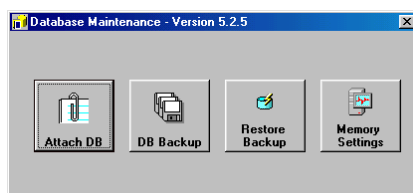
3. Right click on the Start button in the lower left corner of the monitor, and select Explore.



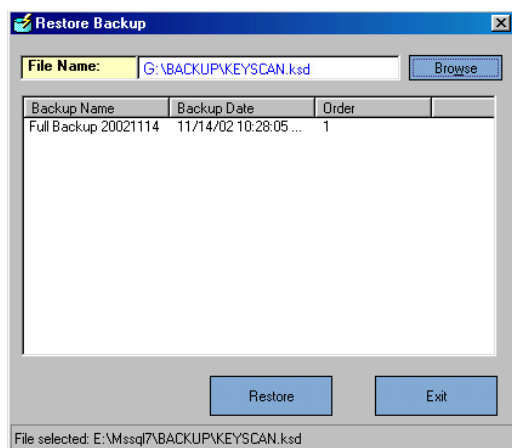
4. From Windows Exploring, select the appropriate drive where the Database Maintenance module was installed, navigate to the Mssql7\Data folder, and double click on the Keyscan DBUtil.exe file.



5. From the Database Maintenance form, click on the Restore Backup button.



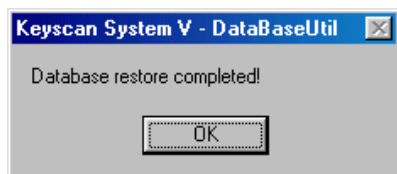
6. From the Restore Backup form, either enter the drive, folder location, and backup file name in the File Name text box, or click on the Browse button, navigate to the correct folder location, select the backup file, and click on the Open button.



7. Click on the Restore button.
8. Click on the Yes button to close the Restore Backup warning box.

If you are prompted with a Restore Database Error warning box, check to be sure that the Client Software and Communication Manager modules are off. Click on the OK button to close the warning box and start the Restore DB Backup procedures over. If the problem persists with the Restore Database Error warning, please call Keyscan for assistance.

9. Click on the OK button to close the Keyscan System V Database Utility confirmation box.



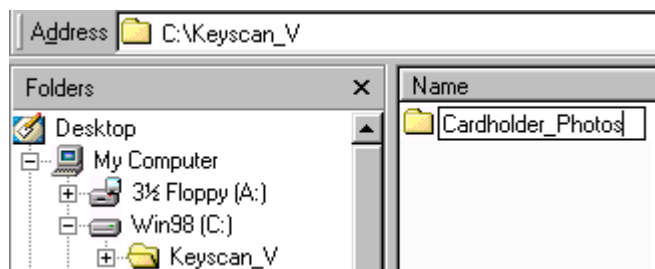
10. Click on the Exit button to close the Restore Backup form.
11. Click on the button in the upper right corner of the Database Maintenance form to exit.
12. Open and logon to the Communications Manager(s) and the Client Software modules.

Steps to Re-establish Card Holder Photos and Folder Location

In order to re-establish card holder photos, site maps, signatures, and alarm images, you must have created a backup copy of these files in order to carry out the following procedures. If your system operates on a network, you may wish to consult with an administrator. Please refer to the sub-heading Card Holder Photo Location on page 32 for network share conventions.

1. From the PC location where the card holder photos are to be stored, click the Start button in the lower left corner of the monitor, and select Explore.
2. Insert the backup medium with the images or navigate to the network location where the backup copies of the images are stored, whichever is applicable.

3. Select the backup image files.
4. With the files still selected, click on the Copy button on the Toolbar.
5. If applicable, create a folder where you are going to paste the backup image files. If a folder already exists bypass this step.



6. With the folder selected on the PC where you are going to re-locate your image files, click on the Paste button.
7. Select all the pasted image files, select the File menu > Properties. In the Attributes section of the Properties form, if Read Only is checked, de-activate this file attribute, and click on the OK button.
8. Close Windows Exploring by selecting the File menu > Close.
9. From the Keyscan Client Software module, select the System Settings menu > Site Setup, and double click on the site name in the yellow table of the Site Information Search form.
10. From the Site Information form, if the Card Holder Folder Location has changed, enter the drive and folder name in the Card Holder Photo Location text box. Please note, for network configurations with multiple Client software modules, the Card Holder Folder Location must be shareable by all users. You only have to specify this location in one Client module. If the Card Holder Folder location is unchanged bypass this step.

Card Holder Folder Location
C:\Keyscan_V\Cardholder_Photos

11. Click on the Save & Exit button to close the Site Information form.
12. Click on the Exit button to close the Site Information Search form and return to the main screen.

Copy Database Files to MSSQL7/Data Folder Method

The second method to restore your database is to copy the following two files into the Mssql7/Data folder:

- KeyscanV.ldf
- KeyscanV.mdf


To use this method, you must have copied these two files directly from the Mssql7/Data folder to another location or on a removable storage medium at some point prior to losing the services of the PC or network location where the Database Maintenance module was installed.

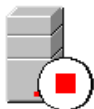
If either the KeyscanV.ldf or KeyscanV.mdf file is larger than 2 gigabytes, they cannot be copied using the following procedures. Please call Keyscan technical support for assistance.

Networks

If your system is operating on a network and you have re-installed the Database Maintenance 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. The Database Location form is accessed from the System Settings menu. You should consult with an IT administrator prior to conducting these procedures.

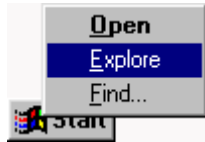
Preliminary Steps

1. Close the Keyscan Client Software module(s) by selecting the File menu > Exit command.
2. At the appropriate PC location(s), close the Communication Manager(s). If the Communication Manager is minimized, double click on the COM icon  in the status bar, enter your User ID and Password, click on the OK button, and then click on the Exit button to close the Communication Manager. You should not see the Communication Manager icon in the lower right corner of the status bar when the Communication Manager is off.
3. Close the Photobadge Template Editor(s) by selecting the File menu > Exit command.
4. Ensure that the SQL Server Service Manager is OFF. The SQL Server Service Manager icon is located in the lower right corner of the monitor on the PC where the Database Maintenance module is installed.

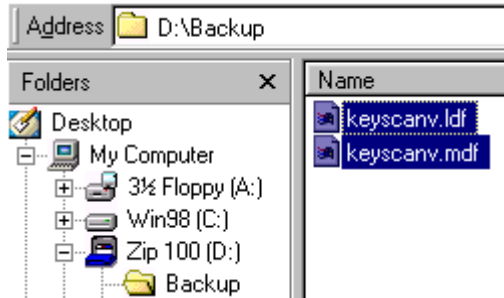


Steps to Copy Database Files to MSSQL7 Data Folder

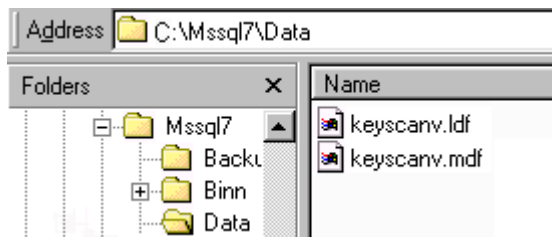
1. From the computer with the Database Maintenance module, right click on the Start button in the lower left corner of your monitor and select Explore.



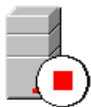
2. Navigate to the drive and folder where the backup copies of the – KeyscanV.ldf and KeyscanV.mdf – files are located.
3. Press the Ctrl key and select both files.



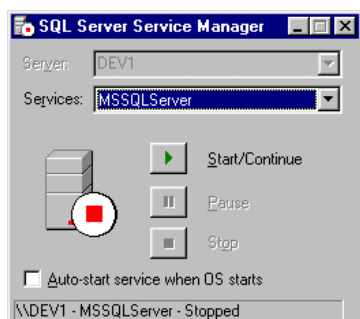
4. Click on the Copy button at the top of the Exploring window, or select the Edit menu > Copy command.
5. Navigate to the Mssql7\Data folder and select the Paste button or select the Edit menu > Paste command.




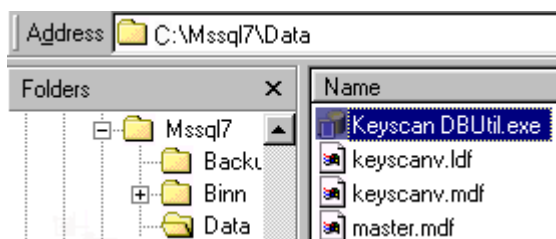
6. Click on the Yes to All button in the Confirm File Replace warning box.
7. Select the File menu > Close command to exit Exploring.
8. In the lower right corner of the monitor in the status bar, double click on the SQL Server Service Manager icon.



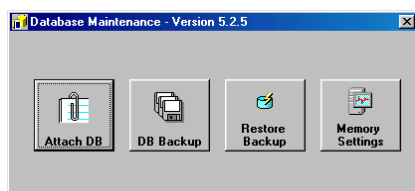
9. From the SQL Server Service Manager window, click on the Start/Continue button.



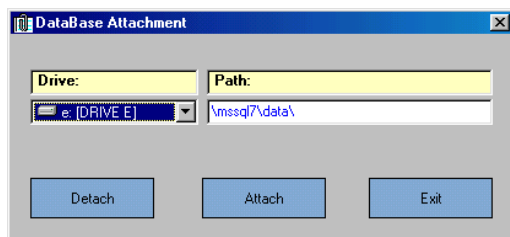
10. Wait until the SQL Server Service Manager has started.
11. Close the SQL Server Service Manager by clicking on the  button in the upper right corner of the window.
12. Navigate to the Mssql7\Data folder and double click on the Keyscan DBUtil.exe file.



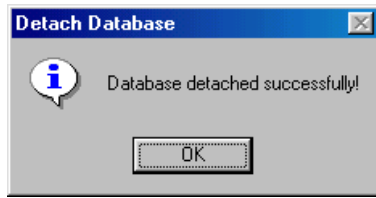
13. Click on the Attach DB button in the Database Maintenance window.




14. Verify the correct Drive and the Path - Mssql7\Data are specified in the Database Attachment form.



15. Click on the Detach button in the Database Attachment window. If either file exceeds 2 gigabytes, do not detach. Call Keyscan for assistance.
16. Click on the OK button in the Database Detached Successfully confirmation box.

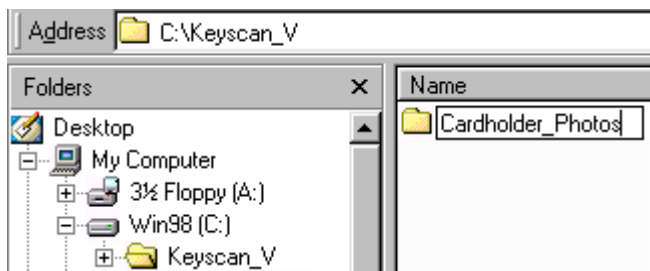


17. Click on the Attach button in the Database Attachment form.
18. Click on the OK button in the Database Attached Successfully confirmation box.
19. Click on the Exit button in the Database Attachment form.
20. Click on the  button in the upper right corner to close the Database Maintenance form.
21. Open the Communication Manager(s) and the Client(s) modules to resume system operations.
22. If you have a network configuration with multiple Client software modules, verify the IP Address of the Database Maintenance module is set correctly on each Client module.

Steps to Re-establish Card Holder Photos and Location

In order to re-establish card holder photos, site maps, signatures, and alarm images, you must have created a backup copy of these files in order to carry out the following procedures. If your system operates on a network, you may wish to consult with an administrator. Please refer to the sub-heading Card Holder Photo Location on page 32 for network share conventions.

1. From the PC location where the card holder photos are to be stored, click the Start button in the lower left corner of the monitor, and select Explore.
2. Insert the backup medium with the images or navigate to the network location where the backup copies of the images, etc. are stored, whichever is applicable.
3. Select the card holder image files.
4. With the files still selected, click on the Copy button on the Toolbar.
5. If applicable, create a folder where you are going to paste the backup image files. If a folder already exists bypass this step.



6. With the folder selected on the PC where you are going to re-locate your image files, click on the Paste button.
7. Select all the pasted image files, select the File menu > Properties. In the Attributes

section of the form, if Read Only is checked, de-activate this file attribute, and click on the OK button.

8. Close Windows Exploring by selecting the File menu > Close.
9. From the Keyscan Client Software module, select the System Settings menu > Site Setup, double click on the site name in the yellow table of the Site Information Search form.
10. From the Site Information form, if the Card Holder Folder Location has changed, enter the drive and folder name in the Card Holder Photo Location text box. Please note, for network configurations with multiple Client software modules, the Card Holder Folder Location must be shareable by all users. You only have to specify this location in one Client module. If the Card Holder Folder location is unchanged bypass this step.

Card Holder Folder Location
C:\Keyscan_V\Cardholder_Photos

11. Click on the Save & Exit button to close the Site Information form.
12. Click on the Exit button to close the Site Information Search form and return to the main screen.

Panel Recovery Method

If you do not have a backup copy of your site database, the panel recovery method acts as a last resort. This method uses the Disaster Recovery utility to retrieve site data directly from the door and elevator control units. It does not recover all your site data, but it does allow you to get your site re-functioning quickly. The Disaster Recovery utility is on the Keyscan System V Software installation CD.

You need the serial number and password for each access control unit to perform the panel recovery. The serial number is listed on the main circuit board inside the access control units. The default password for all Keyscan access control units is KEYSCAN. If you previously changed the access control unit password, you cannot use the default password. Only use Panel Recovery after a fresh install with a clean database. If you have a Cardholder CSV file, which holds more cardholder data than the access control units, you can import that file prior to recovering data from the panels.

The table below lists the data that is recovered:

Access Control Unit	
Card Holder Information	
8000 Card Mode	16,000 Card Mode *
First Name – First character	First Name – No Characters
Last Name – First 8 characters	Last Name – No Characters
Batch Number	Batch Number
Card Number	Card Number
Door Group Access Level A	Door Group Access Level A
Door Group Access Level B	Door Group Access Level B
Temporary Card Options (if specified)	Temporary Card Options (if specified)
Archived Card (if enabled)	Archived Card (if enabled)
Site Details	
Site Setup	Site Setup
Door and Elevator Parameters	Door and Elevator Parameters
Time Zones and Assignments	Time Zones and Assignments
Door/Elevator Groups	Door/Elevator Groups

*** Note**

Access control units with an E-Prom version 6.2 or higher have two card modes – 8000 card mode and 16,000 card mode. For 16,000 card mode, system jumper J16-4 is in the OFF position.

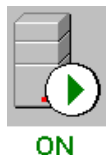
Access control units with an E-Prom version of 6.1 or lower only have the 8000 card mode.



The E-Prom version is listed on the main circuit board inside the access control unit.

Steps to Import a CSV File

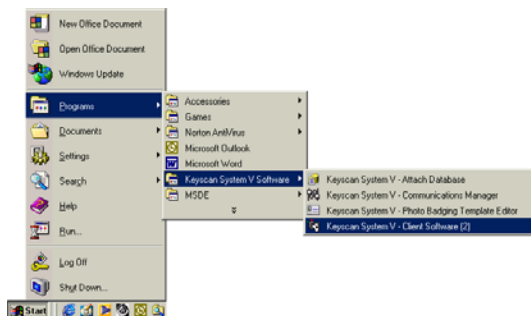
If you have a CSV file containing card holder records you can import that file to recover your card holder data. If you do not have a CSV file, bypass these procedures and start at Preliminary Steps for Panel Recovery.

1. Ensure that the SQL Server Service Manager is ON as illustrated below. The SQL Server Service Manager icon is located in the lower right corner of the monitor.



If the SQL Server Service Manager is off , double click on the SQL Server Service Manager icon; click on the Start/Continue button; wait until the Service Manager starts; click on the  button in the upper right corner to close the SQL Server Service Manager form.

2. Open the Client software module, if it is not open, by selecting Start > Programs > Keyscan System V Software > Keyscan System V – Client Software

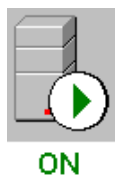




3. From the Client Software main screen, click on the Card Holder Database quick button > Search Access Card Holders.
4. In the upper left corner of the Search Access Card Holders form, click on the Import and Export Card Holder Information menu > Import Card Holder Information.
5. From the Keyscan Import Card File dialog box, select the CSV file that you are importing.
6. Click on the Open button.
7. The Import and Export Card Holder Information form lists the import status - Successfully Imported Card Holders - # or Failed to Import Card Holders - #. If you receive a Failed message, refer to the Client Software Help menu > Contents > Operating the System > Cardholders > Import Cardholder Information > Conventions for Importing CSV files to be sure your CSV file conforms to the correct conventions. You may have to edit the file in a spreadsheet.

8. Click on the Exit button.

Preliminary Steps for Panel Recovery


1. Verify the SQL Server Service Manager is ON as noted below.

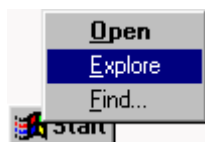


If the SQL Server Service Manager is off , double click on the SQL Server Service Manager icon; click on the Start/Continue button; wait until the Service Manager starts; click on the  button in the upper right corner to close the SQL Server Service Manager form.

2. Verify the Communication Manager is on. If you have a configuration with multiple Communication Managers and all hardware is networked using MSS-COMM, be sure all other Communication Managers are off. Be sure Poll Single Site is unchecked (disabled) on the active Communication Manager.
3. Verify that all Client modules are off.

Panel Recovery Steps

1. Insert the Keyscan System V Software Installation/Program disk in the CD-ROM drive.
2. If the Installation Procedures auto loads, close it by clicking on the  in the upper right corner of the window.
3. Right click on the Start button in the lower left corner of the monitor and select Explore.



4. Navigate to the Utilities/Disaster Recovery folder on the Keyscan CD.
5. Double click on the DisasterRecovery.exe file.
6. From the Disaster Recovery Logon form, bypass selecting a language and a site name. They do not apply to the Disaster Recovery logon.



7. Enter keyscan in the User Name text box.
8. Enter KEYSCAN (upper case) in the Password text box.
9. From the Disaster Recovery window, enter the serial number of the access control unit in the Serial # text box.
10. Enter the password of the access control unit. The factory default password is KEYSCAN unless it has been changed.
11. Click on the down arrow to the right of Communication Setup and select the mode of communication from the drop down list. If Network is selected, enter the IP address in the IP Address text box. If Dial Up is selected, enter the telephone number in the Auto Dial Telephone Number text box.

Communication Setup – Serial

The screenshot shows the 'Disaster Recovery Utility - Version 5.2.5' window. The 'Serial #' field contains 'R1234'. The 'Unit Password' field contains 'KEYSCAN'. The 'Communication Setup' dropdown menu is set to 'Serial'. The 'Communications Port' dropdown menu is set to '1'. There are 'Start', 'Clear', and 'Exit' buttons on the right side of the window.

Communication Setup – Network

The screenshot shows the 'Disaster Recovery Utility - Version 5.2.5' window. The 'Serial #' field contains 'R1234'. The 'Unit Password' field contains 'KEYSCAN'. The 'Communication Setup' dropdown menu is set to 'Network'. The 'IP Address' field contains '123.456.789.123'. There are 'Start', 'Clear', and 'Exit' buttons on the right side of the window.

Communication Setup – Dial-Up

The screenshot shows the 'Disaster Recovery Utility - Version 5.2.5' window. The 'Serial #' field contains 'R1232'. The 'Unit Password' field contains 'KEYSCAN'. The 'Communication Setup' dropdown menu is set to 'Dial-Up'. The 'Communications Port' dropdown menu is set to '1'. The 'Auto Dial Telephone Number' field contains '416-234-1234'. There are 'Start', 'Clear', and 'Exit' buttons on the right side of the window.

12. Click on the down arrow to the right of Communications Port and select the port from the drop down list.

13. Click on the Start button.
14. Repeat steps 9 to 13 to recover the data from each access control unit within the site.
15. Select the Exit button when you have completed recovering data from all access control units from the site.
16. If you have more than one site to recover, start at the Preliminary Steps and repeat the procedures.

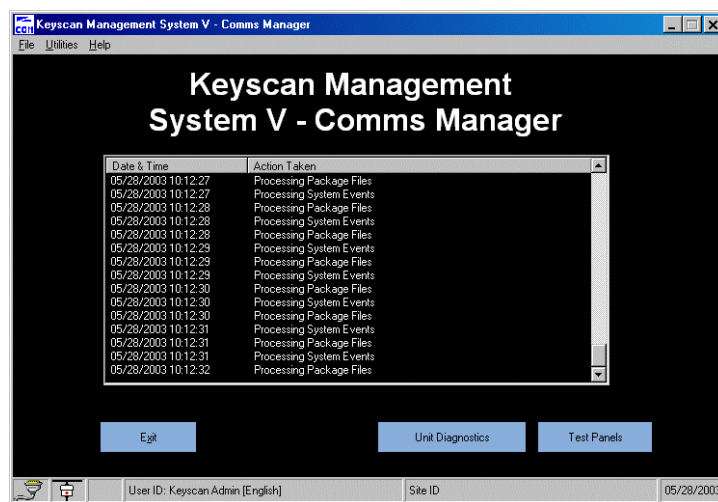
Part 7: Communications Manager

Overview

The Communications Manager, also referred to as the Communications Server, acts as an intermediary software application between the database and the access control and elevator control units. Based on a predetermined cycle, the Communications Manager regularly polls all access and elevator control units for site transactions and updates the database accordingly. Conversely, when an operator enters or edits information in the Client application, the data that is saved to the database is uploaded to the access and elevator control units by way of the Communications Manager.

The Communications Manager must always be on in order for the access control system to function and generally operates in the background in a minimized state.

Communications Manager – Main Screen



Review of Communications Manager Main Screen and Menus

Transaction Window

Date & Time	Lists the Month / Day / Year / Hour / Minute / Second of the transaction.
Action Taken	Processing Package Files is an exchange of data between the database and the Communications Server. Processing System Events is an exchange of data between the access control units and the Communications Server. Test Ends message shows result after selecting the Test Panels button.
Unit Diagnostics button	Unit diagnostics allows a system user to verify the date and time on the access control unit clock or investigate card/reader problems.
Test Panels button	The Test Panels button verifies the data link between the logged on Communications Manager and the tagged access control units is intact. The test responds with one of the following messages: OK – communication with the panel was successful No Response – communication with the panel was unsuccessful Can't Send Data – invalid access control unit password
Exit button	Closes the Communications Manager.

Menus

File

Select Site	Select Site allows an authorized system user to perform Unit Diagnostics at another site that is polled by the Communications Server that the operator is currently logged on.
Auto Start Communications Server	Auto Start Communications Server automatically starts the Communications Server when the computer is powered up.
Remove Start Communications Server	Remove Auto Start Communications Server disengages the automatic startup above.
Display ACU Polling List	Opens the Site/Panels Polling Setup form to tag ACUs to Communications Managers.

Site/Panels Polling Setup form

Site ID/Unit ID table	Lists the sites and access control units by Site ID and Unit ID. A checked box indicates the Site/Unit is tagged to the logged on Communications Manager An open box indicates the Site/Unit is not tagged to any Communications Manager.
Select All button	Selects all sites/units on display in the Site/Panels Polling Setup form of the logged on Communications Managers.
Deselect All button	De-selects all sites/units on display in the Site/Panels Polling Setup form of the logged on Communications Managers.
Clear All button	Clears all site/unit tags for all Communications Managers. Use discretion with this function. All access control units must be re-tagged to

with this function. All access control units must be re-tagged to Communications Managers or the system will not operate.

OK	Saves the site/unit settings.
Cancel	Aborts any changes since the previous save.

Utilities

Communication Port Status	The text of the Communications Port Status reported in the transaction window changes to green for easier identification.
Enable Serial Output	Activating the Enable Serial Output option allows for interfacing with a paging system or other 3rd party product. Emulating the data collected for the database, the system transmits the information to the device via the serial port.

Help

Contents/Index/Search for Help On	Opens the Communications Manager Help for program assistance.
Software Updates	Hyperlink connection to the www.keyscan.ca website download page.
About	Lists the version of the Communications Manager application.

Communications Manager User Account

Keyscan recommends creating a specific system user account, which you must setup in the Client module, for accessing the Communications Manager. The Communications Manager is used primarily by dealers/installers during initial system setup or for troubleshooting after the system is operational. End-users will rarely if ever have cause to log on to the Communications Manager.

If you create one specific user account to access multiple Communications Managers with multiple sites, you must make the following conditions true, irrespective of any other user authority levels:

- The Communications Manager user account is copied to each site
- Enable Viewing All Site Transactions is selected on each account
- User ID and Password are the same for each account

The benefit of creating a specific Communications Manager user account is that it identifies who has logged on and performed activities at each Communications Managers when viewing the System Log in the Keyscan Client module.

For more information on setting up a system user account, refer to Setup System Administrators/Users on page 91.

Log on the Communications Manager


Only operators authorized as system users in the Client application can access the Communications Manager. Each time the Communications Manager is accessed, you must log on with your User ID and Password.

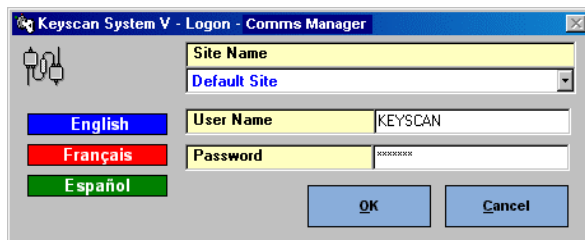
Note

To open or view a Communications Manager you are required to log once. To

perform any tasks within the Communications Manager, you are required to log on twice.

Steps to Log On to the Communications Manager

1. Double click on the Communications Manager icon  in the lower right corner of the screen if it is running in a minimized state, or select the Start button in the lower left corner and select All Programs > Keyscan System V Software > Keyscan System V – Communications Manager if it is closed.
2. From the Log On box, if appropriate, click on the – English, Français, or Español button to change the program interface to your preferred language.




3. If necessary, click on the down arrow to the right of the Site Name text box, and select the name of the site from the drop down list.
4. Enter your User Name in the text box to the right.
5. Enter your Password in the text box to the right. Passwords are case sensitive.
6. Click on the OK button.

Auto Start the Communications Manager

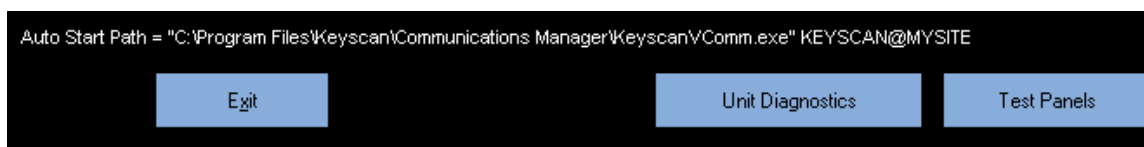
We recommend enabling the Auto Start Communications Server function. In the event a PC with the Communications Manager is shut down from a power failure or system crash, the access control system communications are automatically restored when the PC is re-booted.

Generally, this function is enabled when the Communications Manager is first installed. To verify the Auto Start Communications Server function is enabled, review Steps to Verify Auto Start the Communications Server immediately following this paragraph. If Auto Start is not enabled continue to Steps to Auto Start Communications Server.

Steps to Verify Auto Start the Communications Server

1. Double click on the Communications Manager icon  in the lower right corner of the screen if it is running in minimized state, or select the Start button in the lower left corner and select All Programs > Keyscan System V Software > Keyscan System V – Communications Manager if it is closed.
2. Log on to the Communications Manager as outlined in the preceding sub-topic Steps to Log On to the Communications Manager. Ensure that you have selected the correct site when logging on.

3. Select the File menu. If Auto Start Communications Server is enabled, the function has a check mark (✓). As well, the Auto Start Path is listed near the bottom of the Communications Manager's transaction window confirming Auto Start is enabled.



Steps to Auto Start Communications Manager

1. This assumes that you have continued from Steps to Verify Auto Start the Communications Server and that you are logged on to the correct site. If not minimize the Communications Manager and re-log on to the correct site.
2. From the File menu, select Auto Start Communications Server.
3. Click on the minimize button.

When to Reset Auto Start on the Communications Manager


In the event that you deleted the site or the system user that the Communications Manager was set to auto start on, resetting this function is imperative. Auto start is based on a path when it is set. Part of the path includes the User ID and the Site ID. Deleting either the system user account or the site breaks the continuity of the path. Should the PC with the Communications Manager experience a power failure or it crashes, when it's re-booted, the system reports a communication failure. The following example illustrates an Auto Start Path where KEYSCAN is the User ID and MYSITE is the Keyscan default site.

- Auto Start Path = "C:\Program Files\Keyscan\Communications Manager\KeyscanVComm.exe" KEYSCAN@MYSITE

Auto Start Path = "C:\Program Files\Keyscan\Communications Manager\KeyscanVComm.exe" KEYSCAN@MYSITE

To change the Communications Manager to auto start on an alternative site or a system user follow these procedures.

Steps to Reset Auto Start Communications Manager

1. Double click on the Communications Manager icon  in the lower right corner of the screen if it is running in minimized state, or select the Start button in the lower left corner and select All Programs > Keyscan System V Software > Keyscan System V – Communications Manager if it is closed.
2. From the log on screen, if appropriate, click on the – English, Français, or Español button to change the program interface to your preferred language.
3. Click on the down arrow to the right of the Site Name text box and from the drop down list, select the name of the site that you want the Communications Manager to auto start on.
4. Enter your User Name in the text box to the right.

5. Enter your Password in the text box to the right. Passwords are case sensitive.
6. Click on the OK button.
7. Click on the File menu and de-select Remove Auto Start Communications Server.
8. Click on the File menu and select Auto Start Communications Server.
9. Click on the minimize button.

Conventions for Configuring ACUs on Multiple Communications Managers

When more than one (1) Communications Manager is installed, each ACU in the access control system must be assigned or tagged to a specific Communications Manager. The following three (3) conventions apply when tagging ACUs to multiple Communications Managers:

- 1 Communications Manager for each site
- 1 Communications Manager for a group of access control units within 1 site
- 1 Communications Manager for a group of access control units across multiple sites

Communications may be established by MSS-COMMs (TCP to Serial Converter), modem, or serial connection within the same Communications Manager.

Important

Do not install more than one Communications Manager on a PC.

By default, any untagged ACUs will be polled by the Communications Manager that was installed first.

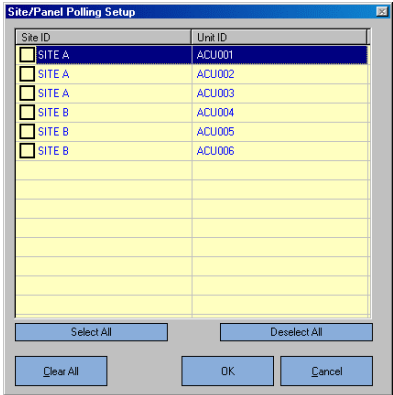
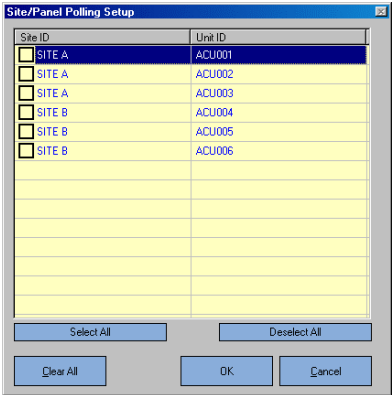
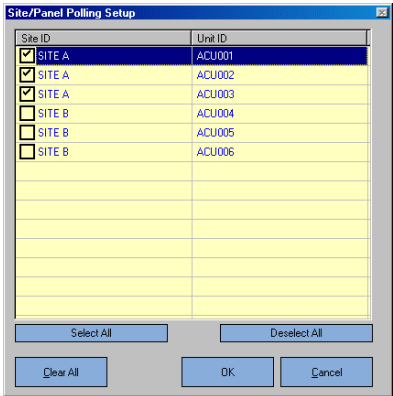
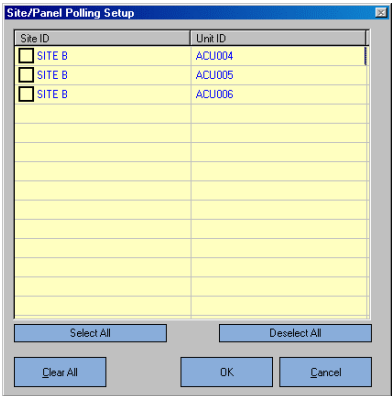
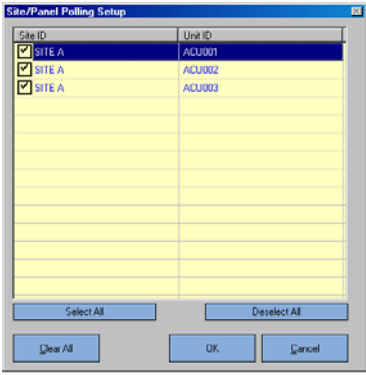
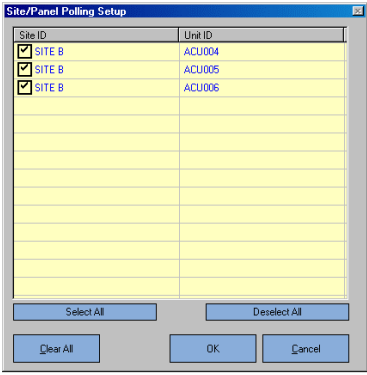
ACUs are tagged using the Site/Panel Polling Setup form in the Communications Manager. Once an ACU has been tagged to a Communications Manager it is unavailable and non-viewable by all other Communications Managers.

Page 131 illustrates the appearance of the Sites/Panels Polling Setup form as ACUs are assigned to multiple Communications Managers. In the example, two Communications Managers will each poll 3 ACUs at two different sites – Site A and Site B. Initially all ACUs are visible to each Communications Manager. Once all ACUs are tagged, the Sites/Panels Polling Setup form lists only those ACUs tagged to the logged on Communications Manager.


For Steps to Tag ACUs to Specific Communications Managers see page 132.

For re-assigning ACUs to an alternative Communications Manager, see page 132, or for adding a new panel with multiple Communications Managers, see page 133.

Tagging ACUs to Communications Managers – Site/Panel Polling Setup form

Communications Manager – PC1	Communications Manager – PC2
ACUs – 001, 002, 003 (Site A)	ACUs – 004, 005, 006 (Site B)
No ACUs selected	No ACUs selected
	
ACUs selected – Communications Manager PC1	ACUs available Communicaions Manager PC2
	
ACUs selected – Communications Manager PC1	ACUs selected – Communicaions Manager PC2
	

Steps to Tag ACUs to Specific Communications Managers

1. Go to a PC where a Communications Manager was installed.
2. Double click on the Communications Manager icon  in the lower right corner of the screen if it is running in minimized state, or select the Start button in the lower left corner and select All Programs > Keyscan System V Software > Keyscan System V – Communications Manager if it is closed.
3. From the Log On box, if appropriate, click on the – English, Français, or Español button to change the program interface to your preferred language.
4. Click on the down arrow to the right of the Site Name text box and from the drop down list select the name of the site.
5. Enter your User Name in the text box to the right.
6. Enter your Password in the text box to the right. Passwords are case sensitive.
7. Click on the OK button.
8. Click on the File menu, and select Display ACU Polling List.
9. From the Site/Panel Polling Setup form, select the ACUs that the Communications Manager is to poll by clicking in the box to the left. Selected ACUs have a check mark ✓ in the box.
10. Click on the OK button.
11. Click on the minimize button to keep the Communications Manager running in the background.
12. Re-locate to another PC with a Communications Manager and repeat the above procedures until all ACUs have been tagged to Communications Managers. As each Site Panel Setup form is opened, only untagged ACUs are listed.

Re-assigning ACUs to an Alternative Communications Manager


In the event an ACU has to be re-tagged to another Communications Manager, first it must be released at the PC with the Communications Manager where it is currently tagged before it may be re-assigned. After it has been released, it may then be re-assigned at another PC with a Communications Manager.

Note

For systems running multiple Communications Managers, if the PC with a Communications Manager you are currently setting crashes, you must log on again, open the Site/Panels Polling Setup form, click on the Clear button and re-tag all access control units at all Communications Managers.

Steps to Re-assign ACUs to an Alternative Communications Manager

1. Go to the PC with the Communications Manager that is tagged to the ACU you are re-assigning.

2. Double click on the Communications Manager icon  in the lower right corner of the screen if it is running in minimized state, or select the Start button in the lower left corner and select All Programs > Keyscan System V Software > Keyscan System V – Communications Manager.
3. If appropriate, click on the – English, Français, or Español button to change the program interface to your preferred language.
4. Click on the down arrow to the right of the Site Name text box and from the drop down list select the name of the site.
5. Enter your User Name in the text box to the right.
6. Enter your Password in the text box to the right. Passwords are case sensitive.
7. Click on the OK button.
8. Click on the File menu, and select Display ACU Polling List.
9. From the Site/Panel Polling Setup form, click in the box to the left to de-select the ACU(s) that you are re-assigning to an alternative Communications Manager. The box does not have a check mark when an ACU is de-selected.
10. Click on the OK button.
11. Click on the minimize button to keep the Communications Manager running in the background.
12. Move to the next PC with the Communications Manager where you are re-tagging the ACU(s).
13. Repeat steps 2 to 7 to open and log on to the Communications Manager.
14. From the Communications Manager transaction window, click on the File menu, and select Display ACU Polling List.
15. The untagged ACUs are listed in the Site/Panel Polling Setup form. Select the ACU(s) that you are re-tagging by clicking in the box to the left. Selected ACUs have a check mark ✓ in the box.

Note

If you do not see the ACU(s) that were untagged in step 9, verify the system user account that you logged on with has been set correctly to view the necessary sites.

16. Click on the OK button.
17. Click on the minimize button to keep the Communications Manager running in the background.

Add a New Panel with Multiple Communications Managers

When you add new ACUs, each new panel must be tagged to a specific Communications


Manager. This involves entering the ACU information in the Client software, then tagging the panels at the designated PC with the Communications Manager, and then uploading the panel(s) from the Keyscan Client software again. Ensure that your user account has the necessary permissions to edit and view the appropriate sites and update the database.

Note

Before beginning, 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 KEYSCAN.

Steps to Add a New Panel with Multiple Communications Managers

1. Go to a PC with the Keyscan Client software module.
2. From the PC with the Client software:
 - If the Client is minimized, click on the Keyscan Management System... button in the status bar at the bottom of the screen, and double click on the User ID box in the status bar in the lower left corner of the Client module window.
 - If the Client is operating, double click on User ID in the status bar in the lower left corner of the Client module window.
 - If the Client is closed, select the Start button in the lower left corner and select All Programs > Keyscan System V Software > Keyscan System V – Client Software.
3. From the Log On box, if appropriate, click on the – English, Français, or Español button to change the program interface to your preferred language.
4. Click on the down arrow to the right of the Site Name text box, and, from the drop down list, select the name of the site that you are adding ACU(s).
5. Enter your User Name in the text box to the right.
6. Enter your Password in the text box to the right. Passwords are case sensitive.
7. Click on the OK button.
8. From the Client module, select the System Settings menu > Site Setup.
9. From the Site Search Information form, in the yellow table, double click on the site name where the ACU(s) were added.
10. From the Site Information form, click on the Panel Setup button.
11. Enter the corresponding information into the following four fields:
 - Unit ID – Enter a unique Unit ID that distinguishes the ACU from other ACU panels at the site. The maximum is 6 alphanumeric characters.
 - Serial # - Enter the unit serial number which starts with an alpha character, followed by 4 numeric characters.
 - Unit Password (For a remote site setup, it is recommended to change the password from KEYSCAN; for a host site setup, it is recommended to retain the default password KEYSCAN.)
 - Unit Type - Use the down arrow to select the correct model.

12. Select the Active radio button in the upper right corner of the form, if it is not selected.
13. Click the down arrow on the right side of the Communication Setup field and select the appropriate option for your system and enter the necessary settings:
 - For a Serial Connection – Specify the Baud Rate and Communication Port.
 - For a Network Connection – Specify the IP Address and Subnet Mask. See Appendix B to program the MSS – COMM, if applicable.
 - For a Dial Up Connection – Specify the Auto Dial Telephone Number, the number the host site dials to connect with a remote site, Baud Rate, Communication Port, and Initializing String, if necessary.
14. If the access control unit has a host number to contact other than that specified on the Site Information form, enter the number in the Host Telephone Number text box, otherwise leave this field blank. This number on the Site Unit Setup form overrides that specified on the Site Information form.
15. In the Unit Location Description, enter a brief caption to indicate the ACU's physical location.
16. Click the down arrow on the right side of Geographical Time Zone Setting and select the site's correct time zone from the drop down list.
17. Select the Add Unit button.
18. If you are entering more than one unit, repeat steps 11 to 17, or if you have finished adding ACUs, select the Save & Exit button to return to the Site Information form.
19. Select the Save & Exit button to return to the Site Information Search form.
20. Select the Exit button to return to the Client main screen.
21. Minimize the Client. You will have to return to upload the data to the panel(s).
22. Go to the PC with the Communications Manager where you are tagging the ACU(s).
23. Double click on the Communications Manager icon  in the lower right corner of the screen if it is running in minimized state, or select the Start button in the lower left corner and select All Programs > Keyscan System V Software > Keyscan System V – Communications Manager.
24. From the Log On box, if appropriate, click on the – English, Français, or Español button to change the program interface to your preferred language.
25. Click on the down arrow to the right of the Site Name text box and from the drop down list select the name of the site.
26. Enter your User Name in the text box to the right.
27. Enter your Password in the text box to the right. Passwords are case sensitive.
28. Click on the OK button.
29. Click on the File menu, and select Display ACU Polling List.

30. From the Site/Panel Polling Setup form, select the ACU(s) that the Communications Manager is to poll by clicking in the box to the left. Selected ACUs have a check mark ✓ in the box.
31. Click on the OK button.
32. Click on the minimize button to keep the Communications Manager running in the background.
33. If more ACUs require tagging at different Communications Manager, re-locate to the next PC with a Communications Manager and repeat steps 22 to 32 until all ACUs have been tagged to Communications Managers. As each Site Panel Setup form is opened, only untagged ACUs are listed.
34. Go back to the PC with the Client.
35. From the Client main screen, select the Update Changes quick button.
36. From the Panel Updates form, 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.
37. From the Upload Type window, select the appropriate items to be updated. 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.
38. Select the Upload button. Wait for the message in the black box indicating the access control panels have been updated.
39. Select the Exit button.
40. Close, minimize, or leave the Client running whichever mode is warranted.

Appendix A

Terminology

Term	Definition
Access Control Unit (ACU)	The ACU works like a mini computer sending and receiving data from the Keyscan software, security cards, card readers, and keypads.
Alarm List	Indicates alarms pending and alarms on hold, providing you with alarm descriptions, locations and times — the oldest listed first.
Archived Card/Cardholder	The card/card holder record remains in the database, however, the card assigned to that card holder is de-activated. The system denies the card holder entry to any doors or elevators controlled by access and elevator control units while Archived Card Holder is in effect.
Archived System User	The system user account remains in the database, however, the individual's account is de-activated and he or she cannot log on, until the account is re-activated.
Baud Rate	The speed that a device sends and receives data.
CCTV	Closed Circuit Television
Card (Security Card)	A card is coded with a specific access number. To enter or exit doors, cardholders present their cards to a card reader near the door.
Card Holder	An individual assigned a card and associated to a door and / or elevator group.
Card Reader (Reader)	A Card Reader is usually mounted beside a door. The cardholder presents his card to the reader in order to enter or exit.
COM Port	A communications port found at the back of a computer terminal.
Door Group	A collective grouping of card holders based on a common association and assigned access levels to doors. (Examples of door groups - Sales Department, Finance Department etc.)
Elevator Group	A collective grouping of card holders based on a common association and assigned access levels to elevators. (Examples of elevator groups - Sales Department, Finance Department etc.)
Function Keys	Function keys are located on your keyboard and include the F keys (F1 through F12), arrow keys, tab, and space bar.

Keypad	A keypad, usually mounted beside a door, is used in conjunction with a card reader. Cardholders key in their PIN number, a personal five-digit code, to enter or exit and then present their cards to a card reader.
Master Login Account	A system user designated with Master Login Account privileges has the authority to create new sites, delete sites, and add users to any site.
Modem	Short for modulator/demodulator, your modem connects your computer to a standard phone line allowing you to send and receive data.
Panel	Access control units are sometimes referred to as panels. See Access Control Unit.
Password	A personal access code keyed into the computer. A password is a software security feature that enables you to gain access to certain applications. Passwords are case sensitive.
PIN	PIN is an acronym for Personal Identification Number. A PIN is a five-digit code entered into a keypad by a cardholder.
Pulse	When a door is pulsed, the software simulates a valid card read at the door. The door 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.
Schedule	A schedule, which resides within a time zone, is a user-defined period of time. See Time Zone.
Site	Site refers to a building or location that is monitored by the Keyscan system.
System Administrator	A system user designated with System Administrator status can display/clear/delete system log events, display/search/print personal identification numbers (PIN), reset user passwords, and add a system user to the current site.
System User	An individual authorized to have access to the Keyscan management software to perform administration tasks to maintain the access control system and database. See Master Login Account and System Administrator.
Time Zone	A time zone is a user-defined period of time that allows or denies cardholders access, locks and unlocks doors, elevators, or outputs, or arms and disarms inputs or supervised inputs.
USB Port	Universal Serial Bus port is used to communicate with a peripheral device connected to the computer terminal.

Appendix B

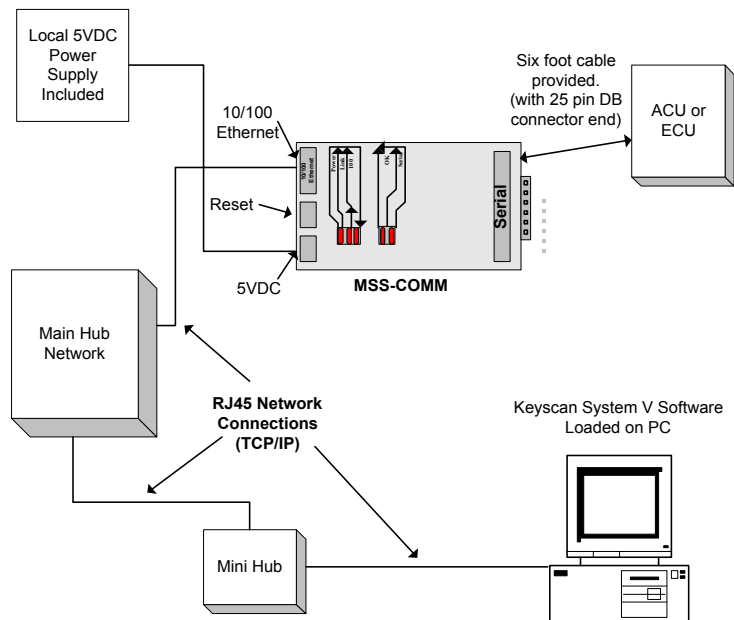
Program MSS-COMM

If a MSS-COMM is used within a LAN, it has to be programmed. The subsections in Appendix B only apply to a Local Area Network. The following block diagrams will assist with addressing connection issues. The step by step programming instructions, which follow the block diagrams, are divided into two segments — Ethernet and Serial Console.

Note

All MSS-COMM units have a reset button located on the rear side near the power connector. When the reset button is pressed and held during the power up, the MSS-COMM returns to its factory default configuration. Release the reset button once the unit is powered. This process may take up to two minutes. We recommend that all units be factory defaulted prior to the programming procedures.

MSS-COMM – Remote Server connected to ACU

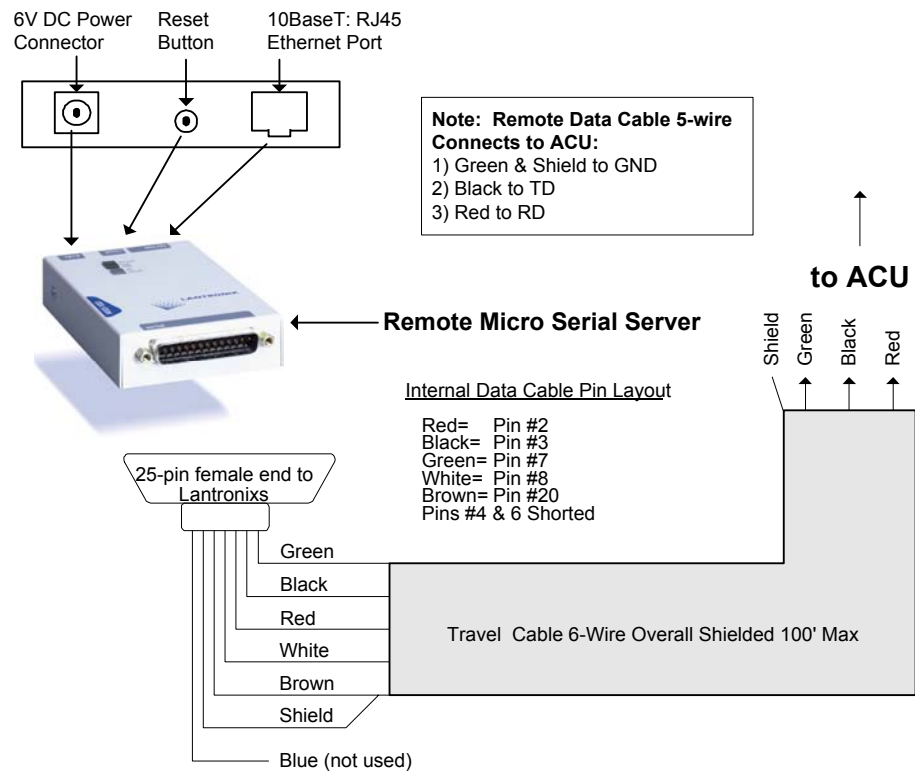


Note: Above Ethernet Network using TCP/IP using 10 or 100 Base -T.

Remote programming notes for set up

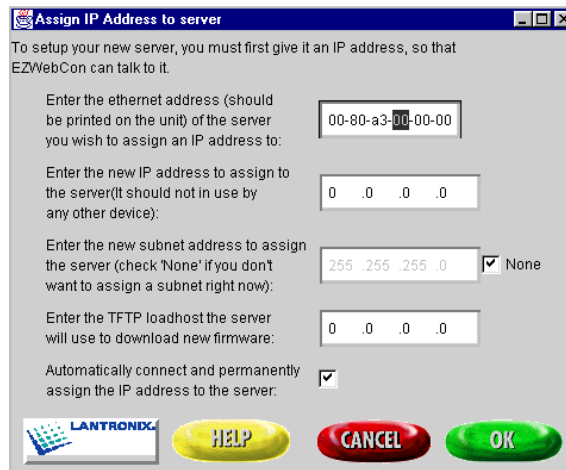
- Remote Part # MSS-COMM
- Program with IP address
- Program as Access as 'Remote'
- Program Subnet Mask
- Program Flow Control = None
- Program Gateway IP if on WAN

Server Serial Connections

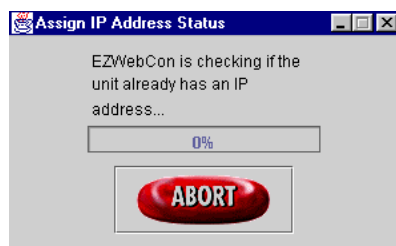


Ethernet (LAN only)

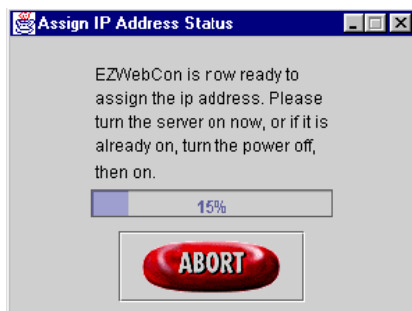
1. Insert the Lantronix CD into the CD ROM drive to install the EZWebCon software. Autorun loads the Launch.exe file. If Autorun does not load the file, select the Start button > Run > Launch.exe.
2. When the installation is completed, click on the Start button > Programs > EZWebCon > EZWebcon.
3. From the EZWebCon main screen, select the Action menu > Assign IP Address to Server.



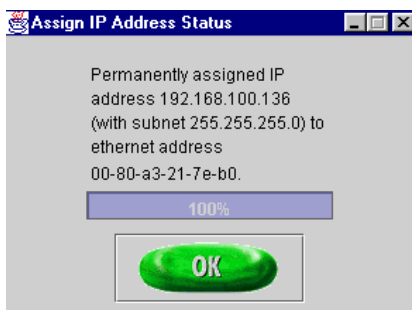
4. Enter the Ethernet address. It is located underneath the unit.
5. Enter the IP address assigned to the unit.
6. Enter a Subnet address to assign the server. Generally, it is set as None.
7. Skip TFTP, no entries are required.
8. Click in the box to the right of *Automatically connect and permanently assign the IP address to the server* to activate this field.
9. Click on the OK button. This initializes the device.



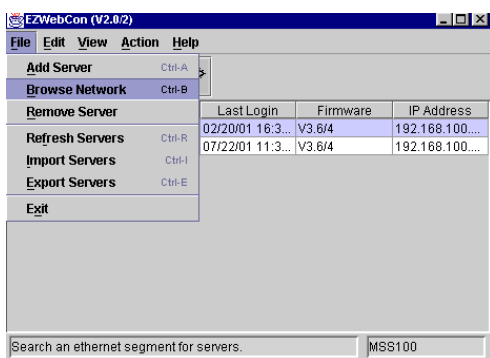
- A message box will come up, and you will have to unplug & re-plug power back to the unit to configure. If your Ethernet address is incorrect or your Ethernet connection has a problem, the Assign IP Address Status dialog box stalls at 15%. Recheck the setting and connection.



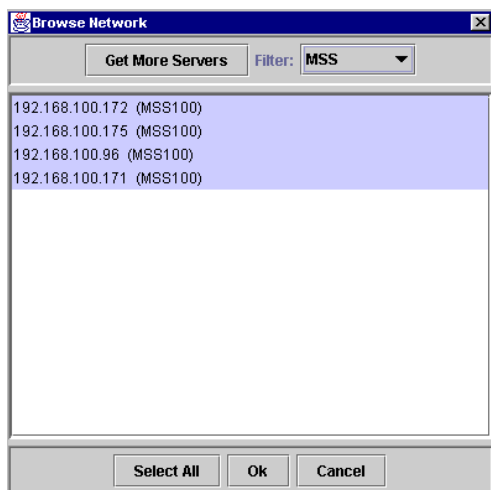
- If you have entered the right Ethernet address and your Ethernet communication is properly connected, the screen will advance from 15% to 100%.



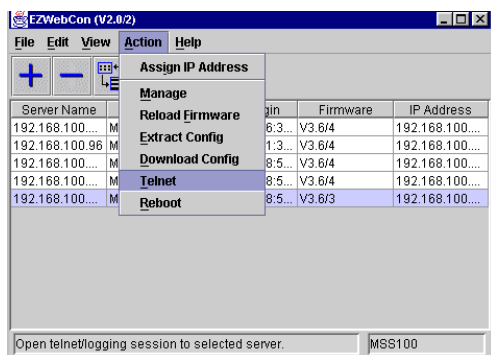
10. Click on the OK button to complete assigning the IP address.
11. Select the File menu > Exit to close the EZWebCon program.
12. From the EZWebCon main screen select the File menu > Browse Network to add a server to the main window on screen.



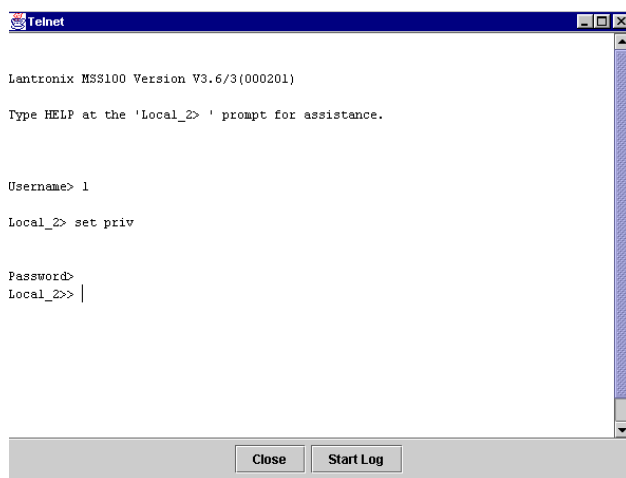
13. Click on the Select All button.



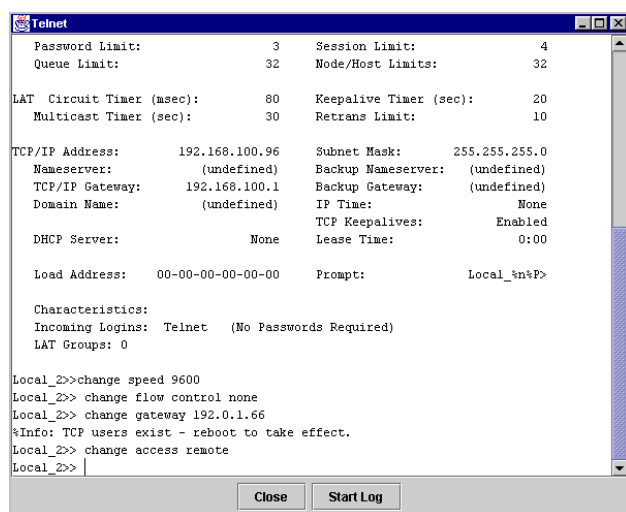
14. Click on the OK button.
15. Highlight one of your server units on the screen, then select the Action menu > Telnet.



16. At Username> type 1 and press Enter on the keyboard.
17. At Local_2>type SET PRIV and press Enter on the keyboard.
18. At Password> type SYSTEM and press Enter on the keyboard. The Password is not displayed.

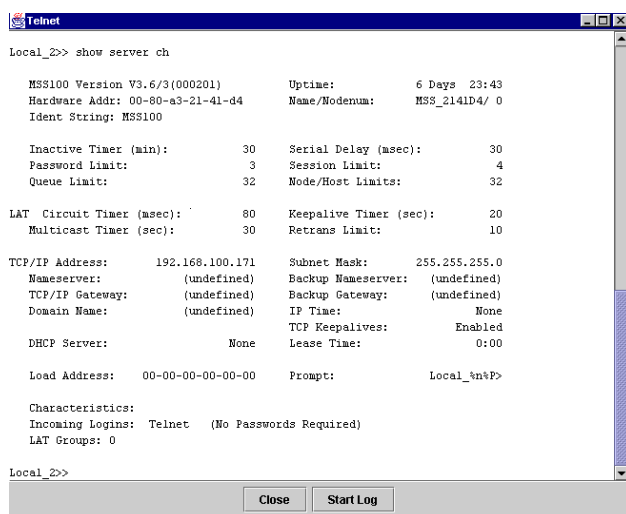


- If the password was entered correctly, you will get a prompt with two >>. For example, Local_2>>.
19. At the Local_2>> prompt, type CHANGE SPEED 9600 and press Enter.
 20. At the Local_2>> prompt, type CHANGE FLOW CONTROL NONE and press Enter.
 21. At the Local_2>> prompt, type CHANGE DHCP DISABLED and press Enter
 22. At the Local_2>> prompt, type CHANGE NETWARE DISABLED and press Enter.
 - If connected to a wide area network (WAN), you will require a Gateway. TCP/IP networks require gateways to transfer network traffic to hosts on other networks. For local area networks (LAN), gateways are not required. Contact your network administrator or IT department to gather your GATEWAY IP address.
 23. At the Local_2>> prompt, type CHANGE GATEWAY XXX.XXX.XXX.XXX and press Enter.
 24. At the Local_2>> prompt, type CHANGE ACCESS REMOTE and press Enter.



- SHOW SERVER CHARACTERISTICS will display any configured gateways.

25. At the Local_2>> prompt, type SHOW SERVER CHARACTERISTICS (or SHOW SERVER CH) and press Enter. This command will display your configured IP, gateways, and Subnet mask.



```

Telnet
Local_2>> show server ch

MSS100 Version V3.6/3(000201)      Uptime:      6 Days 23:43
Hardware Addr: 00-80-a3-21-41-d4   Name/Modenum: MSS_2141D4/ 0
Ident String: MSS100

Inactive Timer (min):      30      Serial Delay (msec):      30
Password Limit:      3      Session Limit:      4
Queue Limit:      32      Node/Host Limits:      32

LAT  Circuit Timer (msec):      80      Keepalive Timer (sec):      20
Multicast Timer (sec):      30      Retrans Limit:      10

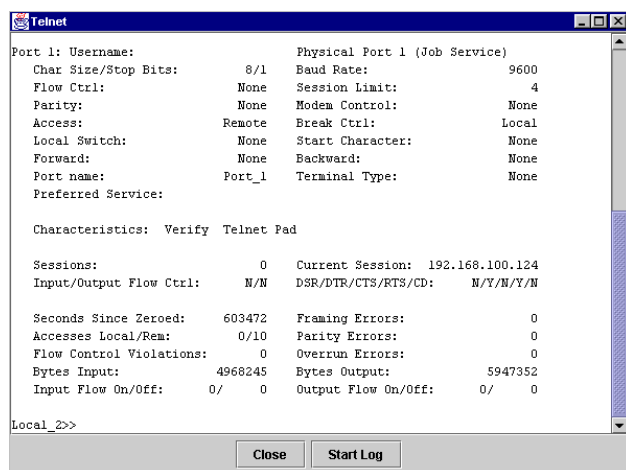
TCP/IP Address:      192.168.100.171      Subnet Mask:      255.255.255.0
Nameserver:      (undefined)      Backup Nameserver:      (undefined)
TCP/IP Gateway:      (undefined)      Backup Gateway:      (undefined)
Domain Name:      (undefined)      IP Time:      None
DHCP Server:      None      TCP Keepalives:      Enabled
Lease Time:      0:00

Load Address:      00-00-00-00-00-00      Prompt:      Local_>>P>

Characteristics:
Incoming Logins: Telnet  (No Passwords Required)
LAT Groups: 0

Local_2>>
  
```

26. At the Local_2>> prompt, type SHOW PORT to display all remaining parameters entered.



```

Telnet
Local_2>> show port

Port 1: Username:      Physical Port 1 (Job Service)
Char Size/Stop Bits:      8/1      Baud Rate:      9600
Flow Ctrl:      None      Session Limit:      4
Parity:      None      Modem Control:      None
Access:      Remote      Break Ctrl:      Local
Local Switch:      None      Start Character:      None
Forward:      None      Backward:      None
Port name:      Port_1      Terminal Type:      None
Preferred Service:

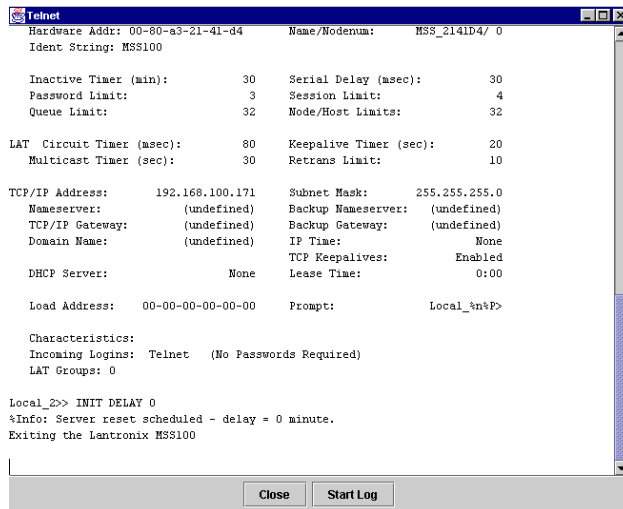
Characteristics: Verify Telnet Pad

Sessions:      0      Current Session: 192.168.100.124
Input/Output Flow Ctrl:      N/N      DSR/DTR/CTS/RTS/CD:      N/Y/N/Y/N

Seconds Since Zeroed:      603472      Framing Errors:      0
Accesses Local/Rem:      0/10      Parity Errors:      0
Flow Control Violations:      0      Overrun Errors:      0
Bytes Input:      4968245      Bytes Output:      5947352
Input Flow On/Off:      0/ 0      Output Flow On/Off:      0/ 0

Local_2>>
  
```

27. If all settings are correct, then at the Local_2>> prompt, type INIT DELAY 0 to initialize the device and close the session.



Serial Console

If you are using a serial console to program the MSS-COMM for Keyscan System V, use the following settings:

- Baud Rate – 9600
 - Bits – 8
 - Parity – None
 - Stop Bit – 1
 - Flow Control – No
1. While pressing the reset switch on the back of the MSS-COMM, apply power to the unit.
 2. Once power has been applied, release the reset switch. During initialization of the factory default settings, the following will be displayed on the monitor. This process may take up to two minutes.

Lantronix MSS100 Initialization...

Ethernet Address: 00-80-a3-52-57-7a Internet Address (Acquiring)

Flash Rom Version V1.6 (Sep 01, 2000)

Flash Version: V3.6/4(000712)

Current Diagnostics report:

NVR Config: Normal Ram Size: 4 MB

ARM ASIC Version: 1

Errors: Network

No network was detected. Press a key within

10 seconds to access bootmode commands>

Request DHCP: no valid reply received.

Request BOOTP: no valid reply received.


```

Request RARP:  no valid reply received.

Checking 4 sections from flash:

From address 0x44001c to 0x20000, 482933 bytes) -> decompressed.

From address 0x4b5ea6 to 0xcb7f4, 72 bytes) -> copied.

From address 0x4b5f02 to 0xcb83c, 74402 bytes) -> decompressed.

From address 0x4c81b8 to 0xebde0, 13165 bytes) -> decompressed.

Loaded 858968 bytes.

Load Completed - Boot in Progress

%% Lantronix MSS100

%% Ethernet Address: 00-80-a3-52-57-7a   Internet      Address
(undefine)

Lantronix MSS100 Version V3.6/4(000712)

Type HELP at the 'Local_1>' prompt for assistance.

```

3. Press Enter on the keyboard.

4. Program the following settings:

```

Local_1> set priv
Password> system

Local_1>> change ipaddress 192.168.100.96
Local_1>> change subnet mask 255.255.255.0
Local_1>> change gateway 192.168.100.1
Local_1>> change flow control none
Local_1>> change access remote
Local_1>> change netware disabled

```

5. Review your entries to the settings shown below:

Local_1>> **show port**

Port 1: Username: Port_	1	Physical Port 1 (Local Mode)	
Char Size/Stop Bits	8/1	Baud Rate	9600
Flow Ctrl:	None	Session Limit	4
Parity:	None	Modem Control	None
Access:	Remote	Break Ctrl	Local
Local Switch:	None	Start Character:	None
Forward:	None	Backward:	None
Port name:	Port_1	Terminal Type:	None
Preferred Service:			

Characteristics:	Verify	Privs	Telnet Pad
Sessions:	0	Current Session:	None
Input/Output Flow Ctrl Y/Y/Y/Y/N	N/N	DSR/DTR/CTS/RTS/CD:	
Seconds Since Zeroed:	1770	Framing Errors:	0
Accesses Local/Rem:	1/0	Parity Errors:	0
Flow Control Violations:	0	Overrun Errors:	0
Bytes Input:	0	Bytes Output:	0
Input Flow On/Off:	0/ 0	Output Flow On/Off:	0/ 0

Local_1>> **show server ch**

MSS100 Version V3.6/4(000712)	Uptime:	0:29:44
Hardware Addr: 00-80-a3-52-57-7a	Name/Nodenum:	MSS_52577A/ 0
Ident String: MSS100		
Inactive Timer (min):	30	Serial Delay (msec): 30
Password Limit:	3	Session Limit: 4
Queue Limit:	32	Node/Host Limits: 32
LAT Circuit Timer (msec)	80	Keepalive Timer (sec): 20
Multicast Timer (sec):	30	Retrans Limit: 10
TCP/IP Address: 192.168.100.96	Subnet Mask	255.255.255.0
Nameserver:(undefined)	Backup Nameserver:	(undefined)
TCP/IP Gateway: 192.168.100.1	Backup Gateway: (undefined)	
Domain Name: (undefined)	IP Time:	None
	TCP Keepalives:	Enabled
DHCP Server:	None	Lease Time: 0:00
Load Address: 00-00-00-00-00-00	Prompt:	Local_%n%P>
Characteristics:		
Incoming Logins: Telnet (No Passwords Required)		
LAT Groups: 0		

Appendix C

Setup a CCTV System

The Keyscan Management System V CCTV system interface is designed principally for alarm monitoring, whereby, when designated alarm events are triggered, specified cameras can be set to capture still images or a designated addressee receives an E-mail notification. Also, using the Show Live Video function, you can view live video feeds with multiple cameras, pan, and zoom commands. The CCTV and Video control is optional and may not be included in your Keyscan software package.

Depending on your specific configuration, before you begin to setup your CCTV system in the Keyscan V software, you must first install any video related software drivers for devices such as a video bus or video capture board. You may require the camera or switcher manufacturer's literature for command and communications settings.

The procedures to setup a CCTV system require completing the following three forms and testing the settings on a fourth form.

- CCTV Type Setup form – identify switcher/matrix manufacturer and set camera commands
- CCTV Command Setup form – set communications
- CCTV Action Setup and E-mail Notification form/CCTV Setup – program cameras to alarm events
- Show Live Video – verify camera settings

CCTV Type Setup Form

This form is used to identify the CCTV switcher/matrix and list camera commands.

To Complete the CCTV Setup Form

From the Keyscan System V Client's main screen, select System Settings > CCTV Setup.



1. Click on the CCTV Type Setup tab.



2. Click on the Add New CCTV Type button.
3. In the CCTV Type text box, enter the name of the switcher/matrix manufacturer.
4. Click on the Save button.
5. Under Settings is a list of Display Camera #s from 1 to 16. Double click on Display Camera #1. This assumes you are entering the first camera.
6. 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/matrix manufacturer's literature. This assumes that you have connected Display Camera #1 into port #1 on your switcher.
7. Click on the Save button.
8. To add another camera or set display, pan, and zoom modes, repeat steps 5 to 7.

CCTV Type Setup form

Settings	Settings Commands
Display Camera # 1	BC1
Display Camera # 2	BC2
Display Camera # 3	BC3
Display Camera # 4	BC4
Display Camera # 5	
Display Camera # 6	
Display Camera # 7	
Display Camera # 8	
Display Camera # 9	
Display Camera # 10	
Display Camera # 11	
Display Camera # 12	
Display Camera # 13	
Display Camera # 14	
Display Camera # 15	
Display Camera # 16	
Display Mode: Full Screen	DM 0,1,2,3,4,0
Display Mode: 2 x 2	
Display Mode: 3 x 3	
Display Mode: 4 x 4	
Zoom Mode	BZ
Zoom Mode: Left	ML

Export/Import CCTV Commands

For dealers, where you will install CCTV with the same camera commands repeatedly, use the Export CCTV Command to save the camera settings on a transportable medium such as a floppy disk or writable CD. When you export the CCTV commands, the file is saved in CSV file format. For subsequent CCTV installations with the same camera settings, use the Import CCTV Commands button to then load the CSV file to save time and eliminate needlessly re-entering the same camera commands.

CCTV Command Setup

After you have completed the CCTV Type Setup form, complete the CCTV Command Setup form to specify communications. Be sure that you select the right port # in the CCTV Port field. After you complete the CCTV Command Setup form, we recommend that you test your camera(s) to be sure the interface settings are correct before you complete the CCTV Action Setup and Email Notification form. See Show Live Video on page 153.

To complete the CCTV Command Setup Form

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 Driver Options 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. At this stage you may wish to verify that your cameras are connected and programmed correctly. You can test you cameras by opening the Show Live Video option outlined on page 153. If you elect to do this, click on the Exit button to return to the main screen.

CCTV Command Setup formA screenshot of the 'CCTV Setup' window with the 'CCTV Command Setup' tab active. The form contains several fields and buttons: 'Site Name' (text box with 'ABC Corporation'), 'CCTV Type' (dropdown menu), 'CCTV Port' (dropdown menu), 'Driver Options' (dropdown menu), 'CCTV Baud Rate' (dropdown menu), 'CCTV Parity' (dropdown menu), 'CCTV Data Bits' (dropdown menu), 'CCTV Bits' (dropdown menu), a 'Save Default Setup' button, and an 'Exit' button at the bottom right.**CCTV Action Setup and E-mail Notification**

The CCTV Action Setup and E-mail Notification form is used for setting your CCTV cameras to capture still images for specified alarm conditions or Email an alarm message to another address.

Note

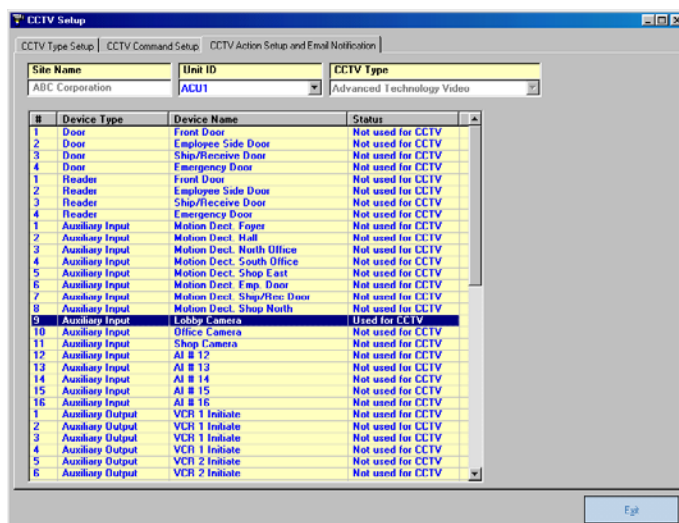
The Keyscan Management System V Email notification function is only compatible with MS Outlook (MAPI Client). It cannot transmit with any other electronic mail software. There are no compatibility restrictions on the receiving electronic mail software.

To Set Cameras for Alarm Conditions

1. Click on the CCTV Action Setup and E-mail Notification tab.



2. From the CCTV Action Setup and E-mail Notification form, click on the down arrow on the right side of Unit ID field, and select the ACU model from the drop down list.



3. From the yellow window under # | Device Type | Device Name | Status, double click on the appropriate input assignment number that correlates to the camera to open the CCTV Setup form.
4. Click on the down arrow on the right side of CCTV Command To Apply field and select the camera # from the drop down list. If you did not enter command codes for cameras, the drop down list will be blank.
5. If you want still images captured after an alarm condition is triggered, enable the Save Still Picture option by clicking in the box to the left.
6. If the Save Still Picture option was enabled, enter a value in the # of Pictures text box to instruct the system how many images to capture.
7. In the Start After text box, enter a value to activate the camera after the alarm event started. A value of 0 would trigger the camera to save a still image immediately after the alarm condition. Units of time are in minutes.
8. In the Interval Between Pictures text box, enter a value that specifies the intermittent time between image captures. Units of time are in minutes.

9. If more than one camera or camera action is to be programmed to an alarm condition, repeat steps 4 to 8 to set the next camera or camera action.
 - The sliding Delay tab, located under the CCTV Command To Apply field, staggers camera initiation time after its assigned alarm event starts. Click and drag the tab along the bar to set the delay time. As you drag the tab, the time is displayed in a yellow box. Units of time are in minutes.
10. In the lower left corner of the CCTV Settings form is a scrollable list of alarm conditions. Click in the box to the left to select the alarm condition(s) to initiate the camera(s) and or Email notification. You can select multiple alarm conditions, however, it is strongly recommended you limit your selections so as not to overburden system resources.
11. In the Email Address text box, enter an Email address to notify the addressee of the alarm event. The Email includes code descriptions as they are listed in the Alarm Event window on the main screen. Keyscan Management System V is only compatible with MS Outlook (MAPI Client).
12. Select the Update CCTV Settings button.
13. Select the Exit button to return to the main screen.

Note

By default, the still images that are captured during an alarm event are saved in the Keyscan Client directory as JPEG files.

CCTV Setup form

Show Live Video

The Show Live Video function will confirm that your settings are correct by displaying a live video feed to the screen.

To Confirm the Interface Connections to the CCTV System

From the Keyscan System V Client's main screen, click on the Show Live Video quick button.



Show Live Video

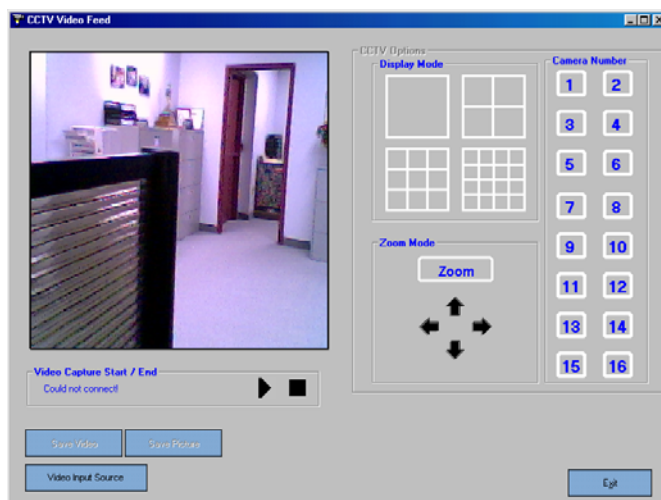
1. Depending on the CCTV configuration, if there are multiple cameras in the system, select the buttons in the Camera Number panel to view the video feed from each camera. Button numbers correspond to the display camera number assigned in the CCTV Setup form. If there is only a single camera, the Camera Number and Display Mode functions will be disabled.
2. If you programmed Display Modes for multiple cameras or Zoom Modes, use the function icons in the CCTV Options panel to test if they operate. If you do not have live video, check all the video hardware connections and the camera setting commands.
3. If you set the CCTV Action Setup and E-mail Notification form to capture still images, try setting an alarm, such as Door Held Open which must be a selected alarm event on the CCTV Settings form, to verify still images were captured.

Note

The still images are stored in either the Client directory on the PC where the CCTV interface was setup or the Card Holder Folder Location directory, if you specified one in the Site Information form, as JPEG files with the following name format: Alarm # - Year/Month/Day/Hour/Minute/Second.jpeg.

4. To return to the main screen, click on the Exit button after you have confirmed that all the cameras are connected with the system and operating as they have been programmed.

CCTV Video Feed form



Appendix D

Alarm Listings

Alarm Type	Device Type
Alarm Tripped	Door – a monitored door was accessed without a valid card presentation (forced open) Auxiliary Input – a monitored auxiliary input point was tripped
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 was now been cleared
Door Held Open	Door – a door was accessed with a valid card but was not closed within the designated Door Held Open Time setting
Door Closed	Door - a door previously in violation of the Door Held Open Time setting has now been closed
Comms Failure	ACU Model Type – an access control unit has lost communication with the access control software
Unit Marked Inactive	ACU Model Type – an access control unit that lost communication has now been marked inactive by the access control system
Comms Restored	ACU Model Type– an access control unit, previously marked as Unit Inactive, has had communications restored and is now active
Power Fail Detect	Input – an access control unit has lost power

For more information on Alarms, refer to Operating the System in the on-line help in the Keyscan Client module software.

Index

A

access levels · 58, 76
activity collection · 33
adding cards · 84
additional card holder information · 88
alarm graphic locations · 61
alarm response instructions · 61
anti-passback · 40
assign elevator floors group access levels · 76
assign elevators to elevator banks · 68
assign specific floor buttons to automatically unlock · 74
assign time zones to auxiliary inputs · 54
assign time zones to auxiliary outputs · 53
assign time zones to doors · 51
assign time zones to readers/keypads · 56
assign time zones to supervised inputs · 55
assigning outputs to auxiliary/supervised inputs · 50

B

backup database · 97
batch number · 84
bitmap · 62
building schematics · 61

C

capture image · 87
capture photos · 86
capture still images · 151
card holder · 84
Card Holder Photo Location · 32
card number · 84
card technologies · 4
CCTV system · 149
Client module · 7
communication problems · 103
communication setup · 35
Communications Manager
 auto start · 128
 log on procedures · 127
 multiple · 130
 multiple, add new ACU · 134
 overview · 125
 re-assign ACUs · 132
 reset auto start · 129

 user account · 127
Communications Manager module · 7
converting and integrating a database · 20
copy DB files to data folder method · 115
CSV files · 101

D

daylight savings · 82
default site · 33
dial up connection · 35
door group access levels · 58
door group name · 38
door held open time · 40
door operation mode · 40, 42
door output · 40
door relay unlock time · 40
door time zones · 44

E

elevator access modes · 74
elevator bank names · 65
elevator button hold time · 67
elevator controllers · 63
elevator group names · 63
Email an alarm message · 151
exporting card holder records · 101
EZWebcon · 141

F

first person in · 47, 51
floor plans · 61

G

general card holder information · 84
geographical time zone · 35

H

HID reader/keypad · 56
holiday calendar date · 80
holiday time zone · 79

I

identify the CCTV switcher · 149
Indala reader/keypad · 56
insert existing image · 86

L

Lantronix · 141

M

MSDE Database Engine · 7
MSS-COMM
 programming · 139
Multiple Communications Managers
 installing · 14

N

name elevator floors · 69
network connection · 35
no collection · 33
Norton Anti-Virus · 10

O

online help · 5
optimum system performance
 network · 9
 single PC · 8
optional card holder information · 89

P

panel recovery method · 120
Photo Badge Template Editor module · 7

R

reader / keypad setup modes · 56
reader information · 40
Reader Port · 40
reader problems · 109
re-establish card holder · 118
re-establish card holder photos · 113
restore DB backup method · 111

S

schedules · 46, 72
search door groups · 38
serial connection · 35
set auxiliary output names & set auxiliary output
 status · 49
set elevator banks to time zones · 71
setting up doors · 38
show live video · 153
signature capture · 89
site contacts · 36
Site ID
 purpose · 33
site information · 33
Site Information form · 32
Site Setup Report · 100
Site Setup Wizard · 25
site unit setup · 34
system requirements · 8
system user · 91

T

temporary card · 85
test the card · 109

U

upload access control units · 99
user authority levels · 91