R A D I O N I C S

READYKEY® K6100 Readykey for Windows™

System Programming Manual

17244 Ver. 5.0
74-07604-000-C 01/99

Notice

The material and instructions in this manual have been carefully checked for accuracy and are presumed to be reliable. However, Radionics, Inc. assumes no responsibility for inaccuracies and reserves the right to modify and revise this manual without notice.

It is our goal at Radionics to always supply accurate and reliable documentation. If a discrepancy is found in this documentation, please mail a photocopy of the corrected material to:

Radionics, Inc.
Technical Writing Department
1800 Abbott Street
Salinas, California 93901

Radionics is a division of Detection Systems, Inc.

UL Listings

UL 294 - Access Control System Units
UL 1076 - Proprietary Burglar Alarm Systems

Trademarks

Windows™ and Windows NT™ are trademarks of Microsoft Corporation
Microsoft® and MS-DOS® are registered trademarks of Microsoft Corporation

Novell™ and Netware™ are registered trademarks of Novell, Inc.

Loronix® and Image*Share*® and registered trademarks of Loronix Information Systems Inc.

The Radionics logo is a registered trademark of Radionics, a division of Detection Systems, Inc.

Table of Contents

Introduction

About this document

This document describes how to configure a Readykey for Windows system. It includes details of all the necessary steps to set up the database and configure the Readykey hardware for operation with Readykey for Windows, and should be read by anyone installing or intending to install a Readykey for Windows system.

It is assumed that users are at least familiar with PCs, MS-DOS and Windows. It is beyond the scope of this document to review all the features of these products. However it is recommended that anyone new to Windows uses the Windows Tutorial which can be found in the Help menu of the Windows Program Manager (Windows 3.11) or from the Contents tab of the Help option on the Start menu (Windows 95, Windows 98, and Windows NT4).

This document also assumes that the Readykey for Windows software has been installed on the PC. If this is not the case, then read th*e Readykey for Windows Software Installation Manual)* **first**, for standalone PC installations, or the *Readykey for Windows Multi-PC Installation Manual)* for multi-PC installations.

The *Readykey for Windows System Overview)* describes the concepts behind a Readykey for Windows system, including Divisions, Sites, Masters and Workstations. Use the Overview document to plan your system and determine how it is going to be configured.

The remainder of this document is divided into three sections:

- The first section (Quick Installation) describes configuring a Readykey for Windows system.

The stages covered include starting the Readykey for Windows software and logging in, setting up the Readykey for Windows database, setting up and establishing communications with the door controllers on each site, and finally completing the installation of the Readykey for Windows system. Including programming door information, creating access groups, and adding keys/cards. This section also includes information on how to create system operators; configure door controller relays, alarm event manager inputs and outputs, etc.. References are made to...

- ... the second section, which provides more detailed information on some stages.
- The final section consists of a number of appendices giving troubleshooting information, using non-Readykey ID devices with Readykey for Windows, and upgrading an existing DOS K6000 or K6000-AM system.

Other Documents

The following documents describe other aspects of the system:

Readykey for Windows System Overview

This document should be read by all people who may install, use, or administer any Readykey for Windows system. It gives a general picture of the whole system and introduces features such as Areas, Access Groups, Departments etc. which should be understood before setting up the system.

This document also provides a useful glossary of any terms which may be unusual or specific to Readykey access control systems.

K2100/K1100 Installation Manual

This document describes the installation of the K2100 and K1100 Door Controllers. Also included are details of installing the K2015 Alarm Module, the K2015A Alarm Event Manager and Readykey Readers.

Central Network Controller Installation Manual

This document is supplied with a Central Network Controller (CNC), as used in some Readykey for Windows systems. It covers all aspects of installing the CNC.

Readykey for Windows Software Installation Manual

This describes the installation of the Readykey for Windows software including preparation of the PC for non-networked PC systems.

Readykey for Windows Multi-PC Installation Manual

This describes the setup of multiple PCs to administer a Readykey for Windows system including preparation of the PCs and installing the software.

Readykey for Windows Network Operational Overview and Requirements

This document describes the requirements and relationship of multiple PCs to administer a Readykey for Windows system including preparation of the PCs and installing the software. Readykey for Windows Alarm Graphics Datasheet,
Readykey for Windows ASCII Transaction File Datasheet,
Readykey for Windows Attendance Report Datasheet,
Readykey for Windows DDE Output Datasheet,
Readykey for Windows Alarm Sound Support Datasheet,
Readykey for Windows Serial Interface Module Datasheet,
Readykey for Windows Audit Trail Module Datasheet,
Readykey for Windows Photo ID Module Datasheet,
Readykey for Windows Elevator Control Datasheet

These documents describe the operation of some additional modules and special features available in Readykey for Windows.

Readykey for Windows Programming Record Sheet

This should be completed in conjunction with the information described in this manual and the On-line Help, and are designed to help you program your Readykey for Windows system.

Readykey for Windows User Instructions

This document provides step by step instructions on basic Readykey for Windows tasks, such as logging in, adding and deleting keyholders, manually locking or unlocking doors, accepting alarms, etc.

On-Line Help

One of the major features of Readykey for Windows is the On-Line Help facility. Throughout the Readykey for Windows system help is available by choosing a **Help** button; selecting **Help** from a drop down menu or pressing the **F1** key on the keyboard. When selected you will be presented with a help topic relevant to the operation you are performing. Once help has been selected you will be able to select other relevant topics or search for assistance with a particular function. Topics can be printed if required.

It is intended that the on-line help should be the primary source of information regarding the use and administration of the system.

Terminology

Throughout this manual reference is made to Windows and Readykey for Windows. **Windows™** refers to the *Operating System* produced by Microsoft Corporation, which is now provided as standard with nearly all Personal Computers (PCs). The same term 'Windows' will be used to refer to Microsoft Windows Version 3.1, Windows for Workgroups 3.11, Windows 95, Windows 98, and Windows NT.

Readykey for Windows refers to the *Access Control Administration Software* distributed by Radionics Inc.. designed to operate under the Microsoft Windows operating system.

A glossary of terms used in this and other Readykey for Windows documents is included in the appendix of the *Readykey for Windows System Overview.*

Description of the System

Readykey for Windows is a means of administering an Access Control System consisting of Readykey door controllers and readers. The software is supplied in several versions depending on the requirements of the particular installation. The *Readykey for Windows System Overview* describes the various options/modules available in detail.

Security Block (Dongle)

The Readykey for Windows software will have been supplied with a Security Block, or most commonly known as a Dongle, which connects to the PC. The security block will have been programmed with information regarding the type of Readykey for Windows system purchased.

The number of Sites, Divisions and Workstations you can use on your Readykey for Windows system, are controlled by the security block. Certain extra-feature modules, including Elevator Control, Photo-ID, Serial Interface, Audit Trail, and Attendance Reporting are also controlled - these features are documented separately.

The security block can be easily upgraded by purchasing a password from Radionics Inc. which can then be entered into a special utility within the Readykey for Windows software.

Readykey Hardware Requirements

Readykey for Windows is supplied in a software only form. In order to use your Readykey for Windows system you may also need to purchase at least one Readykey CNC or Readykey PC Interface Kit to communicate with door controllers. However, you may have up to twenty Readykey CNCs or PC Interface Kits communicating with door controllers on a single Readykey for Windows system with multiple workstations, or any combination of the two.

Radionics previously supplied the CNC in two versions - Single Site (SS) and Multi-Site (MS). The two versions were identical in appearance. However, only the MS version could communicate to door controllers via RS-232 and the Six Wire Bus. The SS version could communicate via the Six Wire Bus only. The SS version was discontinued in Spring 1995 - all CNCs now supplied by Radionics are MS. An upgrade for existing SS CNCs can be purchased from Radionics by ordering a K6005-MS CNC Upgrade Kit.

In addition, you may be using a PC Interface Kit with Wiegand Interface if you are using Wiegand compatible ID devices and readers. Appendix B contains the necessary information to set this up in Readykey for Windows.

System Design

If you have not already done so, then use the 'System Design' section in the *Readykey for Windows System Overview* to determine how your system is going to be installed and configured.

To proceed with the installation and configuration of your Readykey for Windows system, you need to have the following information available as a minimum:

Divisions

How many Divisions are going to exist on your system? How do the Divisions relate to the 'real world'? A large proportion of the installation process will need to be repeated for each Division. It is recommended (and assumed) that you commission your system one Division at a time.

Note: A Division is equal to a *Database*. A single Division can control and administer up to 128 sites (locations). Each Readykey for Windows system includes one Division (database) allowed. Additional Divisions may be purchased from Radionics at any time, for the system expansion. Two Divisions may not communicate with the same site (location). Only one Division can control a site. Divisions are normally used for multiple site and multiple customer applications with each division having separate Personnel in each database. When multiple customers are being serviced across multiple sites, it is convenient to separate the keyholders into multiple databases.

Workstations

How many Workstations (PCs) are being used to administer Readykey for Windows? Each Workstation may have a master connected to it, and/or a PC Interface Kit to provide ID device administration at the Workstation.

If you are using Readykey for Windows from more than one Workstation, then you will have defined the additional Workstations during the software installation process, as described in *Readykey for Windows Multi-PC Installation Manual and the Network Operational Overview and Requirements document*. You may need to further configure each Workstation in Readykey for Windows if you are installing PC Interface Kits for ID device administration.

Masters

The door controllers on your system will communicate with Readykey for Windows via a Master. Three types of Master are available - K2100/K1100, Single Site CNC and Multi-Site CNC. How many and which types of Master will exist on your system? To which Workstation will each Master communicate?

Note: A single workstation with enough serial ports can communicate with up to 4 CNCs. Also, there is a speed advantage to having the masters on the Readykey Server PC.

Sites

How many Sites are there in each Division on your system? A single division is capable of up to 128 total sites. How will each site communicate to a Master? Which Master will each Site communicate to?

Note: A Site is a group of door controllers which share a common communication route to the master. When information is sent to a Site all door controllers in the site receive the information. As with Divisions, it is recommended (and assumed throughout this documentation) that you commission each Site individually.

Door Controllers

Each Site on the system will consist of one or more door controllers. These can be of a variety of types - for example: K2100, K1100, K2000-N, etc. In addition, the availability of certain features may be dependent on the version of software installed in each door controller.

How many door controllers are there on each Site? What type are they? Are there any special options which need to be programmed on each door controller, such as lock sharing (two readers, one on either side of a door, controlling the same lock), anti-passback, etc.?

Alarms Event Managers

These connect to door controllers on the reader channels (a reader can also be installed). Which door controllers are you going to install them to? What areas do you want them to cover? How are you going to use the inputs and outputs?

Areas

Each reader on the system will control access (allow/restrict entry) to an Area. Access of keyholders is restricted on a 'per Area' basis. How will each Site be divided into Areas? A total of up to 128 Areas can be created for each site on the system.

Doors

The term 'door' is used to describe a reader on the system. Which readers are wired to each door controller, and in what order? What type of lock is installed? Is it a fail safe style of lock, which is power to lock, most commonly used for configuring a magnetic lock? Or is it a fail secure style of lock, which is power to release, most commonly used for configuring a strike. What lock release time is required? Is any form of door monitoring installed, such as a door contact? To which Area does each reader restrict access?

Access Groups

Access Groups allow you to easily control which personnel can access which Areas, and at what times/days. This section will help you to create an Access Group that allows access to all Areas on a Site at all times.

Divisional Access Groups

If you have more than one Site on your system, then once you have set up the information for each individual Site, you may need to create an Access Group with access to all Areas on each Site, and then combine these into a Divisional Access Group (DAG) that allows access to all Areas on all Sites in a Division. This can then be assigned to keyholders in Personnel, in place of the Access Group, to allow access to all sites. An example may be to consider a president of a corporation who needs to be allowed into all of the locations across multiple facilities.

Note: The Access Group on some Sites may be **None** so that access to that site will be denied.

Personnel

Each keyholder on your system is defined in the **Personnel** application. This is where you give each keyholder a name, program their ID device into Readykey for Windows, and assign their Access Group or Divisional Access Group (DAG). In addition, up to 20 ‘fields’ of extra information can be entered and stored for each keyholder.

Note: Keyholders may also be given extra access to specific areas, in addition to those areas defined through the Access Group and Divisional Access Group.

Quick Installation

Introduction

This section provides a brief step by step guide to setting up your Readykey for Windows system. Further information on each step is included in the Reference Section of this document.

If you have a multi-site system, then it is recommended that you complete commissioning of each Site individually. Similarly, installers of multi-division systems should complete the commissioning of a single Division before moving onto other Divisions. The remainder of this document assumes you follow these recommendations.

When you install the Readykey for Windows software, a 'default database' is installed, which includes one Division, one Workstation, one Site, and one Operator. Additional Workstations will have been created as required during the software installation process for multi-PC systems.

It is assumed that a new Readykey for Windows installation is being performed - if you are upgrading an existing DOS-based K6000 or K6000-AM system, then refer to Appendix C.

Starting Readykey for Windows

1. Make sure the Readykey for Windows software has been installed on the PC, following the instructions detailed in either *Readykey for Windows Software Installation Manual* (for single-PC systems) or, for multi-PC systems *Readykey for Windows Multi-PC Installation Manual and the Network Operational Overview and Requirements document*.

2. The procedure for starting the Readykey for Windows software is different for Windows 3.1/3.11, Windows 95, Windows 98, and Windows NT:4

   a. **Windows 3.1/Windows for Workgroups 3.11**

      Double-click the Readykey for Windows icon from the Windows **Program Manager**.

   b. **Windows 95, Windows 98, or Windows NT**

      Readykey for Windows has been installed in a Readykey for Windows group under **Programs** from the **Start** button on the task bar.

      Note: This manual assumes the PC is running Windows 95/Windows NT. Some descriptions may not apply for Windows 3.1 or Windows 3.11. Once the Readykey for Windows has been started, operation under all versions of Windows is primarily the same. Consult the Windows 3.1 or 3.11 documentation if you require assistance on starting the Readykey for Windows program.

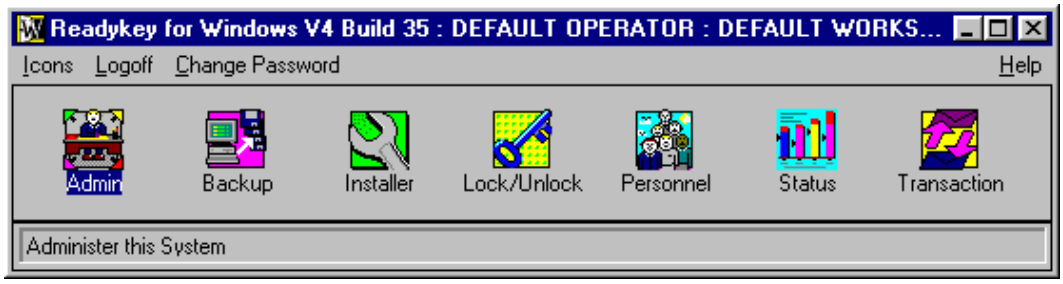
3. As Readykey for Windows starts, the Engine will also start it may be minimized on the task bar or it may appear as an animated icon minimized at the bottom of the screen. The **Alarm** application, **On-line Transaction Display** and **Alarm Graphic Display** may also start after 1-2 minutes has expired - the Alarm and Alarm Graphic Display applications will also be minimized. (The **Alarm** application, **On-line Transaction Display** and **Alarm Graphic Display** will only start if this option was selected when the Readykey for Windows software was installed on the PC.)

   Note: If you receive any messages during the startup process, you should refer to the Reference Section of this manual to find out the meaning of these, and whether they can be ignored at this stage, or whether action should be taken to investigate their meaning and implications.

4. Once Readykey for Windows has started, you will be presented with the **Login** screen - as shown below:

Logging In

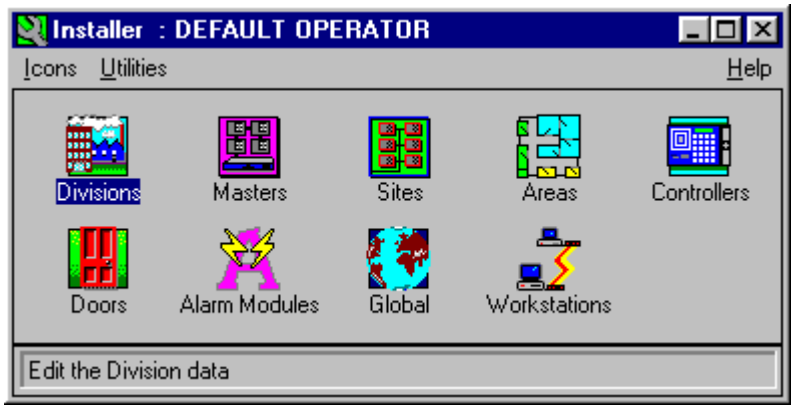
1. As this is a new installation, there is a system operator provided, with full access to the system. This operator (the 'Default Operator'), has the same User name and Password - 'GUEST'. Type the **User name** and **Password** in the correct boxes and choose the **Log in** button.
2. If you have done this correctly, then you should now be logged in to the system. The following screen (the **Login** applications screen) will appear:



Note: The **Alarm** icon will not appear if, during the software installation process, the option was chosen to start **Alarm** automatically with Readykey for Windows.

Installer

The first application to be used will be **Installer**. This allows the Readykey and PC hardware to be defined in the Readykey for Windows system. Start **Installer** by double-clicking on the icon from the **Login** applications screen.

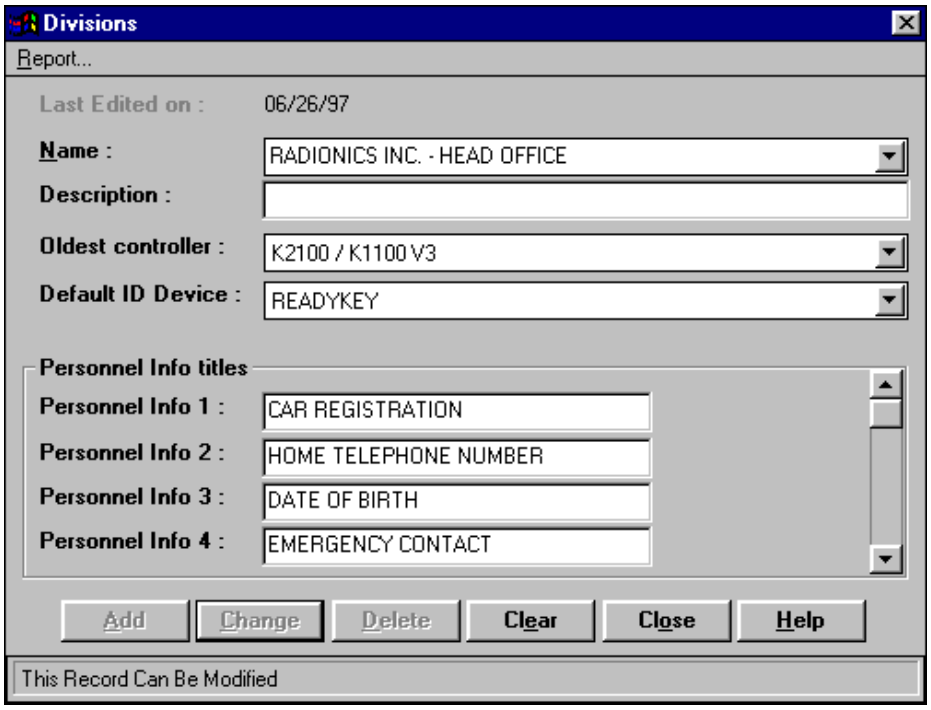


Many Readykey for Windows applications (including **Installer**) consist of a number of sub-applications, each represented by an icon. In **Installer,** as well as the sub-applications, there are a set of 'Utilities', that allow certain special functions to be performed. The next stage of this process will use most of these sub-applications and utilities.

Installer: Divisions

1. The first sub-application to be used will be **Divisions** - even if you are only going to have one division on your system, you still need to set up some information here.

   Start the **Divisions** sub-application from **Installer**.



   There is one division defined as part of the default database. The information programmed should be modified as required.

2. Each division must have a different **Name -** use a meaningful name to make using the system easier.

3. The **Description** is optional, but can be used to give more information about the division.

4. The **Oldest Controller** setting is most important - it affects the quantity and availability of certain features on your system, including:

   a. Number of personnel

   b. Number of Time Profiles / Time Periods

   c. Number of Divisional Access Groups

   d. Availability of Start and End Dates on **ALL** keyholders' access

   e. Availability of Extra Access

   - a table giving further information on these is included in the Reference Section of this document.

   Warning: If you incorrectly set this entry, then you may not be able to program these features or they may not work properly on your system. The default setting on a new installation will be K2100/K1100 V3, which is for all K2100/K1100 door controllers with a software version 3.0 or higher.

   Select the correct **Oldest Controller** setting for the division.

   The default setting is set to K2100/K1100 V3 on a new installation, which means that all door controllers used on the system must be version 3.0 or higher.

5. Readykey for Windows allows a variety of different ID devices to be used on the system. The **Default ID Device** setting determines the 'standard' ID device type that is selected automatically when in the **Personnel** application. If you are using a majority of non-Readykey ID devices in the division, then change the setting accordingly.

   The available settings for the default ID Device are:

   a. Readykey (select for systems using standard Readykey keys and cards)

   b. Sensor 2601 (select for systems using Wiegand 26 Bit readers and ID devices)

   c. Wiegand 2801 (select for systems using Casi Rusco Wiegand 28 Bit format readers and ID devices)

   d. Wiegand 2802 (select for systems using Casi Rusco Wiegand 28 Bit Version 1 format readers and ID devices)

   e. Readykey UK Magstripe Reader (select for systems using the European Readykey Magstripe readers and cards)

   Note: For formats not listed above, use the ID Device type setting of ‘Readykey’ and you must read the ID Devices into the system using the K2012 Wiegand Interface and the corresponding wiegand reader with the K6100-PC PC Interface Kit..

6. **Personnel Info 1** to **Personnel Info 20** - these boxes are used to give titles to the 20 extra lines of information that may be stored for each keyholder in the **Personnel** application. Type the new titles, as required.

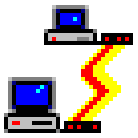
7. Choose **Change** to store the new information programmed.

8. It is recommended that you add and configure divisions one at a time.

   However, at a later stage you may need to add further divisions - to do this choose **Clear** to clear the information displayed, then enter/select the information for the new division, then choose **Add**.

9. Choose **Close** to return to the main **Installer** screen.

Installer: Workstations



The next step is to set up the **Workstations** (PCs) on your system. The **Workstations** application in **Installer** is used to:

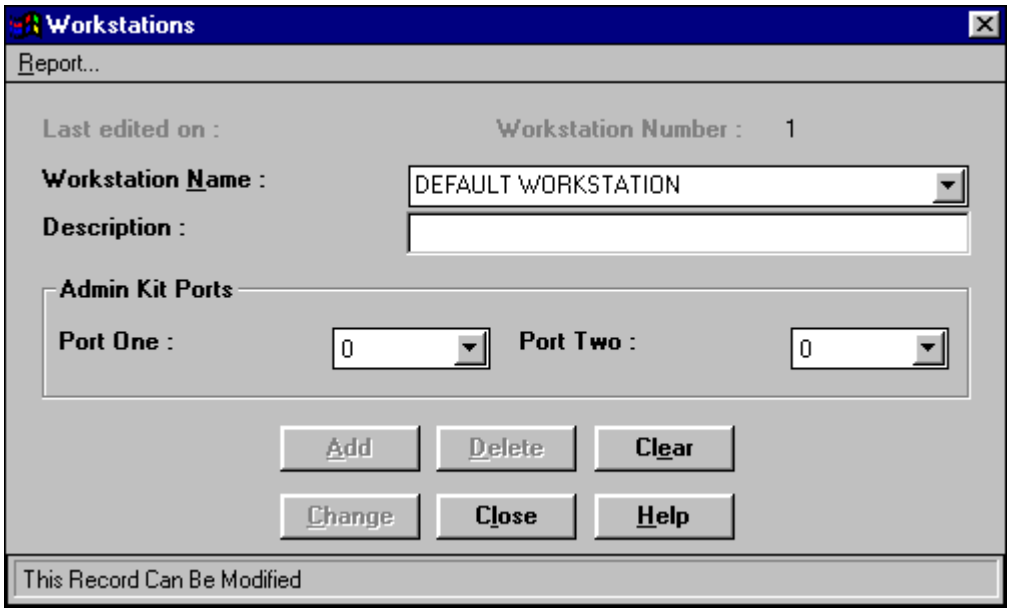
- Give the Workstation a unique name, for example, Workstation 1 etc. Additional information can be added in the **Description** field. The **Workstation Name** is mandatory, the **Description** optional.

  Note: If you have a single PC installation then you can use the default Workstation name or **Change** the name of your Workstation to one of your choice.

- Specify the Admin Kit Ports. These fields are only used if you have one or more PC Interface Kits used **solely** for ID Device administration - that is they are **NOT being used** to communicate to a K2100/K1100 door controller. Any PC Interface Kits or CNCs connected to a Workstation which communicate to a door controller are set up in the **Masters** application (see below) where you specify the workstation and port number.

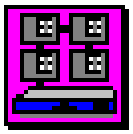
Note: Full details of adding PCs is given in the Multi PC Installation Manual.

Start the **Workstations** sub-application from **Installer**.



1. Enter a Workstation Name for the PC being used on the system.
2. Enter a Description, possibly where the PC is located.
3. Select the first COM Port Number on the PC **(Port One)** to which the first administration PC Interface Kit is connected. Use this selection ONLY if this Workstation is solely for administration, and not communicating to door controllers.
4. Repeat for **Port Two** if a second administration PC Interface Kit is connected. If only one PC Interface Kit is being used for administration, then make sure **0** is selected. Use this selection ONLY if this Workstation is solely for administration, and not communicating to door controllers.
5. Choose **Change.**
6. Repeat the operation for other Workstations on the system.
7. Choose **Close** to return to the **Installer** sub-applications screen.

Installer: Masters



Next, you need to define the Masters you have on your system, and establish communications between them and the Workstations.

There are two types of Masters that you need to be concerned with at this stage:

1. K2100/K1100 controller, connected to a Workstation either directly, or via a PC Interface Kit.
2. Central Network Controller - Multi-Site or Single Site.

Note: You may be familiar with the concept of 'Remote Masters' on sites communicating to a CNC via RS-232 - these are not programmed into this part of Readykey for Windows.

As with Sites and Divisions, you should install and establish communications with Masters one at a time.

If you are not familiar with the different communications methods available on Readykey systems, then you should read the *Readykey for Windows System Overview* before continuing.

A summary of the main points in installing each type of Master is given below:

CNC (K6100-CNC or K6100-CNCII)

1. Connect the CNC 'Host PC' port to a COM (serial) port on the Workstation using the cable provided.
2. Ensure the CNC baud rate is set to 9600 - this is the default setting for all new CNCs supplied by Radionics.
3. Connect the CNC to its power supply, and the supply to the AC mains, using the cables provided.

Refer to the Central Network Controller Installation Manual for additional information.

PC Interface Kit

1. Connect the PC Interface Kit to a COM (serial) port on the Workstation using the cable provided.
2. Connect the PC Interface Kit to the mains, desktop reader (or Wiegand Interface), using the cables provided.
3. Connect the PC Interface Kit to the Line Driver using 4-core cable. The Line Driver is then plugged into the RS-232/Printer port of the K2100/K1100 master controller.

   Note: It is recommended to use a 6-core cable for the connection from Line Driver to PC Interface. The extra wires will needed if there is not a common ground on the system or for ease of future expansion.
4. Make sure the System Type of the master K2100/K1100 is set to 2, and the baud rate to 9600.

Refer to the K2100/K1100 Installation Manual for additional information.

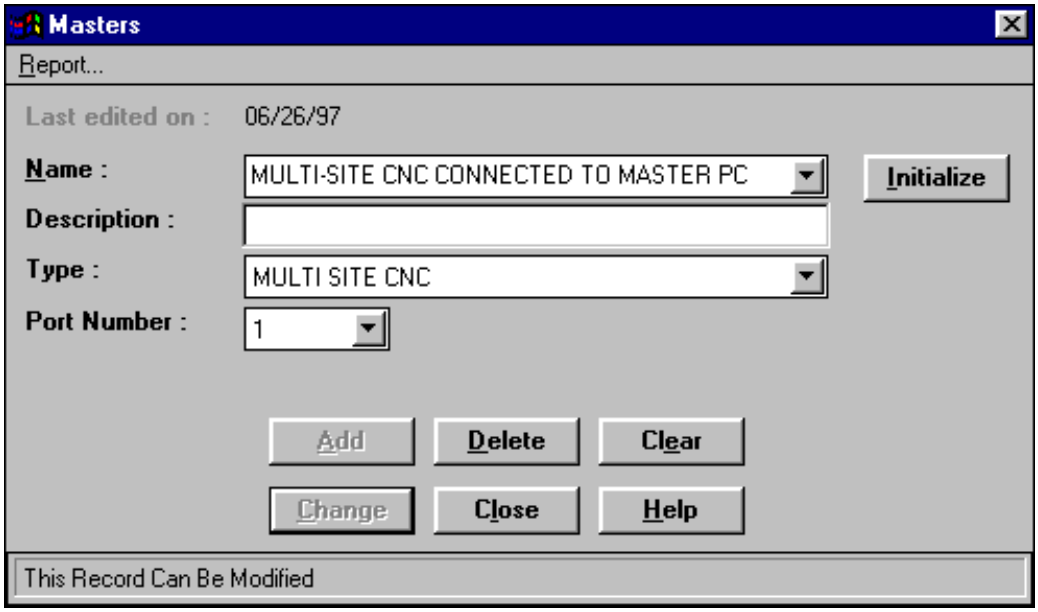
Direct RS-232

1. Connect a COM (serial) port on the Workstation to the RS-232/Printer port of the K2100/K1100 master controller (see the Reference Section for wiring information).
2. Make sure the System Type of the master K2100/K1100 is set to 2, and the baud rate to 9600.

Refer to the K2100/K1100 Installation Manual for additional information.

Adding Master Information

Choose **Masters** from the **Installer** sub-applications.



1. Make sure the **Default Master** is selected.
2. Enter a **Name** and **Description** for the master.
3. Select the **Type** of master - *Single Site CNC*; *Multi Site CNC* or *2100*. Use *K2100* for both a K2100 and a K1100 master controller.

   Note: All new CNCs will be Multi-Site - only select *Single Site CNC* if you know you have a K6000 CNC from an existing system which uses this type.
4. Select the **Port Number** - this is the COM port on the workstation through which the Master communicates.
5. If you have more than one Workstation on the system, then select the **Workstation** to which the Master is connected.
6. Choose **Change** to update the **Default Master** information.
7. **a. CNC Master**

   At this stage a CNC should start communicating to the Workstation. It may not be immediately obvious, however, that this is happening. To prove communications, you should attempt to initialize the CNC. Choose the **Initialize** button. Confirm that you want to do this when requested.

   After a short pause, the PC should report:

   - and the CNC display will change to:

```
** MONITORING **
```

If, however, you receive any other messages, then you should refer to the Reference Section described later, and the Troubleshooting section in Appendix A for assistance.

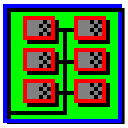
b. K2100/K1100 Master

You will not be able to initialize a K2100 or K1100 master from here, nor will the door controller start to communicate with the PC until you have added it in **Installer: Controllers**, described later.

8. Once you have completed the above steps for the first Master on your system, you should repeat them for each additional CNC/K2100/K1100 master, first choosing **Clear**, entering the new information, then choosing **Add**.

9. Choose **Close** when you have programmed all the Master information, and successfully initialized each CNC.

Installer: Sites



A site is a group of one or more door controllers that share a common communications path to a CNC or K2100/K1100 master.

From this point, most information needs to be programmed 'per Division'. Once you have set up additional Sites, then some information also needs to be programmed 'per Site'. You should concentrate on programming and commissioning a single Site, programming a key or card with access through all readers on the Site, then repeating the operation for additional Sites and additional Divisions where applicable.

Commissioning a Site

Commissioning a site consists of four stages:

1. Programming the Readykey for Windows software with information about the Site - this is done through **Installer: Sites.**

2. Configuring each Readykey door controller correctly - setting the address, baud rate, etc.

3. Connecting the Readykey door controllers to the master, possibly using third-party communications equipment such as modems, line drivers, etc.

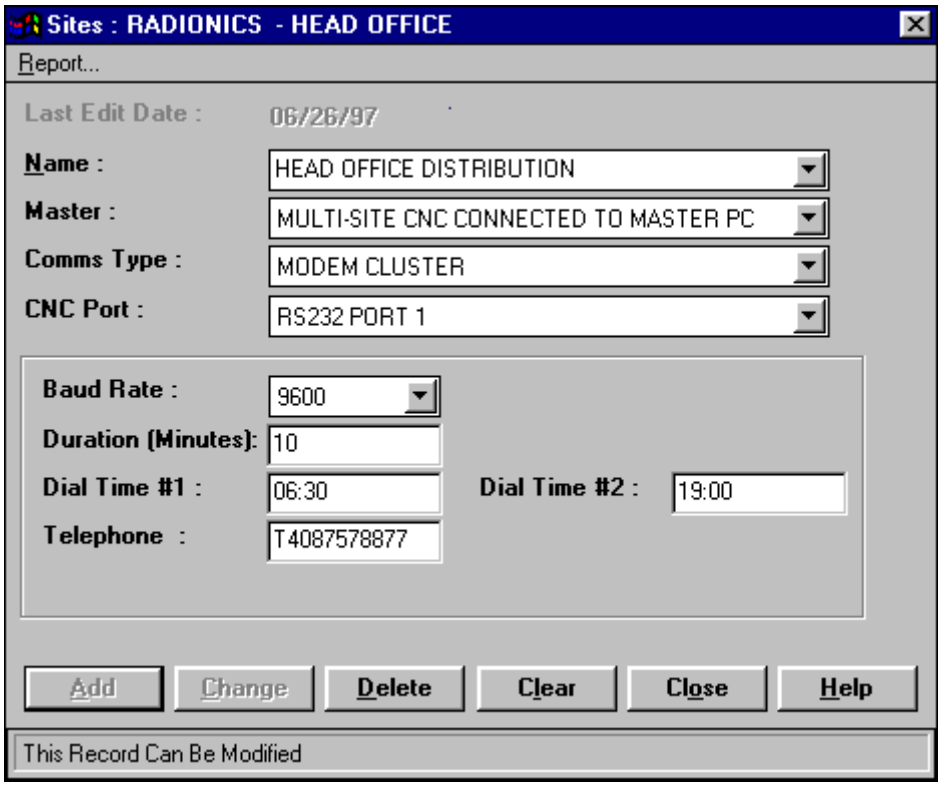
4. Programming the door controller and other Readykey hardware information into Readykey for Windows - this is done through **Installer: Controllers, Installer: Doors** and **Installer: Alarm Modules**.

Note: It is assumed that readers and other Readykey hardware have already been connected to the door controllers - information on this will be found in the documentation supplied with the door controller and/or hardware. K2100/K1100 door controllers should also have been tested as 'stand-alone' units first, as described in Appendix A of *K2100/K1100 Installation Manual.*

Setting Up Sites

Note: One Site is provided as part of the default database. This Site communicates to the default master via the Six Wire Bus. Many Readykey for Windows systems will have a Site of this type - however, this information may be changed if required, and additional Sites programmed.

1. Choose the **Sites** icon from the **Installer** sub-applications.



2. Ensure the default Site, *Site One*, is displayed.
3. Type the **Name** of the Site, with an optional **Description** to give more information about the Site.
4. Select the **Master** to which the Site communicates.
5. Select the **Comms Type -** this is the type of Site installed. Choose from:
   a. *Six Wire Bus* - this includes a Six Wire Bus from a CNC; and a K2100/K1100 connected to the PC; either directly or via a PC Interface Kit.
   b. *Direct RS232* - a single door controller connected to a CNC via a permanent RS-232 link.
   c. *Direct RS232 and Dataswitch* - between 1 and 8 door controllers connected to a CNC via a permanent RS-232 link and COS-4 or COS-8 dataswitch.
   d. *Direct RS232 Cluster* - a K2100 or K1100 door controller connected to a CNC via a permanent RS-232 link, with up to 7 additional door controllers connected to the K2100/K1100 via the Six Wire Bus.
   e. *Modem* - a single door controller connected to a CNC via a dial-up modem link.
   f. *Modem and Dataswitch*- between 1 and 8 door controllers connected to a CNC via a dial-up modem link and COS-4 or COS-8 dataswitch.

g. *Modem Cluster* - a K2100 or K1100 door controller connected to a CNC via a dial-up modem link, with up to 7 additional door controllers connected to the K2100/K1100 via the Six Wire Bus.

Further information on each of the above is contained in the Reference Section described later, and in the *Readykey for Windows System Overview.*

6. Select the **CNC Port** through which, and the **Baud Rate** at which, the Site communicates - there will only be a choice offered for these if the **Comms Type** selected is **NOT** Six Wire Bus.

7. If the **Comms Type** selected includes a modem, then information needs to be also entered in each of the following boxes:

   a. **Duration** - this is the maximum time (in minutes) the Site will stay on-line to the master during a normal dial-up session providing the master is still receiving activity from the site. If no activity is being received, the system will remain on line with the remote site for 1-2 minutes and then hang up.

   b. **Dial Time #1** and **Dial Time #2 -** a CNC can automatically dial a Site once or twice in any 24 hour period. Enter the times for this to happen here. Times must be entered using a 24 hr style of clock. An example of 4pm would be entered in as: 16:00. The ":" is required to separate the hours and minutes.

   c. **Telephone** - enter the telephone number to which the modem at the remote site is connected. Prefix the number with a 'T' if the exchange supports 'Tone' (DTMF) dialing.

8. Choose **Change**, if you have modified the default Site information.

9. You should now complete the programming of other information for the Site - Areas, Controllers, Doors, Access Groups, and a key or card with access through all readers on the Site, before adding further Sites.

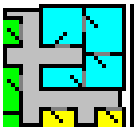
   Note: When programming further Sites, choose **Clear** to clear the information displayed, enter the information for the new Site, then choose **Add**.

10. Choose **Close** to leave **Installer: Sites**.

11. At this stage you should set up the communications links and equipment to the site - modems, dataswitches, six wire bus, PC Interface Kits, etc. Refer to:

    - *Central Network Controller Installation Manual*
    - *K2100/K1100 Installation Manual*

Installer: Areas



Introduction

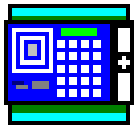
As part of your system design, you will have decided how each Site will be divided into Areas. Each Area needs to be programmed into Readykey for Windows. When you define the readers, (later, in **Installer: Doors**), you will then specify into which Area each reader controls (restricts) access. Areas can also be used for grouping alarm inputs.

Adding Areas

1. Double-click the **Areas** icon from the **Installer** applications.

2. If you have defined more than one Site, then make sure the correct **Site** is selected - click on the drop down box to change Site if necessary.
3. Choose **Clear**.
4. Enter a **Name** for the Area - each Area must have a unique name. You cannot have two Areas with the same name, even if they are on different Sites or in different Divisions.
5. Enter a **Description** for the Area. This can be used to provide system operators with extra information about the Area.
6. You will not be able to make any entries in **Entry Doors** - this will be done automatically when you define the relationship between doors and areas in **Installer: Doors**.
7. Choose **Add**.
8. Repeat steps 2-7 for each Area on the Site.
9. Choose **Close** when you have added all the Areas for the first Site. You will need to return to **Installer: Areas** later if you have further Sites on your system.

Installer: Controllers



Each site on your system will consist of one or more Door Controllers, which, in conjunction with the readers, actually control the access to each of the areas on the site.

In this section, you will program all the Door Controller information into Readykey for Windows, and establish communications with the Door Controllers.

Configuring Door Controllers

Each Door Controller will need to be configured correctly before it will communicate with Readykey for Windows. This involves programming each Door Controller with an Address and, in some cases, a System Type and Baud Rate.

The table below lists the settings that should be made for each Door Controller on the different types of Site available. Refer to the documentation that came with each Door Controller for information on how to make these settings.

Some Site types will consist of a 'Master' (possibly a 'Remote Master') and 'Slave' controllers, others just 'slave' controllers.

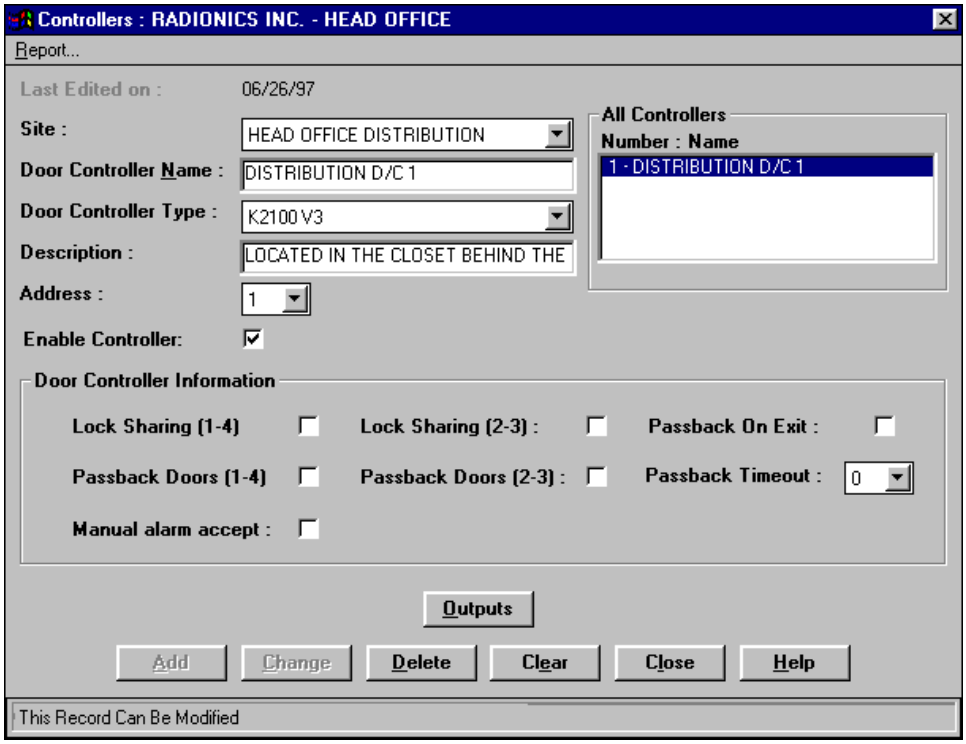
	Setting/ Type of Site	**'Mode'**	**Address**	**Baud Rate (see Note 1)**	**System Type (see Note 2)**
a	2100/1100 Master via PC Interface Kit or direct	*Master*	1	9600	2
		Slave	2-8	N/A	3
a	Six Wire Bus from CNC	*Slave*	1-32	N/A	3
b	Direct RS-232	*Remote Master*	1	300-9600	2
c	Direct RS-232 via Dataswitch	*Slave*	1-8	300-9600	3
d	Direct RS-232 Cluster	*Remote Master*	1	300-9600	2
		Slave	2-8	N/A	3
e	Modem	*Remote Master*	1	300-9600	2
f	Modem and Dataswitch	*Slave*	1-8	300-9600	3
g	Modem Cluster	*Remote Master*	1	300-9600	2
		Slave	2-8	N/A	3

Notes:

1. The Baud Rate does not need to be programmed in certain cases. However, where applicable, the same setting needs to be programmed for each Door Controller on a Site, and needs to match the Baud Rate programmed in **Installer: Sites**.
2. The System Type setting only needs to be programmed for K2100 and K1100 door controllers. However, K2000-N controllers can only be used as slave controllers (System Type 3).

Programming Door Controller Information

1. Double-click on the **Controllers** icon from the **Installer** applications.



2. Make sure the correct **Site** is selected - click on the drop down box to change sites if necessary.
3. **Door Controller Name** - each door controller must be given a unique name.
4. **Door Controller Type** - select the type of door controller that exists. The choice available will be restricted, dependent on the setting you made for the **Oldest Controller** in **Installer: Divisions.**

   Note: Some controller types are described as 'K2100 or K1100 with Version x.y or later' or similar - this refers to the software installed in the door controller. Press the **?** key on the door controller keyboard faceplate to reveal the software version.
5. Enter a suitable **Description** for the controller; this may be the physical location of the door controller. A recommendation for the description would be the location of the door controller. Example Description: Located in the closet behind the front reception desk.
6. Select the **Address** - this must match the setting programmed in the door controller itself. The range of values available will depend on the type of site.
7. Make sure **Enable Controller** is selected. Readykey for Windows or the CNC master will not attempt to communicate with any door controllers that are not enabled.

   Warning: Disabling a Master or Remote Master door controller will disable communication to all Slave controllers on that site.

8. **Door Controller Information** - select any 'special' options that may be in use. These are summarized below:

   a. **Lock Sharing (1-4) -** select if the readers connected to channels 1 and 4 are to control the same lock. On a K1100 controller this option will be **Lock Sharing (1-2)**. Channel number 1 **must** be the entry reader and channel number 4 (number 2 for a K1100) **must** be the exit reader. The door contact, request to exit device (if used), and the lock must always be connected to the 'Entry' reader.

   b. **Lock Sharing (2-3) -** select if the readers connected to channels 2 and 3 are to control the same lock. This option will not be available on a K1100. Channel number 2 **must** be the entry reader and channel number 3 **must** be the exit reader. The door contact, request to exit device (if used), and the lock must always be connected to the 'Entry' reader.

   c. **Passback Doors (1-4) -** select if you wish to use Anti-Passback between the readers connected to channels 1 and 4. On a K1100 controller this option will be **Passback Doors (1-2)**. Channel number 1 **must** be the entry reader and channel number 4 (number 2 for a K1100) **must** be the exit reader.

      Note: If a door open time of 1 or greater has been set then the door **must** be opened before Passback comes into effect. If you present you ID device and then do not open the door then the option is not activated.

   d. **Passback Doors (2-3) -** select if you wish to use Anti-Passback between the readers connected to channels 2 and 3. This option will not be available on a K1100. Channel number 2 **must** be the entry reader and channel number 3 **must** be the exit reader.

      Note: If a door open time of 1 or greater has been set then the door **must** be opened before Passback comes into effect. If you present you ID device and then do not open the door then the option is not activated.

   e. **Passback Timeout** - select the time in minutes after which a key will be allowed entry to an area again without first leaving the area.

      Note: The time is selectable, in 5 minute steps, between 10 and 30 minutes (10, 15, 20, 25, 30 minutes). The time starts once an attempt is made to use an ID Device on the entry or exit reader.

   f. **Manual Alarm Accept** - this feature affects the behavior of relays on K2100/K1100 door controllers. When a relay is activated by the occurrence of an alarm event at the door controller, then, if this option is selected, the relay will latch until the alarm is accepted only at the PC.

      Note: This option will only be available when the **Door Controller Type** is a K2100 or K1100 with either *Version 2.0; V3.0 or later;* or *V3.0 with 18,000 Personnel*.

9. Choose **Add**. The name of the controller, prefixed by the address, will now appear in the box to the right of the screen of all door controllers on the site.

10. Repeat the operation for all other door controllers on the site - choose **Clear** to empty all the boxes first.

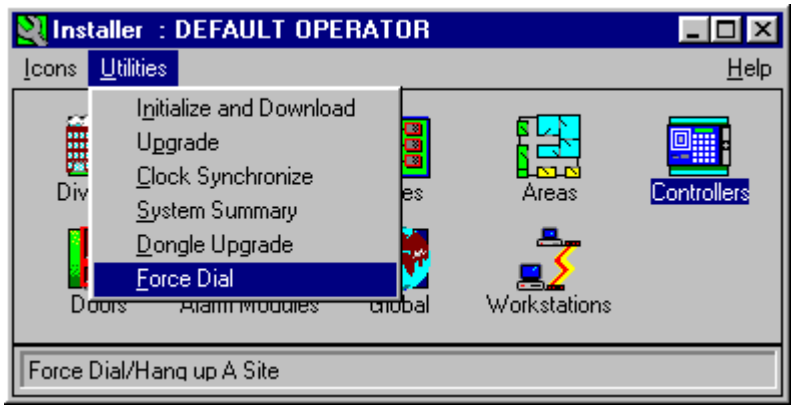
11. Choose **Close** when you have added all the door controllers for the site, to return to the **Installer** sub-applications.

Establishing Communications

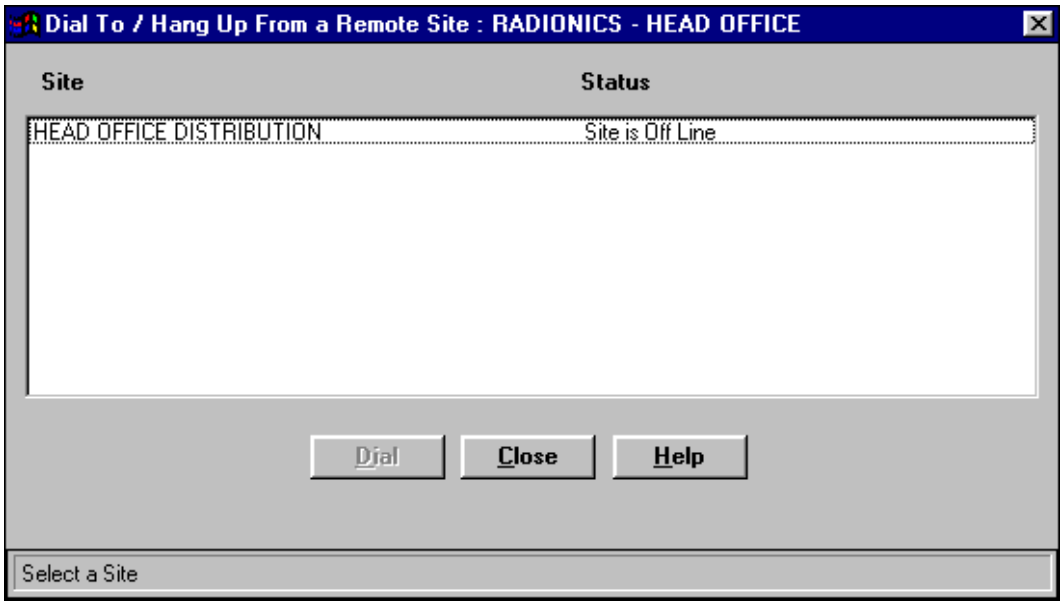
Once the information has been added for each door controller, Readykey for Windows will try to communicate with it, assuming the communications link is in place. Sites that communicate via dial-up modem will need to be 'force dialed' first.

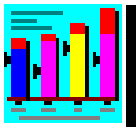
Force Dialing a Remote Site

1. From **Installer**, select **Force Dial** from the **Utilities** menu:



2. The **Force Dial** screen will now be displayed:





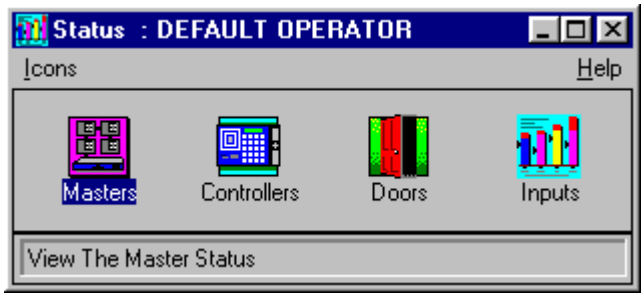
3. The display will list all dialup sites, along with their current communications status.
4. Select the **Site** which you wish to force dial from the list displayed.
5. The current **Status** of each site will be displayed - usually this will be *Site is Off Line*.
6. Choose **Dial**. The **Status** will change to '*Dialing Site'*. The **Dial** button will change to **Hang Up.** The modem should now dial the site. If no problems are encountered by the CNC in establishing communications with the site, then, after a short time the **Status** will change to - '*Site is On Line'*. (Refer to the Troubleshooting section in Appendix A if you have problems establishing communications.)
7. Choose **Close** to leave **Installer: Force Dial** once the site is on-line.

Note: You should leave the site on-line until programming of the test ID device and you have confirmed that all readers and door controllers on the site are working correctly, and the test ID device is allowing access through all doors on the system.

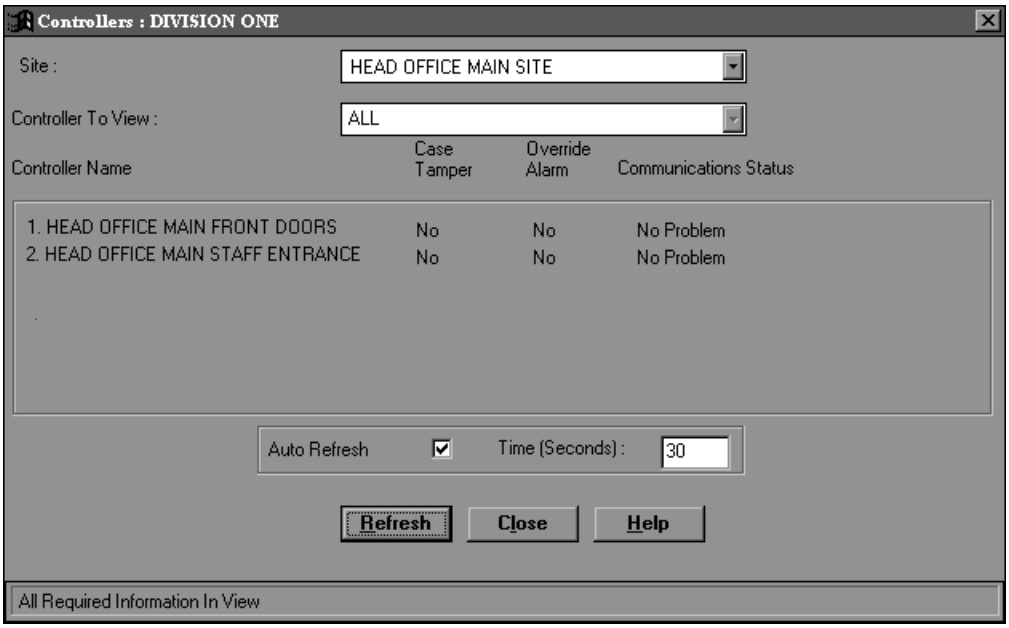
Status - Checking Communications

1. From the main **Login** applications screen, choose **Status**.

   Note: You may wish to close **Installer** first to enhance system performance. Use **Alt+F4** or click on the **x** in the top right-hand corner of **Installer** to close down the Installer applications**.**



2. From the **Status** sub-applications, choose **Controllers**.



3. Make sure the correct **Site** is selected - click on the drop down list to change site if necessary.

4. Make sure **All** is selected in **Controller To View**.

5. Readykey for Windows will now attempt to determine the communications status of each door controller. Each **Controller Name** will be listed, along with the **Communications Status**, **Case Tamper** and **Override Alarm** conditions.

6. The **Communications Status** for each controller should be *No Problem*. The display of each controller itself should also be flashing its address, e.g.:

   1

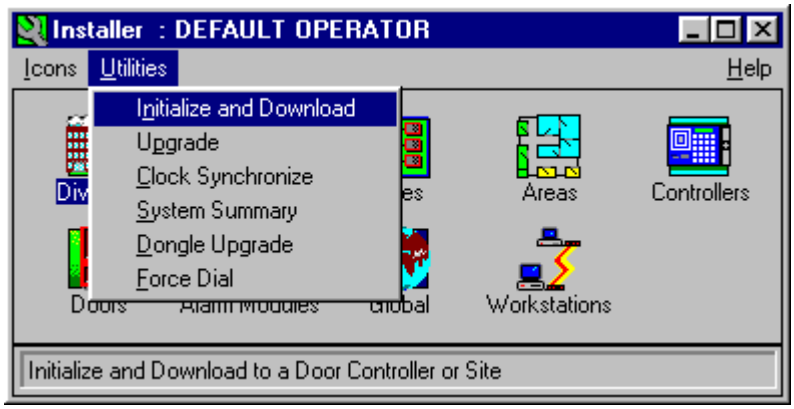
   Refer to the Troubleshooting section in Appendix A if status reports a communications error for any door controllers.

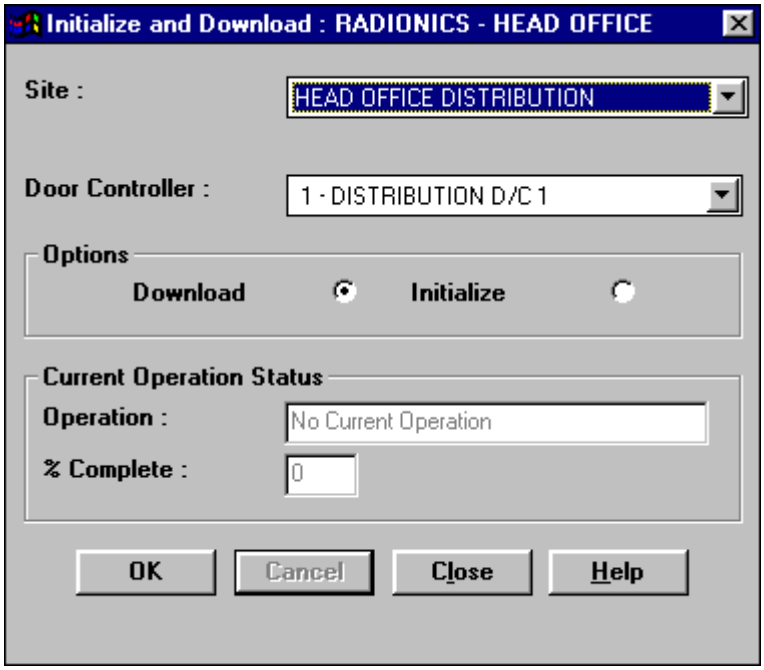
7. Once you have verified communications to all door controllers on the site, then choose **Close** to return to the **Status** sub-applications. You should then close down **Status** and return to **Installer** for the next stage.

Initialize and Download

Now communications have been established with each door controller, it is important to initialize and download to each to clear the memory (initialize) and to make sure each is correctly programmed (download).

From the **Utilities** menu in **Installer**, choose **Initialize and Download**.

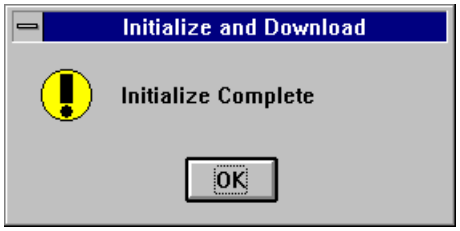




Initialize

You will need to initialize each door controller individually:

1. Select the **Door Controller** from the list.
2. Select **Initialize** from **Options**.
3. Choose **OK**. Assuming the door controller is still communicating, then after a short delay you should receive the message:



- the door controller will also bleep and there may be a click as some relays are reset.

4. Repeat the operation for each door controller in turn from step 1, above.

   Note: If your site communicates via a CNC, then the display of the CNC may change from

   ```
   ** MONITORING **
   ```

   to something similar to:

   ```
   ** SITE 001*00023
   ```

   - the number at the right hand side of the display indicates the number of 'updates' in the CNC which are waiting to be sent to the door controllers - it should be decreasing. When the number of updates reaches zero, the *** MONITORING ***** display should return.

Note: If there is an = sign on the display instead of the *, or if the number of updates remains static for any length of time, then there may be a communications problem with the site - you may need to use the **Force Dial** utility to re-establish communications, or the **Status** application to verify communications.

Download

It is possible to download to all door controllers on a site simultaneously. The download will take place in two stages - firstly from the PC to the master (CNC or K2100/K1100), then to the slave door controllers.

Note: On a CNC-based site, you should ensure *** MONITORING ***** or ***SITE nnn*00000* is displayed on the CNC before proceeding.

---

1. Select **All** from the **Door Controller** list box **- Download** will be automatically selected from **Options**.

2. Choose **OK**. You will see the **% Complete** increase to 100%.

   Note: As the download progresses, on a CNC-based site, then you will notice the CNC display change as described earlier.

3. When the download from the PC is complete, you will see:

   Choose **OK.** You now need to wait for the second stage of the download to complete to the door controllers - make sure the CNC display shows *** MONITORING ***** or *** SITE nnn*00000.*

   A K2100/K1100 master will have a display similar to:

   ```
   D/C 2 UPDATE-34 1
   ```

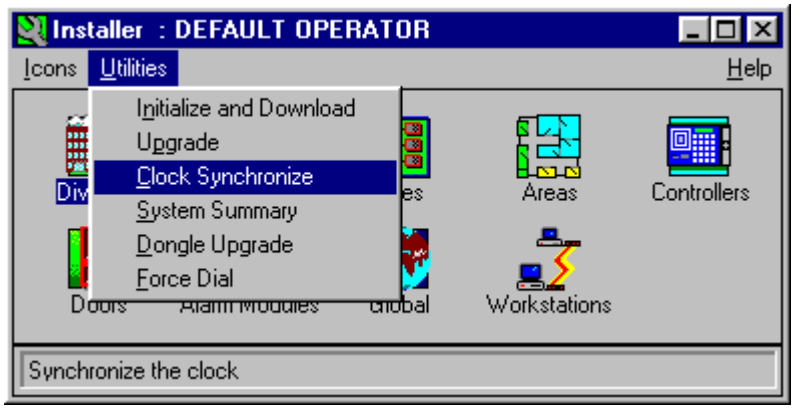
   if there are any updates outstanding for slave door controllers. If the display of the master K2100/K1100 is only flashing the address, then the download to the slave controllers is complete.

4. Choose **Close** to leave **Initialize and Download**.

Clock Synchronize

The next step is to ensure that the system clocks in the door controllers (and CNC) are synchronized to the PC time.

From the **Utilities** menu in **Installer**, choose **Clock Synchronize**.



The CNC and door controller displays should flash:

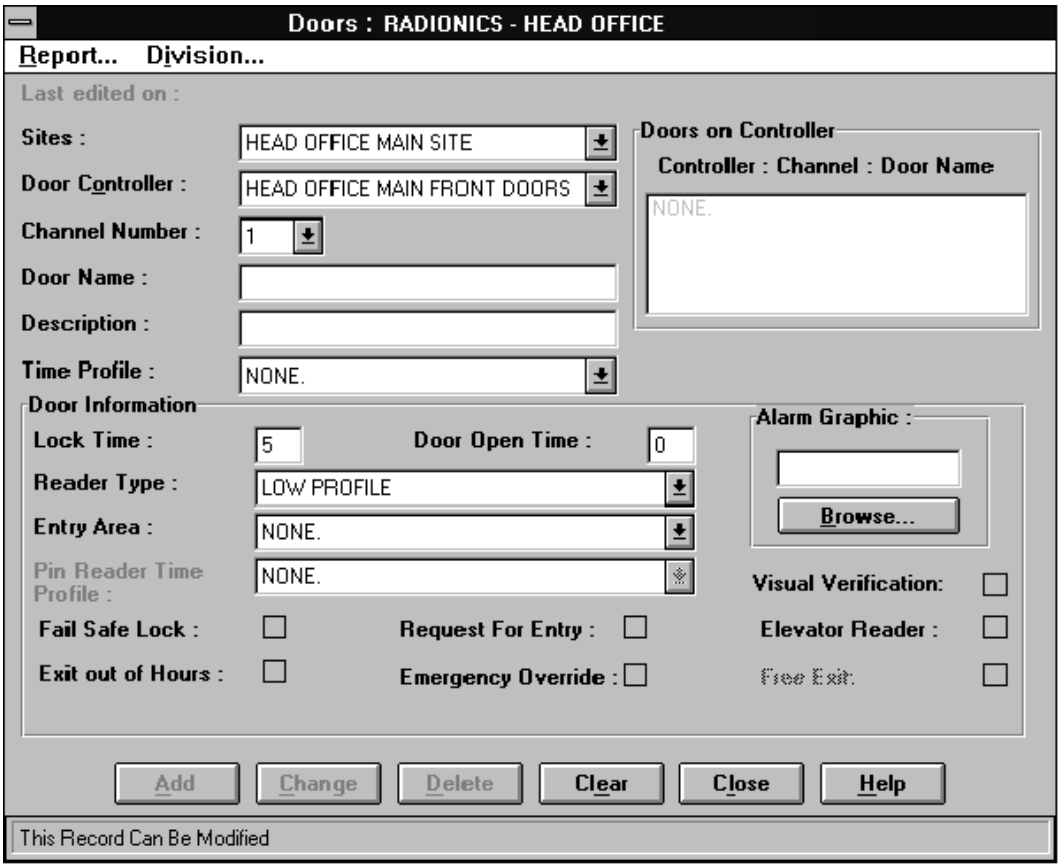
```
** CLOCK SYNC **
```

and there will be a series of short beeps.

When the operation is complete, the PC will report:

Installer: Doors

The next stage is to define the doors (readers) on each door controller. Start the **Doors** sub-application from **Installer**.



1. Make sure the correct **Site** is selected - click on the drop down list to change sites if necessary.
2. Select the **Door Controller** to which the reader is connected - you will need to repeat this process for each reader on all door controllers on the site.
3. Select the **Channel Number** - this will be the 'port' on the door controller to which the reader is physically wired.
4. Enter a **Name** for the door - all doors on the system must have a unique name.
5. Enter a **Description** for the door, if required - this may be used to give extra, for example, information about the location of the door.
6. At this stage you will probably not have set up any **Time Profiles** - you can return to **Installer: Doors** later, or set this information in **Admin: Doors** , if you wish a door to automatically unlock and lock at specific times.
7. **Door Information:**
   a. **Lock Time -** enter the number of seconds you wish the lock to release for following a valid access. The default is set to 5 seconds. The maximum that can be set is 255 seconds.
   b. **Door Open Time** - if the door is monitored, enter the number of seconds the door can remain open after the lock time expires before a 'Door Left Open' alarm condition is to be generated. The default entry is 0 seconds, which means that no door monitoring is set. The maximum that can be set is 255 seconds.

c. **Reader Type** - select the type of reader installed. For most types of reader, the setting made here is not important. However, if you are using a *K2001-P PIN Reader with Time Profiles* then the correct setting **MUST BE MADE.** It is **highly recommended** that the correct reader type is selected to avoid confusion when programming or servicing the system at a later date.

d. **Entry Area** - select from the drop-down list the area (as defined earlier in **Installer: Areas**) to which access is gained after using this reader.

Note: leaving this selection set at 'None', will not allow anyone to gain access through this door using their ID device. This selection must always have an 'Entry Area' assigned unless this reader (Door) is used for elevator control.

e. **PIN Reader Time Profile** - if the **Reader Type** selected was *K2001-P PIN Reader with Time Profiles* then, when you have defined some Time Profiles, select the time profile during which **only** a valid key/card needs to be used to gain access. The PIN number is **Not Programmable, it is actually part of the Readykey key or card. This** will be automatically displayed when adding keyholders when using Readykey ID Device type.

Note: Outside the time profile, a valid key or card **PLUS PIN** will need to be used. If it is desired to always use a valid key or card PLUS PIN, then select 'None' for PIN Reader Time Profile.

f. **Fail Safe Lock** - select this option if a fail safe (power to lock) lock is installed at the door. If a fail secure (power to release) lock is installed, then leave this box unchecked.

g. **Exit Out Of Hours** - select this option to allow keyholders to use an exit door to leave an area, even though their time profile has expired. **Warning: Use this setting only on exit doors on the system. Selecting this option on entry doors on the system will prevent any time restrictions on personnel.**

h. **Request for Entry** - if selected, this option will cause the transaction generated when a request to exit switch is operated to be 'Request for Entry' instead of the usual 'Request for Exit'.

i. **Emergency Override** - this option, if set, allows the Request to Exit and Door Contact circuits on a K2100/K1100 controller to be used in a special way, as described in detail in *K2100/K1100 Installation Manual.* This selection will override the lock when the request to exit input is operated, and remain overridden until the request to exit input goes back to the normal open state. Selecting this option eliminates the use of door monitoring for Alarm conditions when the door has been forced open. This allows personnel to exit freely for low priority doors, where notification for forced unauthorized access is not required.

See **Free Exit**, described later in this section.

j. **Visual Verification** - this option sets the door to trigger visual verification. This means that a picture of keyholders attempting to access the door can be automatically displayed to an operator. For more information refer to *Readykey for Windows Photo ID Module Datasheet*.

k. **Elevator Reader** - this option will only be available if your system includes the Elevator Control module. If set, this reader will be designated as an 'Elevator Reader' - refer to *Readykey for Windows Elevator Control Datasheet* for detailed information on setting up Elevator Control.

l. **Free Exit** - this option will only be available if you have selected **Emergency Override**. This option is also only available on K2100 / K1100 door controllers.

With just the **Emergency Override** option set, then breaking the DR1 loop on the reader channel will generate a *Free Exit* transaction for that door. No other activity will occur. However if the **Free Exit** option is also set, then the lock output will also be activated for that door. Selecting this option and the Emergency Override option eliminates the use of door monitoring for Alarm conditions when the door has been forced open. This allows personnel to exit freely for low priority doors, where notification for forced unauthorized access is not required.

8. Choose **Add.** The information for the door will be saved and also passed to the door controller.

   Note: Once the door has been added to the system, before any changes to the existing door information can be made, the door must first be selected by clicking onto the desired door within the 'Doors on Controller' box. This calls up the existing door record so that it may be modified.

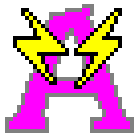
9. Repeat the process for other doors on the door controller, then for other door controllers on the site. You will need to return to **Installer: Doors** later to configure the door information as you commission other sites on the system.

10. Choose **Close** to leave **Installer: Doors** when you have finished programming the door information for the site.

11. It is a good idea at this point to confirm that the areas and doors are correctly assigned, as per your system designs. Any errors could result in keyholders being given access through the wrong doors.

    To check the area assignments, choose **Close** to leave **Installer: Doors**. From the **Installer** sub-applications, choose **Areas**. For each **Area** you have defined, make sure that the correct doors are in the **Entry Doors** box. When you have confirmed that everything meets with your plan, then choose **Close** to return to the **Installer** sub-applications.

Installer : Alarm Modules



If you have alarm modules, usually Alarm Event Managers (AEMs), the next stage is to define them and their inputs and outputs.

1. Install your Alarm Modules according to the instructions provided.

2. Start the **Alarm Modules** sub-application from **Installer**.

3. Make sure the correct division name is selected (the division name is displayed in the title bar - if not, select Division... from the menu).

4. Select the Site which the door controller is on.

5. Select the Door Controller to which the module is attached. Any existing modules will appear in the box on the right.

6. Select the Channel Number (1-4) to which the module is attached.

7. Enter a Name for the module, and a Description if required.

8. Select the Alarm Module Type, different alarm modules allow different features to be selected. Make sure you select the right type. Select K2015 or K2015A Alarm Event Manager. Only use the K2015 option if you are sure this is the exact type that you have. The K2015A Alarm Event Manager has replaced the K2015 and is the only Alarm Module sold for many years. K2015A is the default setting for type.

   Note: Once you have selected an Alarm Module Type and chosen Add you will not be able to change the type without deleting the record and re-entering the information.

The K2015 Alarm Module has 8 inputs, that may be selected as normally open or normally closed by switches on the Alarm Module, and 4 relay outputs.

The K2015A Alarm Event Manager has 8 inputs that may also be supervised for tamper detection, and 8 relay outputs.

9. Choose Add or Change before choosing Inputs or Outputs.

Note: if you are using alarm areas to enable and disable groups of inputs then you must give the operators the correct privilege to do this in **Admin, Operators, Setup Privileges, Alarm**.

10. You have now finished with the **Installer** applications. Close the **Installer** application by using **Alt+F4.**

Note: To configure the Inputs and Outputs refer to the section *Configuring Optional Hardware* later in this manual. Alternatively, you can click on the **Help** button provided on the relevant dialog boxes.

Admin

The next stage is to program access group information - Access Groups consist of lists of areas, possibly with a time profile (to restrict access to those areas to certain times of day); these access groups are then assigned to keyholders in the **Personnel** application.

Access Groups only allow access to areas on a single site. To give access to areas across more than one site you will need to use Divisional Access Groups. Divisional Access Groups consists of a combination of one Access Group from each site, and are assigned to keyholders in the same way as ordinary Access Groups.

Note: If your system consists of more than one division, then you will need to add the information **in each division** for any keyholder who needs to gain access to areas in more than one division.

Extra Access

Extra access can be useful if you wish to 'fine-tune' the access for specific keyholders - for example if a particular keyholder needs access to a specific area in addition to those defined in the keyholder's access group.

If all the door controllers on your system are K2100 or K1100s with version 3.0 software or later, then it is possible to completely avoid using Access Groups. Instead, you can assign lists of areas to individual keyholders.

It is recommended however that access groups are used for ease of administration, particularly on systems with a large number of keyholders, where, to set up a list of areas for each keyholder would be time consuming. Additionally, it is not possible to search for personnel records by selecting only the Extra Access areas to obtain a database printout.

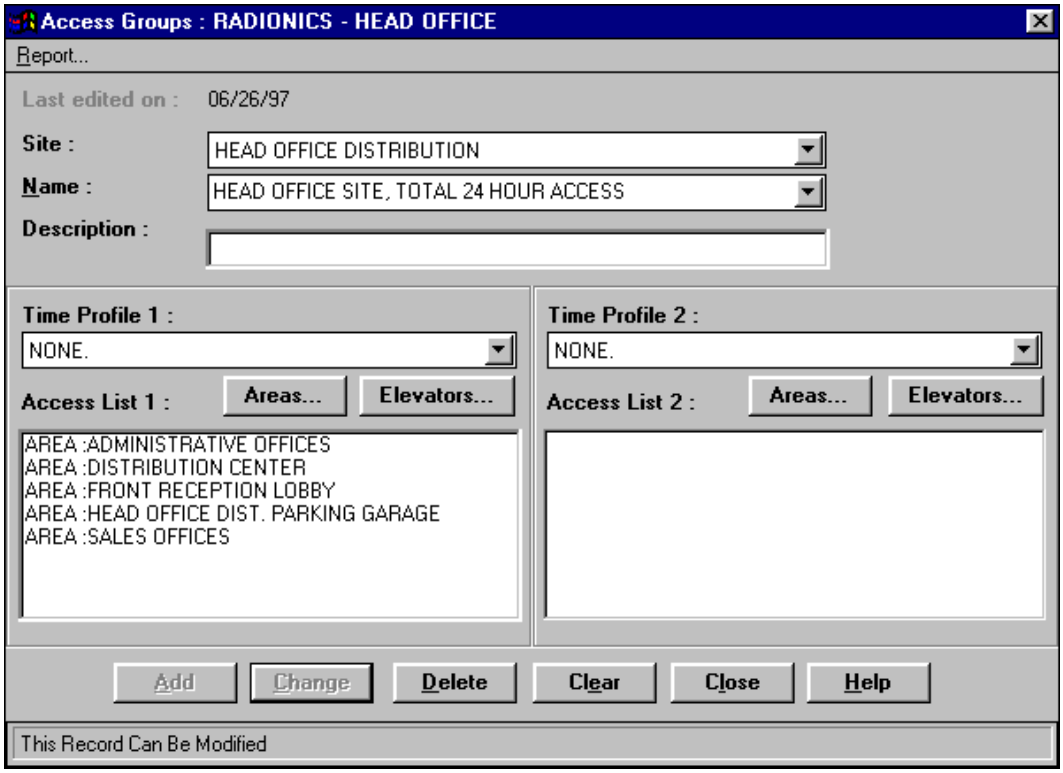
Both an Access Group and Extra Access can be assigned to keyholders, and you can mix and match the use of both on your system.

Admin: Access Groups

The first step is to create the access groups for the individual sites.

From the **Login** applications screen, start the **Admin** application.

Like **Installer**, **Admin** consists of a number of sub-applications. The part of **Admin** that is required at this stage is **Access Groups** - double-click on the Access Groups icon.

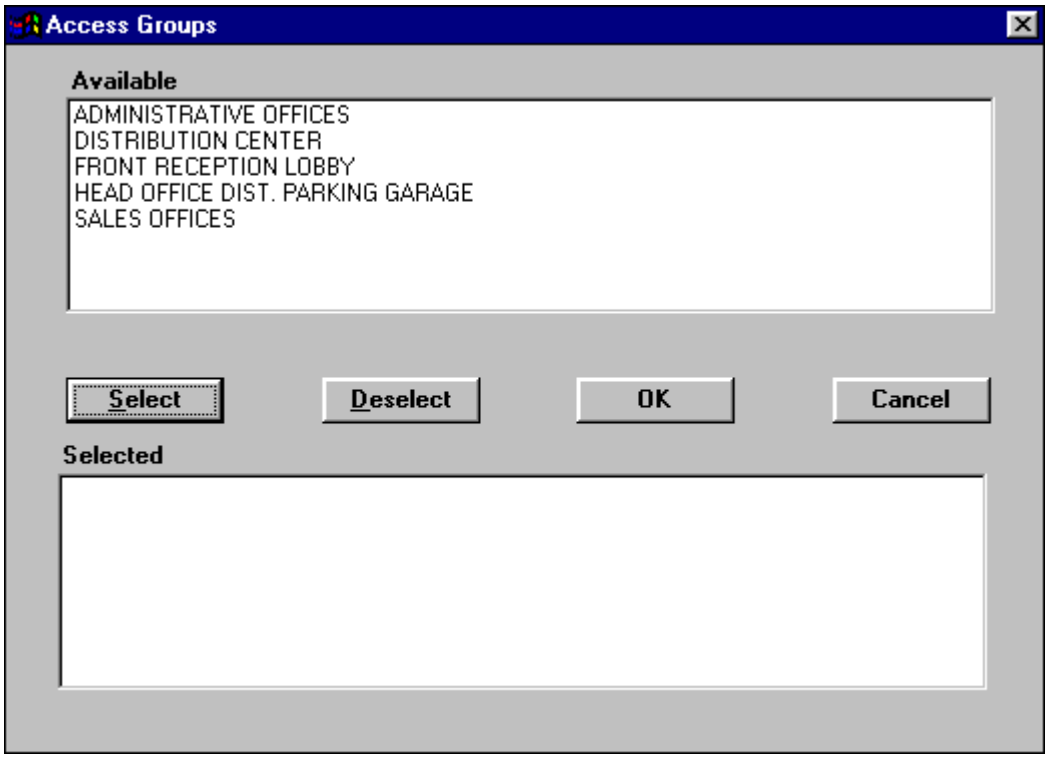


Note: If you have the elevator module installed then you should at this stage set up the elevator access groups from this dialogue. *Refer to the Readykey for Windows Elevator Control Datasheet* for more information**.** The **Elevators…** button is only displayed if the Elevator Control option has been added to the system.

An access group consists of one or two lists of areas - these are the areas to which keyholders assigned to this access group will be allowed access. Each list of areas may have an optional time profile assigned - if so, then access to these areas will be restricted only to the times and days contained in the time profile and time periods.

At this stage we are going to create an access group for the site we are commissioning, that will give continuous (24 hours, 7 days) access to all areas on the site. This will enable us to verify the Readykey for Windows system has been programmed correctly.

1. Make sure the correct **Site** is displayed - if not select the site being commissioned from the drop-down list.
2. Type a **Name** for the Access Group - each access group must have a unique name. Make the name meaningful - it will be easier for other operators to administer the system on a routine basis if the access group names are logical. You could use *Head Office Site, Total 24 Hour Access* for this access group.
3. Type a **Description** - this is optional, but should be used to provide additional information about the access group - for example *Provides 24 hour, 7 day access to all areas on the Head Office Site*.
4. Leave **Time Profile 1** and **Time Profile 2** set to *None* for this access group - note that if no (None) time profile is assigned as part of an access group then this means that access to the areas listed will be available 24 hours a day, 7 days a week for keyholders assigned this access group.
5. **Access List 1** - this is the list of areas to which keyholders with this access group will be allowed access. None will be listed at this stage. Choose **Areas...** to modify the list.
6. This will bring up the following screen, which shows all areas defined for the current site in the top 'Available' box.



7. Select each area from the list by holding down the Control key (Ctrl) on the keyboard and clicking on each area in turn, or by dragging the mouse down the list of areas while holding the mouse button down. Each area selected will become highlighted. Clicking on the area a second time while holding down the Control key (Ctrl) on the keyboard would remove the highlight and de-select the areas.
8. When all areas have been selected, choose **Select** - the areas selected will move to the lower 'Selected' box at the bottom.

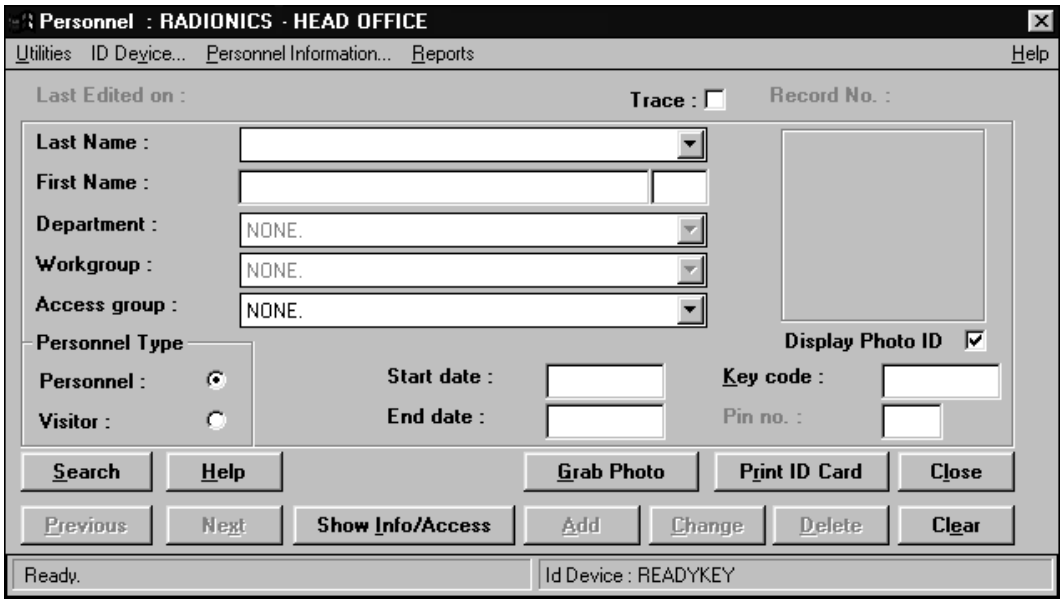
   (Areas can be removed from the lower box by selecting them and choosing **Deselect**.)

9. Choose **OK** to return to the main Access Groups screen - the areas which were 'selected' will now appear in **Access List 1**.
10. Time Profile 2 and Access List 2 are also available for Access Groups that require a secondary set of times and areas that access needs to be controlled. This would commonly be used where it is required to have access to one set of areas during specific times/days and a different set of areas during other specific times/days. If a time profile is being used to restrict access to certain times/ days, then the process could now be repeated using a different Time Profile (**Time Profile 2**) and a different list of Areas (**Access List 2**).
11. Choose **Add** to save the information.
12. You will need to repeat the process for any other sites on your system as you commission them - however, at this stage you should concentrate on adding a key or card with access only on the current site, to enable the system to be tested.
13. Choose **Close** to leave **Access Groups** and return to the **Admin** applications screen.
14. Close **Admin** using **Alt+F4** to return to the **Login** applications.

Personnel

The final stage is to add the test ID device to the system - this is achieved using the **Personnel** application.

Start **Personnel** by double-clicking the icon from the **Login** applications.



The **Personnel** application consists of a database of keyholder information. For each keyholder a Last Name, First Names, Access Group and Keycode are stored as a minimum. A Department, Workgroup, Start and End Dates (outside of which the key/card will not be allowed access), up to 20 lines of 'extra' information and up to two lists of 'Extra Access' areas/time profiles are optional entries.

Adding a Key/Card

1. Type a **Last Name** - this could be 'Test' for this example, or the last name of the installing engineer.
2. Enter one or more **First Names** - as each name is typed the initials will appear automatically in the small box at the end of the **First Names** box, and also at the end of the last name.

Note: The Last Name, plus the first three initials, must be unique in the division- for example you cannot have a *Mike Dreksler* and a *Mark Dreksler* in the same division, as these would both result in *DREKSLER_M* - add a number to one of the names (e.g. *DREKSLER_M2)*, use a middle name or initial (more than one first name) to make the names different, or enter the entire name in the Last Name and leave the First Names blank.

3. As you have not created any **Departments** or **Workgroups** yet, then leave these boxes set to *None.*
4. Select the test **Access Group (***Head Office Site, Total 24 Hour Access*) that was created in **Admin**.
5. If you are using Readykey ID devices, then present the key/card to the administration reader or type in the keycode. If you are using other ID devices, then you have two choices:

   a. If you have a desktop administration reader or CNC reader, then use the ID device on the reader (e.g. swipe the card, present the tag, read the bar-code etc.).

   b. Enter the code manually: From the drop menu, select **ID Device** - this will present a list of all ID device types recognized by the system. (Additional types can be defined - see Appendix B of this document for information on how to do this.) Select the ID device type required and choose **OK**. You can now enter the site (facility) and serial number codes for the ID device directly into the **Key code** box. To do this type in the 3 digit site (facility) code followed by a dash "-", then type in the 5 digit serial number.

      A listing of the different ID Device types are the following:

      - Readykey (select for systems is using standard Readykey keys and cards)
      - Sensor 2601 (select for systems using Wiegand 26 Bit readers and ID devices)
      - Wiegand 2801 (select for systems using Casi Rusco Wiegand 28 Bit format readers and ID devices)
      - Wiegand 2802 (select for systems using Casi Rusco Wiegand 28 Bit Version 1 format readers and ID devices)
      - Readykey UK Magstripe Reader (select for systems using the European Readykey Magstripe readers and cards)

   Note: Formats other than the above list use the ID Device type of ‘Readykey’.

6. Choose **Add**. The keyholder information will now be stored in the Readykey for Windows database, and the key code and access information will be sent to the door controllers. You can now add further test ID devices in the same way, to make testing of the system easier.

   Note: You can display the total number of personnel or visitors by selecting **Reports**, **Total Personnel**.

7. Choose **Close** to leave the **Personnel** application and return to the **Login** applications.

Note: The **Display Photo ID**, **Grab Photo**, and **Print Card** options only appear if the Photo ID module has been added to the system. Refer to the *Photo ID Module Datasheet* for more details.

Force Dial

Once the test ID devices have been added to the Readykey for Windows system, then the key code and access information will normally be sent immediately to the door controllers. However, if the site is remote, and communicating to a CNC via a dial-up modem link, it may be necessary to force dial the site first, unless the site is still on-line. Follow the procedure described earlier, after the controllers were added using the **Installer** application.

It is probably also a good idea at this stage to verify the communications to the door controllers - if there are problems with communication, then it is likely that the key code and access information will not have reached the door controllers.

Use the **Status** application to confirm there are no communications errors to the site, and, if a CNC is being used to communicate to the site, ensure the display shows *** MONITORING ***

Testing

The programming of the system information for the site being commissioned is now complete.

The next stage is to use the test ID device(s) at each of the readers on the site, and confirm that:

1. The key/card, when used on the reader, operates the lock for the correct time, as programmed in **Installer: Doors**.
2. A transaction is received by Readykey for Windows, and that the transaction information - keyholder and door name, time and date are correct.

The best way to verify the above, is to use the Readykey for Windows **On-line Transaction Display**. This is a part of the **Alarm** application, which is normally started automatically when Readykey for Windows starts. (If this is not the case, then start the **Alarm** application now by double-clicking its icon from the **Login** applications screen.)

Note: If your Readykey for Windows system consists of more than one workstation, then you should use the Readykey Server for this stage, as all transactions for the first division will be displayed on the **On-line Transaction Display** by default.

1. Maximize the **On-line Transaction Display** by double-clicking its icon.

   Note: When commissioning second and subsequent divisions, you will need to set up the transaction routing for the divisions before proceeding. Refer to the On-line Help for information on how to do this.

2. Walk round the site, using the ID device at each reader. Make a written note of the order in which the readers were visited. Confirm that each lock releases for the programmed time, and that the reader LED indicates 'Access Authorized'.
3. Return to the PC and view the **On-line Transaction Display** - use the scroll bars to view all the transactions generated. There should be an 'Access Authorized' transaction for each reader. For readers designated as 'In' and 'Out' by using Lock Sharing or Passback, the transactions should be 'Entry Authorized' and 'Exit Authorized' respectively.
4. Verify the door name for each transaction corresponds with the order in which the readers were tested.
5. If any door names are incorrect, then use **Installer: Doors** to correct the information.
6. If any other transactions are generated, or no transaction is generated for a particular door, then refer to the Troubleshooting section - Appendix A.

7. Once you have successfully tested all readers on a site, you need to repeat the process for other sites in the division, including remote sites using Force Dial, then for other divisions on the system, if applicable.
8. If the site just commissioned communicates via a dial-up modem, then now is the time to return to the **Force Dial** utility in **Installer**, select the site name from the list, and choose **Hang Up**.
9. If your system includes more than one site, or more than one division, then you should refer to the following sections before proceeding.

Personnel

This section explains how keyholders can be given access to more than one site in a division, if required.

Multi-Site Keyholders / Divisional Access Groups

Divisional Access Groups (DAGs) are used to enable keyholders to be given access on more than one site in a division, as described below.

When a keyholder is added, then the list of **Access Groups** given in the **Personnel** application includes the following:

- All defined Access Groups **for all sites in the division**
- All defined Divisional Access Groups **for the division**.

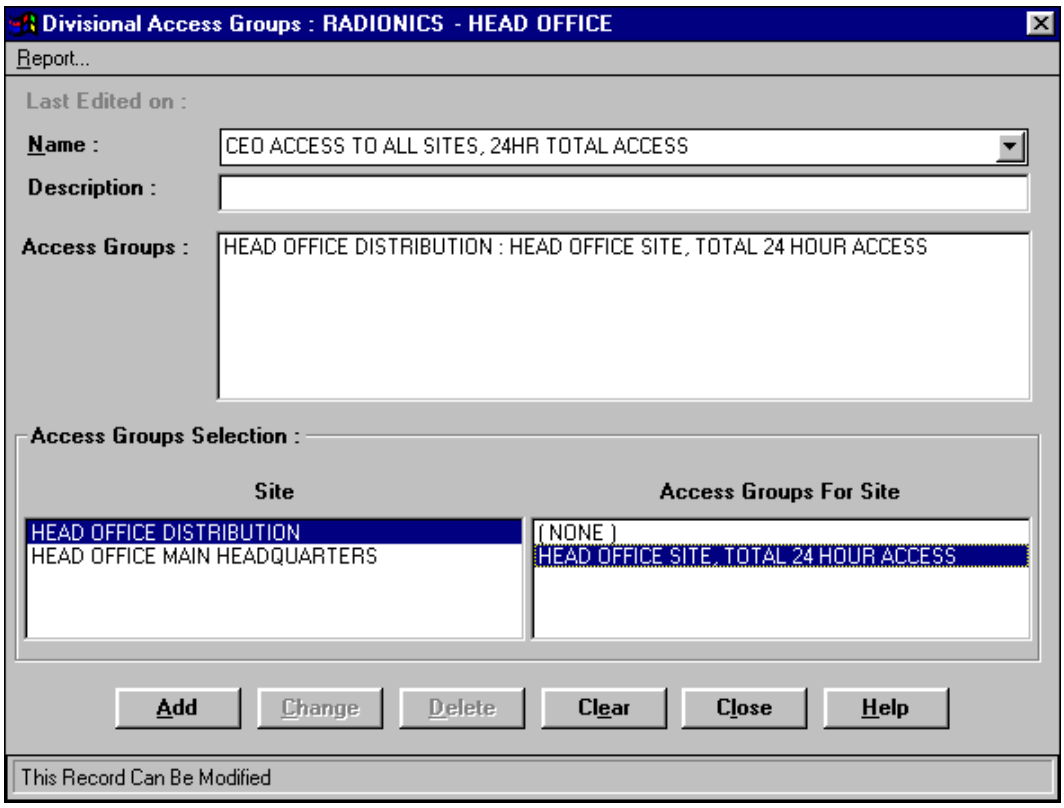
The list can be restricted by the use of Departments and Workgroups - refer to the Readykey for Windows On-line help and System Overview for information on how to use these facilities.

Divisional Access Groups

A Divisional Access Group (DAG) consists of a combination of site access groups. You need to set up the site access groups first (use **Admin: Access Groups**, as described earlier).

As additional sites are commissioned, you should create access groups with complete access throughout the site, then combine these into a single DAG, which can then be assigned to the test keyholder.

Start the **Divisional Access Groups** sub-application by double-clicking the **DAGs** icon from the **Admin** screen.



To create a Divisional Access Group:

1. Enter a unique **Name** for the DAG. Note that a DAG cannot have the same name as an Access Group.
2. Enter a **Description** for the DAG - this can be used to give additional information about the DAG.
3. The **Access Groups** box will be empty at this stage, but will later show which access groups the DAG consists of for each site.
4. In the lower section of the screen (**Access Groups Selection**) you will be presented with a list of **Sites** in the box on the left.
5. Select a site from the list by clicking on it with the mouse. A list of all defined **Access Groups for Site** will appear in the box on the right. This list will include '*None'.* This would be used if, for example a DAG was required to give access on certain, but not all sites - the Access Group for the sites where no access is required would be set to *None.*
6. Select the required access group for the site from the list. The site name and the Access Group selected will now appear in the **Access Groups** box at the top of the screen.
7. The process can be repeated now for other sites, by selecting a new site, then an access group.
8. Choose **Add** when the process has been repeated for all sites where access is required. Repeat the process if you need to create any additional DAGs.
9. Choose **Close** when all required DAGs have been created.
10. DAGs are assigned to keyholders in **Personnel** in the same way as standard access groups. However, they will need to be downloaded to sites when any modifications are made to existing DAGs.

Note: Whenever a change is made to a DAG you must then download that change to all the affected sites. This is done from the **Installer** application by clicking on **Initialize and Download** in the **Utilities** menu. Refer to the downloading section on for further details.

Finishing Off

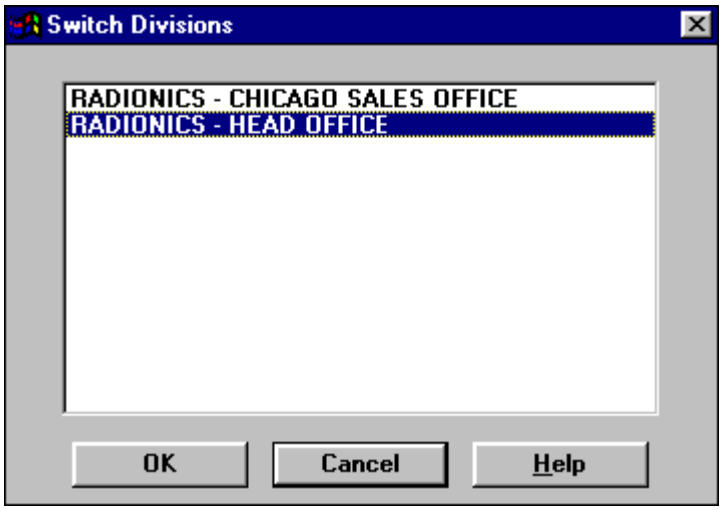
Once a single site has been programmed, tested, and is operating correctly, then the previous procedures can be repeated to create a test Access Group for other sites in the division, then for other divisions on the system, as applicable.

Some system information also needs to be programmed - including time profiles, holidays, the system title, supervisor key/card, and some system operators which will be described later.

Multi-Division Systems

As previously mentioned, you should concentrate on programming and commissioning divisions one at a time. However, you will reach a point when you need to switch from one division to another.

If you have defined more than one division, then on all division-dependent screens an extra drop down menu item will appear - '**Division...**'. Clicking on this menu will bring up the following screen:



- select the division you now wish to view / edit, then choose **OK.**

The name of the division currently being edited is shown on the title bar of 'division-dependent' screens. Once you have changed to a different division, then that will remain the 'active' division throughout Readykey for Windows until you switch division again.

Multi-Division Keyholders

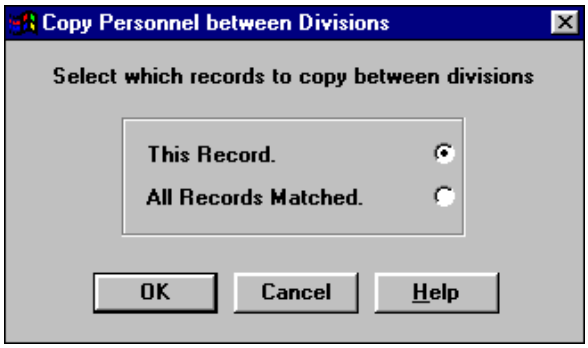
Keyholder information is stored on a 'per-division' basis. Hence if certain keyholders need to have access in more than one division, then they will need to be added to each division separately.

Similarly, if these keyholders are subsequently deleted, they will need to be **DELETED IN ALL APPLICABLE DIVISIONS separately.**

Copying Personnel between Divisions

A special utility in the **Personnel** application allows keyholder information to be copied between divisions, as follows:

1. Search for the keyholder or group of keyholders to be copied by first choosing **Clear**. Then type in the keyholder's Last Name or choose the Access Group for a group of keyholders and choose **Search**. Additional information searching for keyholders can be found by using the On-line Help facility within Readykey for Windows.
2. Select the **Copy Personnel...** drop down menu item in **Personnel**.



3. Select whether to copy just the keyholder displayed (*This Record*) or all keyholders that matched the search information given (*All Records Matched*), and choose **OK**.
4. You will now be asked which division or divisions you wish to copy the keyholder(s) to - select the division(s) required by clicking on them with the mouse, then choose **OK**.

Note: If any of the keyholders being copied already exist in the destination divisions, you will be given a warning, followed by an option to cancel the whole operation, or continue, skipping the duplicate keyholder.

Only certain information will be copied, i.e.:

- Last Name
- First Names
- Personnel Type (Personnel/Visitor)
- Start and End Dates
- Key code
- Photo ID
- Personnel Trace
- Extra Information Fields

Note: If the Extra Information boxes are being used, then you should be aware that the titles of these can be different in different divisions. Hence, when copying keyholders from one division to another, the contents of these could be such that they no longer make sense in the new division - e.g. if the first box was being used to store Home Telephone in the source division, but 'Car Registration' in the destination - the result of a copy operation would be that the 'Car Registration' boxes in the destination division would be filled with the 'Home Telephone' after the copy operation.

The following information will **not** be copied:

- Department
- Workgroup
- Access Group

Time Profiles & Time Periods

Time profiles and Time Periods are available to provide time control over several features of the system:

- Personnel and Visitors may be allowed access to some areas only at certain times of the day or on certain days of the week, restricted to the time periods contained within. Time Profiles and Time Periods to allow access to personnel 24 hours a days, all of the time including Holidays, do not require a Time Period and Time Profile to be created.
- Doors may be unlocked and locked automatically, for instance, a public access door may be unlocked during office hours.
- Alarm points may be active only at certain times.
- A relay on a Door Controller or Alarm Event Manager may be activated at specific times.

Up to 128 time profiles may be created, each with up to 3 time periods. In addition, system holidays, covering times such as Christmas, Easter, public holidays etc., may be defined that override the normal time profiles.

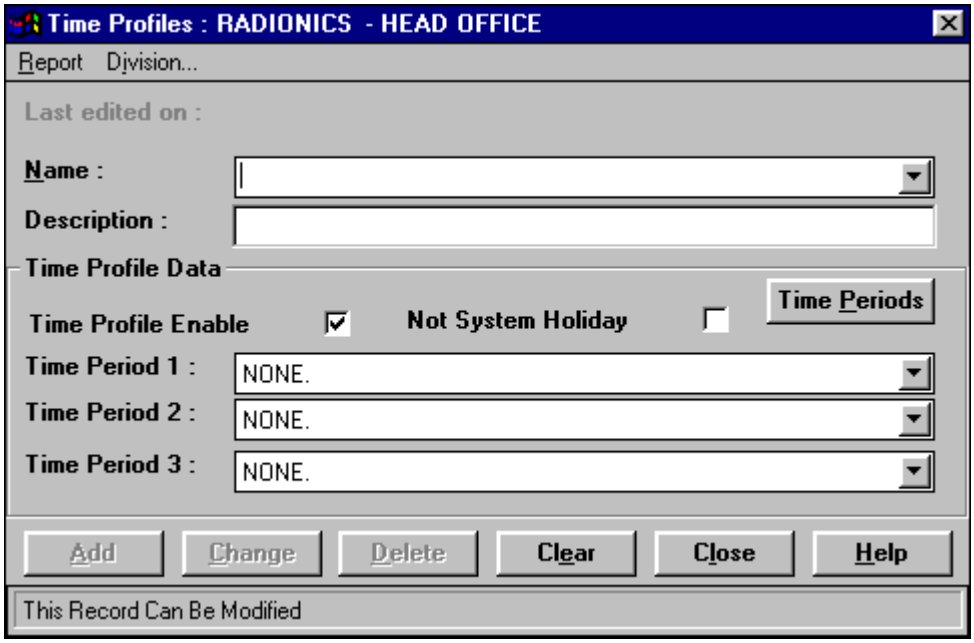
Note: The number of Time Periods and Time Profiles that can be created may be determined by the type of door controller used. All K2100, K1100, and K2000N door controllers, prior to version 3.0 software, are limited to 32 Time Periods and 32 Time Profiles.

Some examples may be:

- Office staff are allowed in the building between 8:30am and 5:30pm Monday to Friday, and 8:30am to 1:00pm Saturday, but not on Bank Holidays, Christmas and Easter.
- Cleaning staff are allowed access throughout a building between 4:30pm and 7:30pm Monday to Friday.
- Night shift staff are allowed access between 8:00pm and 6:00am Monday to Friday.
- A public entrance door is required to unlock automatically at 9:00am and lock again at 5:00pm; it must also be unlocked between 9:00am and 12:30pm Saturday morning.
- An alarm point is to be active only outside normal working hours.
- A door controller or alarm module relay can be active for certain time periods, e.g. to control outside lighting,

If you have no intention of using time control on any feature then there is no need to create any time profiles. Any feature that may be controlled by a time feature will operate 24 hours a day, 7 days a week when no time profile is applied. This means that if a door has no time profile assigned, then a valid key/card will ALWAYS be required to gain access. If a person's access group has no time profile assigned, then they will be able to use their key/card to gain access whenever they wish.

The part of **Admin** that is required at this stage is **Time Profiles** - double-click on the Time Profiles icon.



Before the Time Profiles can be created, the Time Periods must be first be created. Up to 3 Time Periods can be contained within 1 Time Profile.

1. Click onto the Time Periods button on the right hand side of the screen to enter into the Time Period setup screen.

2. Enter a **Name** for the Time Period - this can be used to give additional information about the Time Period. An example would be "9AM-5PM Mon-Fri Use for Public Ent Dr"

3. Enter in a Start Time separating the hours and minutes with a ":". **Note**: Time Periods must be entered into the system using a 24:00 style clock and cannot cross midnight. An example of 9AM would be "09:00".

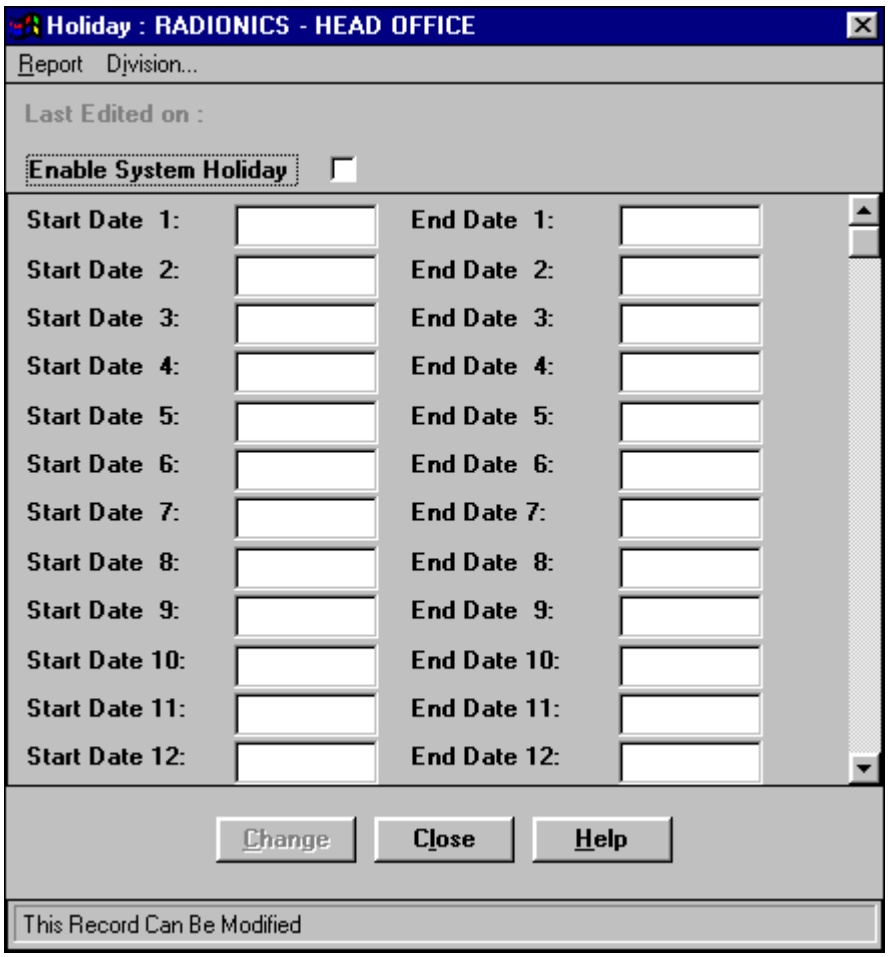
4. Enter in a End Time separating the hours and minutes with a ":". **Note**: Time Periods must be entered into the system using a 24:00 style clock and cannot cross midnight. An example of 5PM would be "17:00".
5. Select the days of the week by clicking onto the boxes on the right of the corresponding days desired for this Time Period to be active.
6. Choose **Add.** Repeat the same process for all the Time Periods required for the system.
7. Choose **Close** when all required Time Periods have been created.
8. Enter the Name of the Time Profile - this can be used to give additional information about the Time Profile. An example would be "Auto Unlock Public Entrance M-F 9am-5pm".
9. Enter the Description, if desired, of the Time Profile to give any additional information.
10. Choose **Time Profile Enable** to turn on and activate the Time Profile. Note: this can be used to 'disable" the Time Profile if required in the future.
11. Choose **Not System Holiday** , only if using K2100/K1100 door controllers revision 3.0 or higher, to disable the Time Profile from being active during a Holiday condition. **Note**: this will prevent doors from automatically unlocking or personnel from obtaining access during specified observed Holiday conditions during the year.
12. Select the Time Period or Time Periods to be contained with this Time Profile by use the down arrow button for **Time Profile 1, Time Profile 2,** and **Time Profile 3. Note**: select **None** for the additional Time Periods 2 & 3 if not used.
13. Choose **Add.** Repeat the same process for the Time Profiles, including the Time Periods within each profile, required for the system.

System Holidays

System Holidays are used as a special override which would normally be used to prevent doors from automatically unlocking by a time profile during an observed Holiday condition. Holidays are also use for restriction of specific personnel that would normally obtain access by a time profile during normal working shifts except during Holiday conditions.

Holidays will only affect Time Profiles or Time Periods that have **Not System Holiday** checked, all other Time Profiles and Time Periods will function as normal.

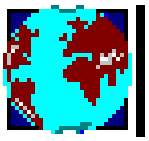
The part of **Admin** that is required at this stage is Holidays - double-click on the Holidays icon.



1. Select **Enable System Holiday** to turn on and activate the System Holiday programming. **Note**: this can be used to 'disable" the Time Profile if required in the future.
2. Enter the Start Date separated by a "/" between the month, day, and year entries.
3. Enter the End Date separated by a "/" between the month, day, and year entries. **Note**: holidays that are observed for only one day of duration must use the same start date and end date to observe a one day holiday condition. The maximum duration of days a single holiday can be observed is 32 days.
4. Choose **Change** after all of the Start and End Dates have been entered.
5. Choose **Close** when finished programming System Holidays.

A total of 20 Holiday Start and End Dates can be entered into the system per division.

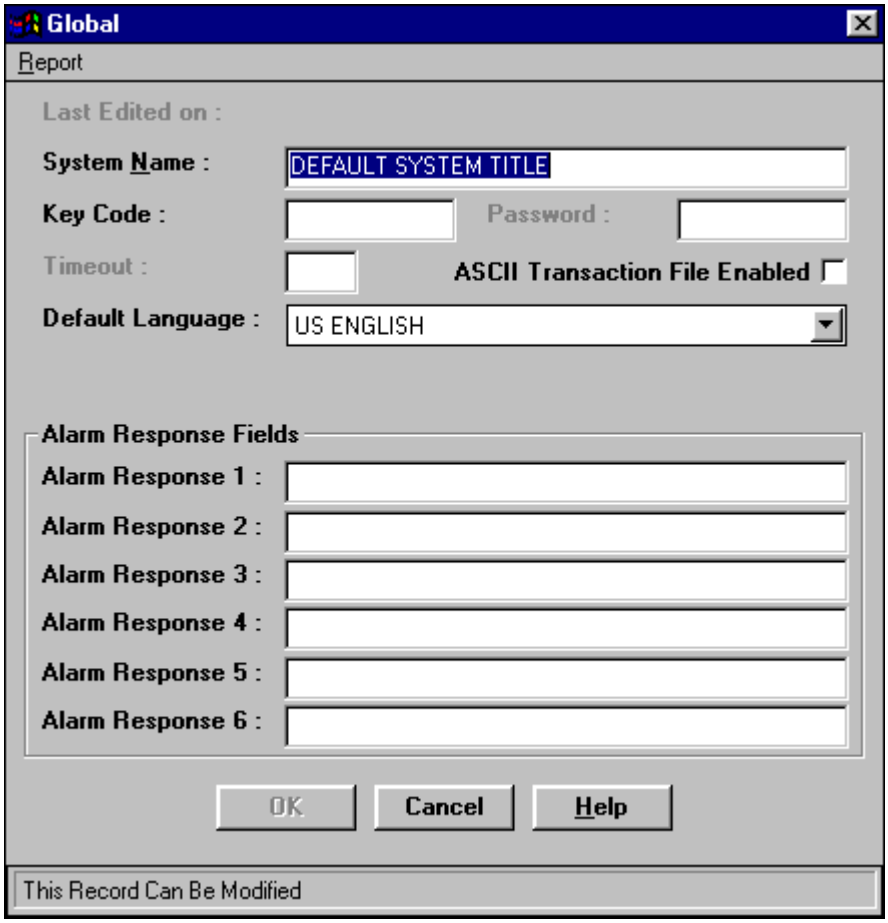
System Information - Global



The system title and supervisor information can be set up from both the **Installer** and **Admin** applications - both of these have a **Global** sub-application. However, some additional information can only be programmed from **Installer**, some from **Admin**.

Installer

Start the **Installer** application from **Login**. Double click on the **Global** sub-application.



1. Enter the **System Name** - this will appear on the main **Login** screen and some reports.
2. Use an ID device that is to become the Supervisor ID with the administration reader. The code will appear in the **Key Code** box. **Note**: the Supervisor ID device will have full authority to view and modify all section of the Readykey for Windows program. For security measures this key or card should be kept in a secure place or remain with the system supervisor at all times.
3. Enter a suitable **Password** - this can be between 2 and 8 characters in length.
4. Enter a **Timeout** between 2 and 60 minutes - if the Supervisor is logged in and the system is left unattended, this is the length of time before which the system will logout the operator and return to the **Login** screen.

   Note: 0 can be entered - if this is done, then the supervisor will **NEVER** be timed out when logged in.
5. **ASCII Transaction File Enabled** - put a cross in this box if you are using this facility - see *Readykey for Windows ASCII Transaction File Datasheet* for further information.
6. **Default Language** - Choose the default language to be used for multiple language systems.

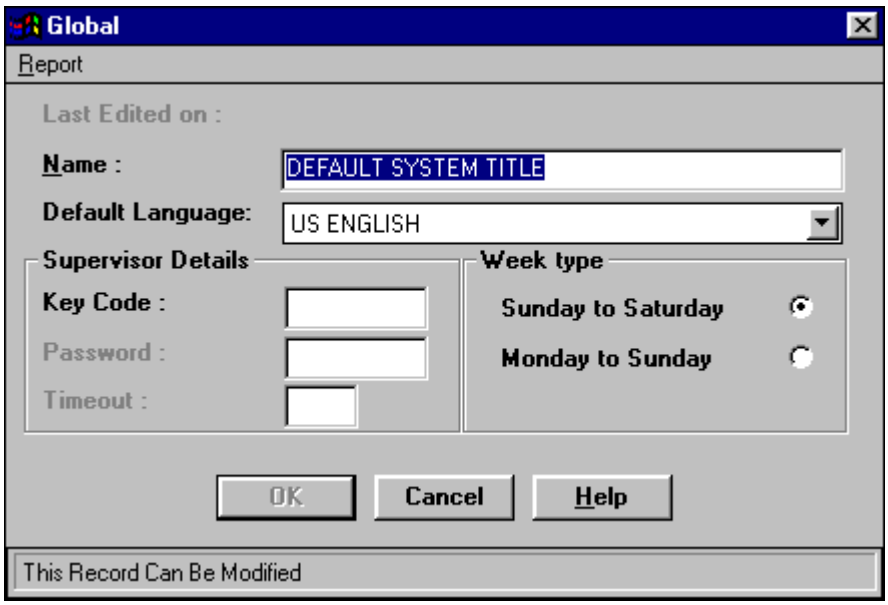
7. **Alarm Response Fields** - these are the possible choices that an operator can use when accepting an alarm, to indicate the action taken in response to the alarm event. Examples might include '*DOOR CHECKED AND SECURED', 'POLICE CALLED',* etc.

8. Choose **OK** when all the information has been entered.

Admin

The System Name and Supervisor key/card information can also be entered from **Admin: Global**. However, an additional option is available here: to decide whether a 'week' runs from 'Sunday to Saturday' or from 'Monday to Sunday'. Within in the **Transaction** application, it is possible to search for transactions that have occurred 'This Week' or 'Last Week' - the appropriate dates to search between are then entered automatically, dependent on the option setting here.

Start the **Global** sub-application from **Admin**.



Select the **Week Type** required, and choose **OK** (or choose **Cancel** if no change was made).

Operators

You will want to set up a number of system operators - these are the people who will administer the Readykey for Windows system on a day-to-day basis.

Note: You should not use the Supervisor Key/Card defined in **Global** for routine administration - you can create an operator key/card, with the same privileges, if required.

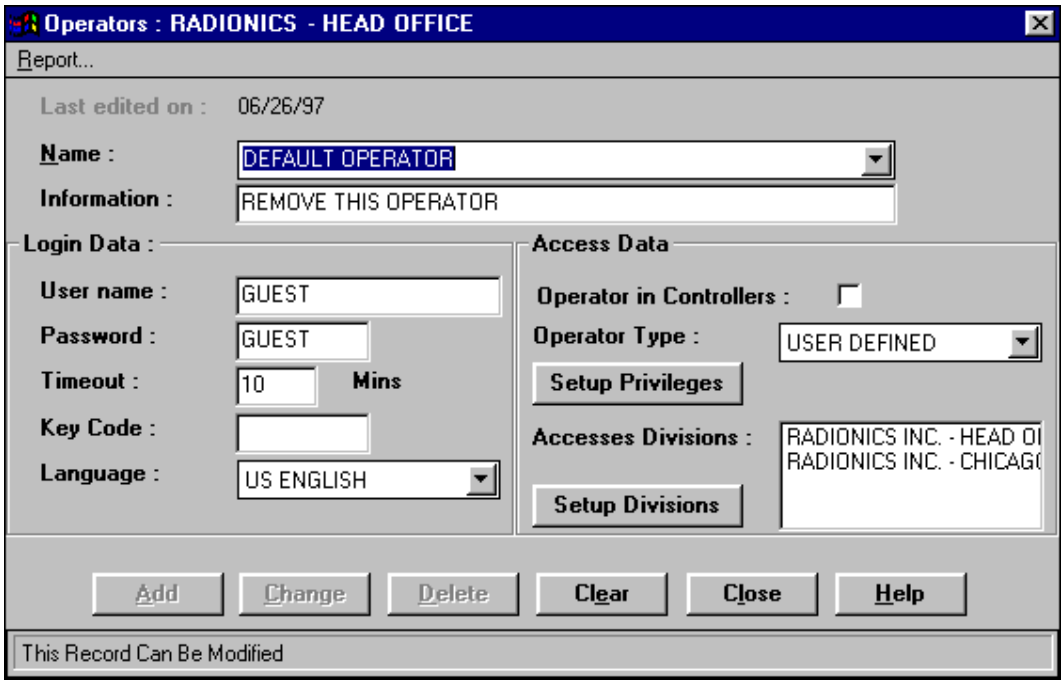
Each operator will have defined some login information - this is required when the operator is logging into the system and accepting alarms; a set of privileges, which define what information in the Readykey for Windows system they can view and/or modify; and a list of divisions, which define which divisions they can view and/or edit, and accept alarms in.

Once you have added and tested your own operators, you will most likely want to remove the *Default Operator* that was supplied with the Readykey for Windows software.

CAUTION: When the default operator is removed, if you forget the passwords or lose the operator tokens, you cannot log into the system. **Always** set up a 'backdoor' operator with a password (without a key/card) for use in case of emergency.

Up to 128 operators can be defined, in addition to the Supervisor created earlier.

Start the **Operators** sub-application from the **Admin** application.



To add an operator:

1. Choose **Clear** to clear the information displayed.
2. Enter a **Name** for the operator - this is used for reference purposes only - the user name used to login is defined later.
3. The **Information** field may be used to describe the operator.
4. **Login Data** - this information is used when the operator logs into the system, and to accept alarms:
    a. **User name** - this is the name the operator will use to log into the system - if an ID device is assigned to the operator, this name will be entered automatically when their ID device is used with an administration reader.
    b. **Password** - an optional password of between 2 and 8 characters may be entered.
    c. **Timeout** - this is the time the operator will remain logged in if there is no keyboard or mouse activity. Enter a value from 2 to 60 minutes.
    d. **Key Code** - if an ID device is to be assigned to the operator, then this code will contain the code of the device. Use an ID device with the administration reader, and the keycode will appear. **Note**: if an ID device has been assigned to the Operator, the Operator must always use the ID device to enter into the system for administration and accepting alarms.

    Note: If non-Readykey ID devices are being used, then the code will be converted to and displayed in the standard Readykey format (8 hexadecimal characters).
    e. **Language** - if multiple languages are being used on the system it is necessary to choose the language this operator will be using while administering the system.

5. **Access Data** - these boxes determine what the functions of the Readykey for Windows system the operator can view/edit/use (the *Operator Privileges*), and in which divisions:

   a. **Operator in Controllers** - this box determines whether this operator can acknowledge alarms at the door and/or network controllers if, for example, the Readykey for Windows system is not running, or, on remote sites where alarms may be initially accepted locally. This option is only to be used for operators that have an ID device assigned for administering the system.

   b. **Note:** A maximum of 32 out of the 128 operators may have this function enabled.

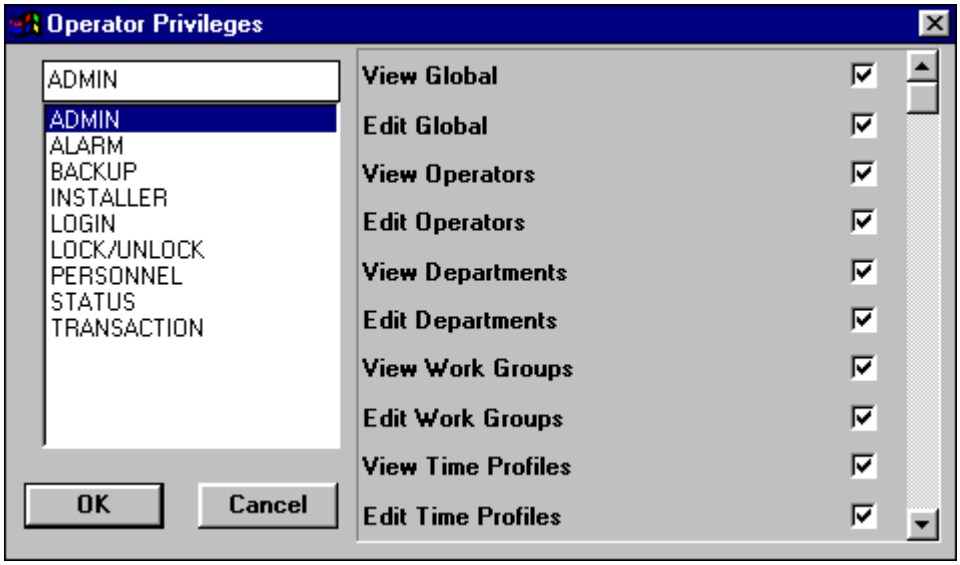
   c. **Operator Type** - these define what the operator is allowed to do within the Readykey for Windows system. Four standard Operator Types are available, or 'User Defined' custom sets of privileges can be defined.

   d. The four standard Operator Types are:

   - **Supervisor -** allowed full access throughout the system.
   - **Administrator -** access to most administrative functions, except **Admin: Operators** (view only) and **Installer**.
   - **Operator -** access to edit **Personnel** only, accept alarms, and to view most **Admin** settings.
   - **Guard -** accept alarms, use **Lock / Unlock** and **Status** only.

   Note: A full list of privileges for each standard operator type is given in the Readykey for Windows On-line Help.

   If different privileges are required to one of the standard types, then choose **Setup Privileges:**

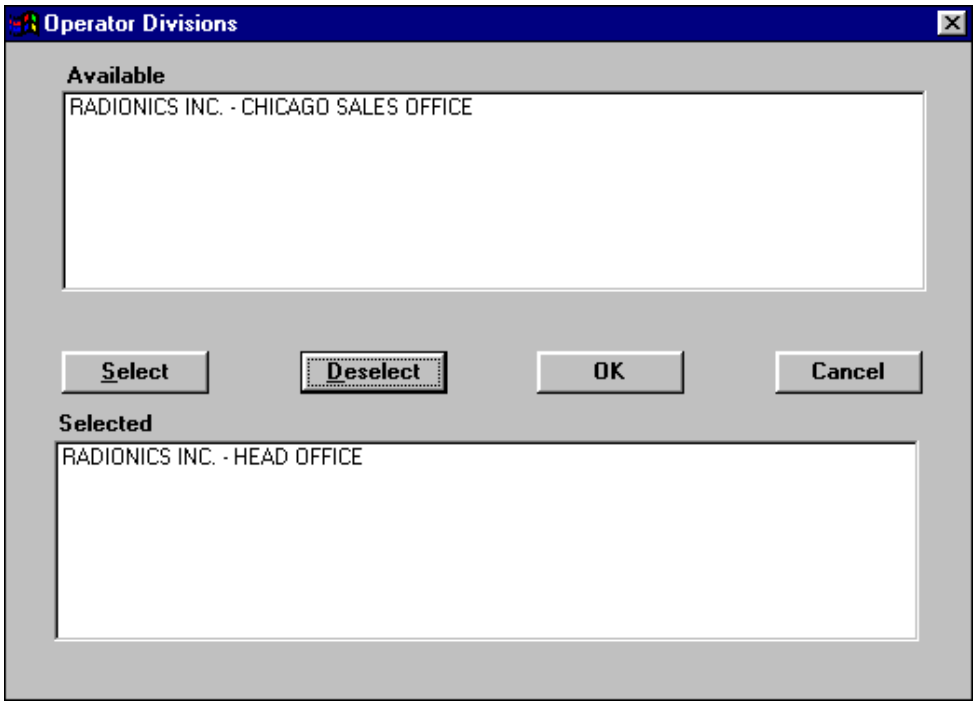


   Select one of the Readykey for Windows applications from the list on the left, and the privileges available will be displayed on the right. Amend the privileges as required, and repeat for other applications. Choose **OK** when the desired privileges have been selected.

   Notice that the **Operator Type** has changed to *User Defined*.

6. If you have more than one division on your system, then each operator can be restricted in which division(s) they can view/edit/use functions of the Readykey for Windows system.

Choose **Setup Divisions** to assign the divisions to which this operator has access.



This screen works in a similar way to the one in **Admin: Access Groups** to set up the lists of areas. A list of all defined divisions appears in the 'Available' box at the top. Select the divisions to which the operator is to be given access, and choose **Select**. The divisions selected will move to the 'Selected' box at the bottom. Choose **OK**.

7. The operator information has now been set up - choose **Add** to save the information. Repeat for additional operators as required.
8. Before deleting the *Default Operator*, it is a good idea to test the new operators that have been added. Return to the **Login** applications screen and choose **Logoff**. Now try to login with each of the new operators (including the Supervisor key) and confirm that they operate correctly.
9. To delete the Default Operator, return to **Admin: Operators** and select the operator from the list by clicking on the arrow to the right of the **Name** drop-down list. Choose **Delete**. Choose **Yes** when prompted to confirm the deletion.

Alarms / Transactions

On large Readykey for Windows systems, particularly those with more than one division or site that are being administered from more than one workstation, you may want to configure the system so that alarms and transactions for different divisions and/or sites are displayed and/or printed at different workstations.

The **Transaction Routing** sub-application in **Admin** defines the behavior of all Readykey for Windows transactions. Using this feature, different transactions can be programmed to behave in different ways on different workstations at different times of day.

For example, during office hours you may decide that you require only alarm transactions to be displayed and printed on a workstation in the company reception. Outside office hours, however, you may require all transactions to be displayed and printed only at a workstation in the 24-hour manned security lodge.

If your system includes more than one division or site, then it possible to extend this facility within the **Alarm** application on each workstation so that only transactions and alarms for individual or groups of sites and divisions are displayed and printed at that workstation.

Hence, if you have two different workstations, in two different locations, where each location is a separate division within Readykey for Windows, then you can configure Readykey for Windows such that only alarms and transactions from the 'local' division are displayed and printed at the 'local' workstation.

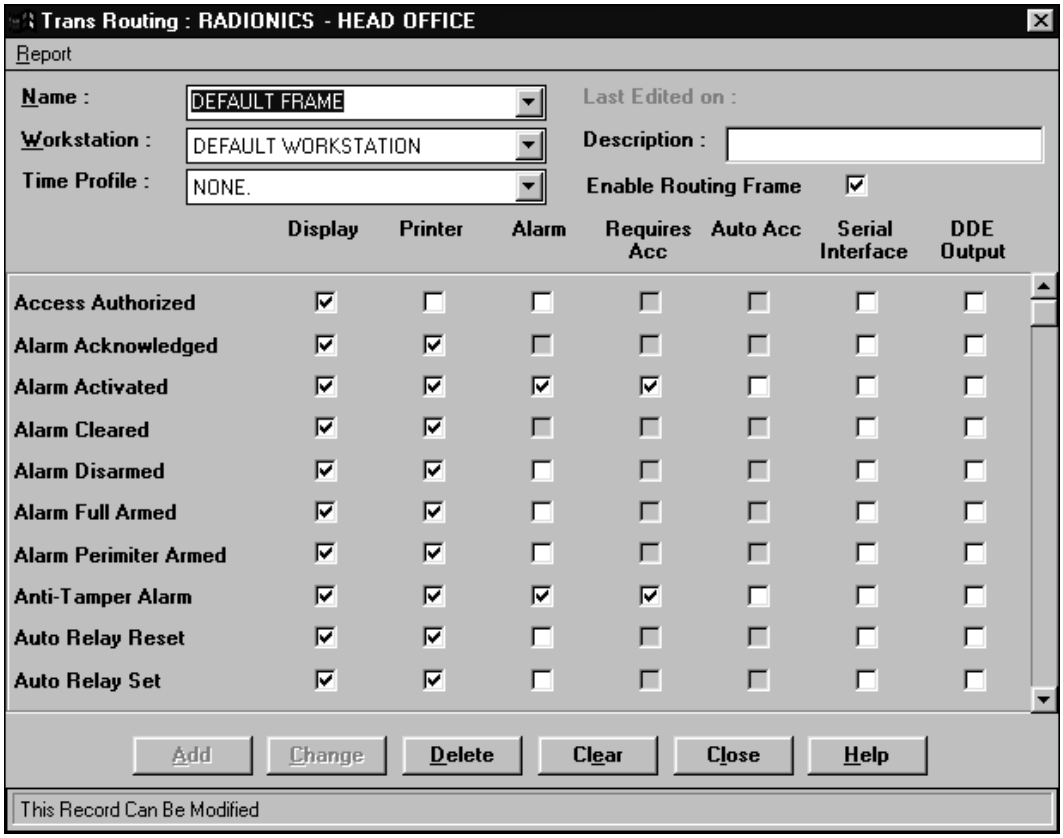
Note: Transactions from all divisions can be searched for from any workstation, regardless of configuration.

Transaction Routing

As previously described all transaction types can be customized to control what is printed, causes alarm conditions, outputs to the DDE, and what event go to the on line transaction display.

The way these events are configured is by creating **Transaction Routing Frames**. A total of up to 128 routing frames can be created, which may also be time profile controlled. Additionally, the routing frames control which workstation these events will be sent too.

The part of **Admin** that is required at this stage is **Trans Routing** - double-click on the **Trans Routing** icon.



1. Enter a **Name** for the routing frame or choose Clear to create a new routing frame.
2. Select the **Workstation** that this routing frame will control.
3. Select a **Time Profile** if this routing will only be active within specific times/days. Use 'None' if the routing frame is to be active 24 hours a day on all days.
4. Enter in a **Description** for the routing frame, if desired.

5. Choose **Enable Routing Frame** to turn on and activate the Routing Frame programming. Note: this can be used to 'disable" the Routing Frame if required in the future.

6. A list of all the different transactions that may occur is shown on the lower half of your screen. Not all transactions in this list may be applicable to your Readykey for Windows system. Beside each one are 6 check boxes:

   a. **Display**. Any transactions marked here will be displayed on the screen in the On-Line Transaction Display if the Alarm application is running on the workstation. If you send all transactions to the on-line display then you may reduce the performance of your system.

   b. **Printer**. This refers to the on-line transaction printout - again, routed transactions will only be printed if the Alarm application is running on the workstation. The On-line Transaction Printout is a continuous record of events as they are received by Readykey for Windows.

   c. **Alarm**. If this box is checked then the transaction will be treated as an alarm, and will appear in the alarm queue(s). The next two check boxes determine how the alarm will be treated when it occurs.

      The following types of transactions cannot be set as alarms:

      i) Alarm Acknowledged

      ii) Alarm Cleared

      iii) Duress Acknowledged

      iv) Override Alarm Accepted

      v) Override Alarm Reset

      vi) Zone Restored / Rearmed

      vii) Zone Tamper Accepted

      viii) Zone Tamper Cleared

      ix) Zone Trouble Accepted

      x) Zone Trouble Cleared

   d. **Requires Acceptance**. The alarm will need to be accepted by an operator with the privilege to do so. The alarm transactions above should all require acceptance.

   e. **Automatic Acceptance**. Alarms can be set to be accepted automatically. In which case they are still recorded as alarms but require no acceptance. This may be a useful feature to operate when the system is unattended, the printout can be examined or the alarm history can be viewed to see if any alarms had occurred.

   f. **Serial Interface** – is a special module that may be added to your Readykey for Windows system. The Serial Interface output allows for other third party applications to receive and process selected transactions, for example CCTV camera control or building management package. The Serial Interface will only operate if the Alarm application is running on the workstation. Refer to the *Serial Interface Output Module Datasheet* for more details on this feature.

g. **DDE Output** - DDE (Dynamic Data Exchange) is a special facility that can be used by Windows-based applications to communicate with each other. The Readykey for Windows DDE Output facility allows other third-party applications to receive and process selected transactions, for example to a dedicated time and attendance, CCTV camera control or building management package. The DDE Output will only operate if the Alarm application is running on the workstation. Refer to *Readykey for Windows DDE Output Datasheet* for detailed information on this feature. If you are not using the DDE Output, then leave these boxes empty for all transactions.

7. Select **Add** to add the new Transaction Routing Frame, or choose **Change** to modify the existing Default Routing Frame.

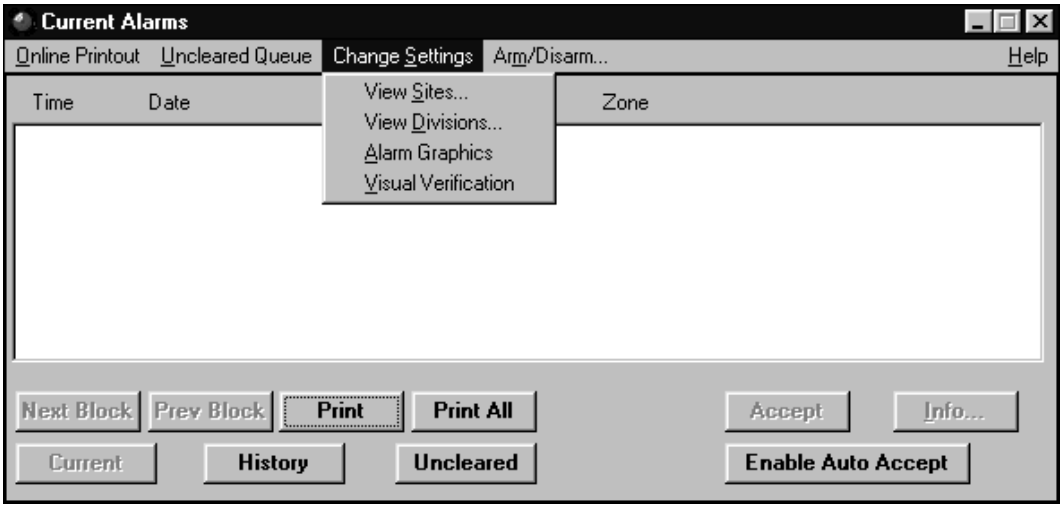
8. Select **Close** after all desired Routing Frames have been created.

Divisions / Sites to View / Alarm Graphics

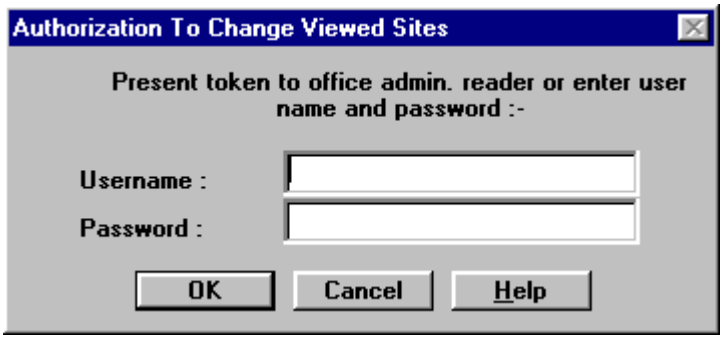
In the **Alarm** application, it is possible to configure the system so that alarms and transactions from only a limited number of divisions and sites are displayed, printed and enunciated for each workstation.

These settings are in addition to the Transaction Routing information.

The configuration of these settings is performed by using the **Change Settings** drop down menu within the Alarm application.

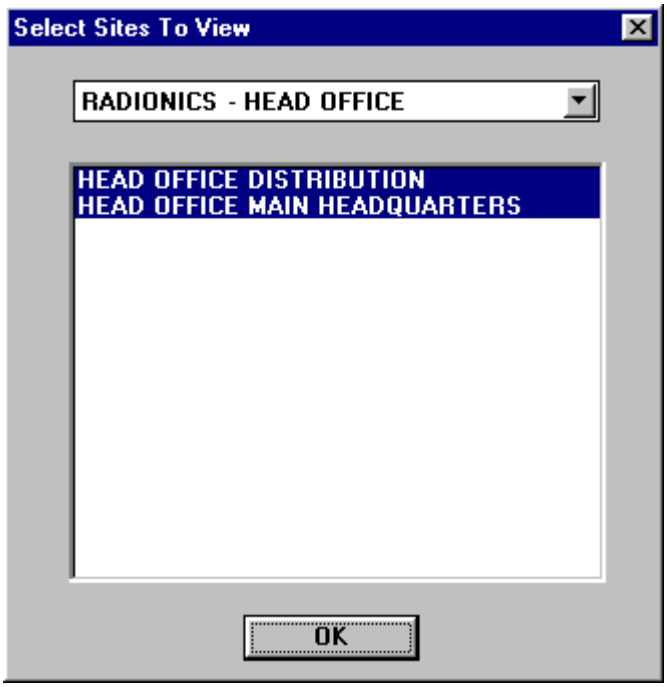


You will then be presented with a security clearance screen know as an **Authorization To Change Viewed Sites** verification.



Enter your **User Name** and **Password** and click on OK.

If your Operator Privilege allows you to change this information, the next **Selected Sites To View** screen will appear. Otherwise you will receive a message stating that your Operator does not have the Privilege does not allow this function of the system.



Select the Sites to view by clicking on each and then choosing OK.

You will now return to the Alarm application.

Repeat the same steps to configure **View Divisions, Alarm Graphics**, and **Visual Verification**.

Completing the Installation

The Readykey for Windows installation now needs to be completed by programming the following:

- **Door Controller Relays, K2015 Alarm Modules / K2015A Alarm Event Managers**, if these are being used. Use **Installer: Controllers: Outputs** and **Installer: Alarm Modules**.
- **Time Periods / Time Profiles** - if required. Use **Admin: Time Profiles**.
- **Access Groups** - restricting access to a limited number of areas on the site(s), possibly incorporating Time Profiles to restrict access to certain times/days. Use **Admin: Access Groups**.
- **Divisional Access Groups** - if you have a multi-site system, you may need to allow some keyholders access to more than one site. Use **Admin: DAGs**.
- **Departments/ Workgroups -** these should be used to make keyholder management easier. Use **Admin: Departments** and **Admin: Workgroups**.
- **Personnel** - add ID devices and assign departments, workgroups and access groups to each keyholder. Enter the Extra Information and Extra Access for each keyholder if these facilities are being used.
- **Doors** - assign Time Profiles to any doors that are to lock and unlock automatically at certain times of day. Use **Admin: Doors**.
- **System Holidays -** define the dates of public and company holidays, so that doors which normally automatically lock and unlock do not, and keyholder's access is restricted. Use **Admin: Holiday**.
- **Transaction Routing** - set up how each workstation is to handle the different types of events on the system. Use **Admin: Trans Routing**.

Information on installing and programming Door Controller Relays, K2015 Alarm Modules and K2015A Alarm Event Managers is included in the Reference Section. Information on all the above is included in the On-line Help.

Finishing Readykey for Windows

In order to continuously monitor alarms and to print events as they happen, Readykey for Windows should never be shut down. However, when you have finished using the system to make changes then you should always log off.

If you do need to shut down Readykey for Windows, such as before switching off the PC, or when you do not want continuous monitoring, then refer to Closing Down Readykey for Windows described later in this section.

If you shut down Readykey for Windows completely, then alarms will still be enunciated at the CNC or door controllers.

Logging Off

Return to the **Login** applications screen and choose **Logoff** from the menu bar. You will then be returned to the **Login** screen. The **Engine** and **Alarm** (if running) will continue to operate and, if there is an alarm event, will bring up a dialog box on top of whatever Windows application is active.

Remember: When nobody is using Readykey for Windows the **Login** screen should be displayed. For Readykey for Windows to monitor alarms it must be running in the background - the **Engine** icon should be moving all the time, on Windows 3.1 or 3.11 systems only, and the **Alarm** icon should be on the screen as well.

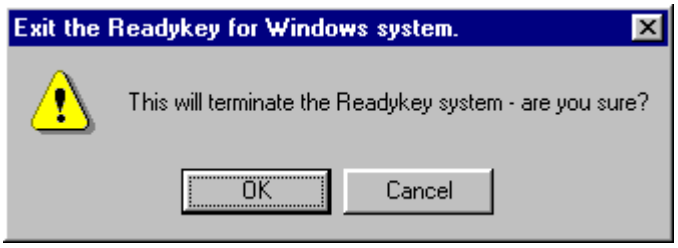
Closing Down Readykey for Windows

Note: The ability to close down Readykey for Windows can be restricted to certain system operators through the use of Operator Privileges.

To close Readykey for Windows completely you need to log out, if you are not already logged out. With the **Login** screen displayed you should:

1. Enter your **User Name**, or use your operator ID device with the administration reader.
2. Type your **Password**.
3. Choose **Shut down**.

This will bring up the following screen:



Choose **OK** to close down Readykey for Windows, **Cancel** to return to the **Login** screen.

Multi-PC Systems

If the Readykey for Windows system is administered from more than one workstation, then one of these workstations will be designated the Readykey Server - this will have the Readykey for Windows security block installed.

It is recommended that Readykey for Windows is never closed down on the Readykey Server, as this will prevent operators starting Readykey for Windows on other workstations, and some parts of the system may not operate correctly.

The above is especially important if the network is a peer-to-peer network - in this case the Readykey Server will have all the Readykey for Windows database files stored on its hard disk - the workstations will not be able to access these files unless the Readykey Server is running Windows.

For additional information, refer to Readykey for Windows Multi-PC Installation Manual and the Network Operational Overview and Requirements document.

Reference Section

This section is not designed to cover all the steps necessary to configure a complete Readykey for Windows system. It should be used in conjunction with the Quick Installation section of this document, and provides supplemental or additional information that will assist installers new to Readykey for Windows, or where more detailed information might be required for some stages of the installation.

Starting Readykey for Windows

When Readykey for Windows starts up, several different activities occur, these may result in error messages if some items, such as a CNC or PC Interface Kit, are not connected as expected. Most of these error conditions are described below.

If the PC is running Windows 3.1 or Windows for Workgroups 3.11, then from the **Windows Program Manager Readykey for Windows** is started by double-clicking its icon.

If the PC is running Windows 95 or Windows NT, then, from the **Start...** button, choose **Programs...**, then choose **Readykey for Windows.** Two items should be shown - the **Readme** file and the **Readykey for Windows** program itself. Choose this and Readykey for Windows will start.

Note: This manual assumes the PC is running Windows 95 or Windows NT. Some descriptions of activity may not apply to or be different from Windows 3.1 or Windows for Workgroups 3.11. Consult the Windows documentation if you require assistance on starting programs within your specific Windows environment.

Once you have started Readykey for Windows, several different processes will occur. These are now described in detail:

The Engine

Firstly the **Engine** will start up and appear of the task bar. The Engine icon is animated for Windows 3.1 and Windows for Workgroups 3.11, indicating that the application is alive and working. The Engine operates continually in the background while the system is running. All communications between the Readykey for Windows administration system and the door controllers, through a CNC or PC Interface Kit, are controlled by the **Engine**. If you make changes to personnel, for instance, the **Engine** passes those changes to the correct door controllers via the CNC or PC Interface Kit. Similarly, events that occur at the door controllers are collected from the CNC or PC Interface Kit by the **Engine** and are then passed to the **Alarm** application for processing.

Alarm

Current Alarm Queue

Next the **Alarm** application may start automatically. This is the application that monitors incoming events from the system and determines whether they should be printed, sent to the On-Line Transaction Display or treated as an Alarm. A function of the **Admin** application called **Transaction Routing** allows the user to decide whether individual events are printed, displayed or treated as an alarm.

During the software installation process on each PC, you will be asked if you require the **Alarm** application to start automatically when Readykey for Windows starts. If you choose not to start **Alarm** on a particular workstation, then no transactions will be processed (displayed, printed, or generate an alarm event) on that workstation.

If you choose not to start **Alarm** automatically when Readykey for Windows starts, then the **Alarm** icon will appear on the **Login** applications screen when you have logged in.

On-line Transaction Display

This is part of **Alarm**

. It starts at the same time and displays transactions on the screen as well as the printer. You can select which transactions appear on this display by using **Admin: Transaction Routing**.

Remember that the **On-line Transaction Display** will only be available if the **Alarm** application is running on this PC.

The On-Line Transaction Display will only store events while the display is open, prior events will not be stored within the display. Prior events can be recalled by using General Search within the Transaction applications.

Alarm Graphic

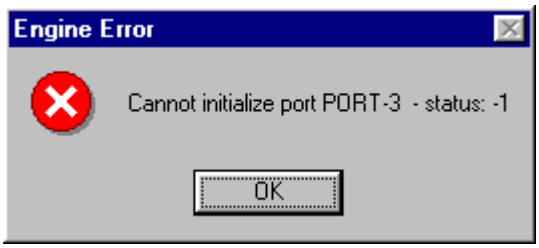
This is also part of **Alarm**, and allows graphics associated with alarm events to be viewed. Alarm Graphics are assigned to doors (via **Installer: Doors**) or Alarm Module/Alarm Event Manager Inputs (via **Installer: Alarm Modules: Inputs**).

For more information on setting up Alarm Graphics refer to Readykey for Windows Help facility or the *Alarm Graphics Datasheet*.

Startup Messages

Some or all of the messages below may appear during the startup process:

Comms Port Error



First Time Installation

If the Engine cannot find a CNC or PC Interface Kit in **COM1:** then it will give an error similar to the one shown above. Even if you have connected a CNC or PC Interface Kit to **COM2:** you will still get this error. Choose **OK**, and the start-up process will continue. Use **Installer: Masters** to change the Comms Port.

Other Occasions

If this error appears at any time after Readykey for Windows has been operating normally, then it may indicate:

- The COM port has been reassigned in **Installer: Masters**.
- Another device, such as a mouse or modem, has been assigned to the COM port.
- The CNC, PC Interface Kit or COM port in the PC has failed.

Deleting Old History Transactions

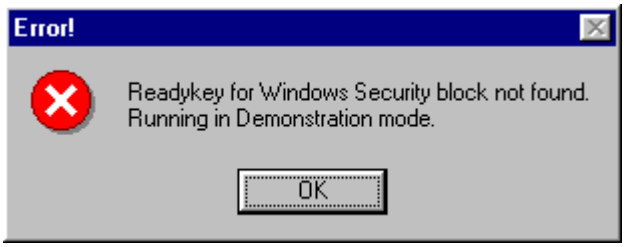
One of the features of the Alarm application is the **History Queue** of alarm events. This provides a quick reference to recent alarm events, restorals and acknowledgments. When Readykey for Windows starts up for the *first time each day* or *just after midnight each night*, transactions older than seven days will be removed from this list.

The following message will appear when this activity occurs:

Again, this message will only be displayed if the **Alarm** application is running on the PC.

Security Block Not Found

If no Security Block (Dongle) is connected to the LPT1 parallel port of your PC, or for some reason it is not detected, then the following message will appear:



Press **OK** to carry on in Demonstration Mode, or see Appendix A: Troubleshooting for advice on why the Security Block may not be detected.

Logging In

When the **Login** screen has appeared, you need to log in to gain access to the system. Access to the system is controlled by means of system operators. Each operator has a user name and a set of 'privileges' assigned, which determine which parts of the system that operator can view and/or edit. A key/card and/or password may also be assigned to enhance security.

When Readykey for Windows is first installed, no **System Operators** have been created. In order to gain access to the system for the first time there is one operator defined, the Default Operator. This operator has full access to the whole system, and no key has been assigned. You can therefore enter the system as follows:

1. Type **GUEST** in the **User name** box.
2. Press the **TAB** key (or click in the **Password** box).
3. Type the password - **GUEST**. As you type each password character, a * will appear on the screen preventing anybody observing what you have typed.

Note: Unlike previous DOS Readykey systems you should **not** press the ENTER (or RETURN) key after typing in an item of information. Instead use the TAB key to move from one item to the next, Shift-TAB (pressing TAB with the Shift key pressed) will move to the previous item. If you press ENTER in a Windows dialog box it will usually interpret this as if you had pressed the default button (a button with a darker surround than the others) - often **OK**, or, in this case, **Log in**.

Now choose **Log in** with the mouse, or just press **Enter** (as **Log in** is the default button in this dialog box, pressing **Enter** is the same as choosing **Log in)**.

Note: Now that you have started Readykey for Windows you have access to the On-Line Help. Just choose **Help** either from a button or from a drop-down menu for immediate help relevant to the function you are currently performing. Pressing the **F1** key will also summon the On-line Help.

Warning: The Default Operator only exists on new installations and may not be a valid operator on existing systems. If this operator has been removed on an existing system, contact the system supervisor to obtain the key or card to log into the system.

The Applications

You have just logged-in. You will now be presented with all the Readykey for Windows **Applications**. Normally you will only see the applications your **Operator Privilege** allows you to use. One special case is the **Alarm** icon which will only appear if you have chosen NOT to start **Alarm** automatically when Readykey for Windows starts.

As the Default Operator has full access to all areas of the system all icons are available.

Installer

At this stage the application you will be using is **Installer**. This has a set of sub-applications that will appear as another set of icons.

First choose **Installer** by double clicking its icon.

The **Installer** sub-applications will now be shown. The **Installer** application is used to define all the hardware (PCs and Readykey equipment) on your system.

Divisions

You will understand from reading the *Readykey for Windows System Overview* the concept of 'divisions'. Most Readykey for Windows systems will only have one division. However, larger systems may have additional divisions defined, each with its own database of sites, door controllers, doors, access and personnel information.

This part of the **Installer** application allows you to define the divisions on your system, and to specify certain division information, such as the types of door controller and default ID device in use, and the titles of the 20 items of extra information that can be stored with each personnel record in the division.

The maximum number of divisions available on your system is programmed into the Readykey for Windows security block - additional divisions (up to a maximum of 128) may be purchased if required.

The information for the division supplied as part of the default database needs to be changed to accurately reflect the first division on your system. Other divisions may be added as required later.

Note: A division consists of one or more sites; the number of divisions cannot therefore exceed the total number of sites on a system.

Oldest Controller

You need to tell Readykey for Windows the oldest type of controller you have in each division. The choice made here affects the quantity and availability of certain features available within the division:

Key to table:

- **Personnel per division** - Maximum number of Personnel per division
- **AGs/DAGs** - Number of Access Groups per site/Divisional Access Groups per Division
- **Extra Acc?** - Extra Access available for Keyholders?
- **Time Profiles/Time Periods** - Maximum Time Profiles/Time Periods per Division
- **Start/End Dates** - Start and end dates available on all keyholders? (See note below).

Oldest Controller (newest listed first)	Personnel per division	AGs	DAGs	Extra Acc?	Time Profiles / Time Periods	Start/ End Dates?
K2100/K1100 Version 3.0 or higher and 18,000 Personnel	**18,000**	**128**	**256**	**Yes**	**128**	**Yes**
K2100/K1100 Version 3.0 or higher	**10,000**	**128**	**256**	**Yes**	**128**	**Yes**
K2100/K1100 Version 2.1 or earlier	**10,000**	**128**	**128**	**No**	**32**	**No**
K2000-N	**10,000**	**128**	**128**	**No**	**32**	**No**

Note: Start End/Dates on all keyholders - within the **Personnel** application, it is possible to restrict the dates between which a keyholder' s ID device will be valid. On all door controllers it is possible to program up to 750 'visitors' in this way. However, when the door controllers in the division are K2100/K1100 with Version 3.0 software or later, then all keyholders may have a start and end date programmed for their access, **both** personnel and visitors.

Warning: It is important to correctly set the **Oldest Controller** option. If this option is incorrectly set, then some parts of the system may not operate correctly. For example, if you set the option to 'K2100/K1100 with 18,000 Personnel' and have one or more standard K2100/K1100 controllers on the system, then you will be allowed to add 18,000 personnel to the division. However, personnel 10,001 to 18,000 will not be recognized by the standard K2100/K1100 controllers, and will not be allowed access through doors on those controllers.

Door Controller Types

K2100/K1100

They can be configured to operate in one of four different 'modes', or system types, two of which are used on Readykey for Windows systems - 'master' and 'slave'.

K2000-N

K2000-N controllers can only be used in place of K2100/K1100 controllers in 'slave' mode. They cannot be used as 'master' controllers.

Upgrading Controllers

It is possible to upgrade or update certain controllers to overcome some of the limitations described above, as follows:

- **K2000-N** - these controllers can be upgraded to a standard K2100 using the Upgrade Kit, part number K2105, or to a K2100 with 18,000 personnel using the 18,000 Personnel Upgrade Kit, part number K2105-18K.
- **K2100 / K1100** - these can be updated to the latest software version, using the K2100/K1100 Software Update Kit, part number K2199.
- Alternatively, they can be upgraded to a K2100/K1100 with 18,000 personnel using the 18,000 Personnel Upgrade Kit, part number K2105-18K.

Default ID Device

Readykey for Windows allows different types of ID device (Readykey proximity, Wiegand-compatible or Magnetic Stripe card, etc.) to be used.

When non-Readykey ID devices are being added the code of each device can be programmed into Readykey for Windows by using a desktop administration reader, or by entering the code directly.

The purpose of this setting is to define the default type of ID device when adding personnel in this division.

Refer to Appendix B - Using non-Readykey ID devices for further information.

Masters

A ‘Master’ is a term used to describe either a K2100/K1100 controller which is connected to the serial port of a workstation either directly or via a PC Interface Kit, or a Readykey CNC. Readykey for Windows supports 3 types of masters - K2100/K1100, Single Site CNC and Multi-Site CNC.

Note: Radionics previously supplied two versions of the CNC - Single Site (SS) and Multi-Site (MS). Only the latter can be used to communicate to sites using RS-232. The SS CNC was discontinued in Spring 1995 - all CNCs supplied since then will be MS.

Readykey for Windows supports up to 20 masters. Each master will be used to communicate to one or more sites on the system. Each master will be physically connected to a workstation on the system. Some workstations may have one or more masters, whereas some workstations will not have any masters connected.

Each site on the system will communicate with the Readykey for Windows software through a master controller.

Sites from different divisions may communicate via the same master.

It should be noted that K2100/K1100 controllers may operate as a master in one of two ways:

- Local Master - connected either directly to a workstation or via a PC Interface Kit
- Remote Master - communicating to a CNC via RS-232. Masters of this type are not defined in Readykey for Windows - only the CNC itself.

The CNC includes a reader for administering Readykey keys. The PC Interface Kit is available with a Readykey Desktop reader. A Readykey Wiegand Interface may be used in place of the normal Readykey Desktop reader with the corresponding wiegand reader for administration purposes.

It is recommended that you configure and establish communications with masters one at a time.

Communications Methods

Communications to the door controllers from the master may be via the Readykey Six Wire Bus or RS-232.

Further information on these methods is contained within the *Central Network Controller Installation Manual*.

Six Wire Bus

The Six Wire Bus is Readykey's own communications medium. This uses 6 core unscreened signal cable, 0.22mm^2, to connect the CNC and/or door controllers.

The distance between any two items on the bus must not exceed 1500ft/500m, and the overall bus length must not exceed 3000ft/1km.

The Six Wire Bus (6WB) can be extended by using a K21232 Six Wire Bus to RS-232 converter (6WB/RS-232). Once converted to RS-232 alternate methods of direct line communication can be achieved. The most common would to use fiber optic drivers, which can extend the 6WB up to 30 miles. Other methods such as line driver or short haul modems can also be used with the K21232 to accomplish extended distances of the 6WB. Refer to the K21232 Installation Instructions manual for more details on use of the K21232.

CNC

Up to 32 Readykey door controllers may be connected to a CNC on a Readykey for Windows system using the Six Wire Bus. Only one six wire bus is available on each CNC.

All door controllers connected to the six wire bus are designated as 'slaves', the CNC itself being the master controller.

PC Interface Kit/Direct

One of the door controllers is connected to the PC via the PC Interface Kit or directly via RS-232 (described later). This door controller becomes the 'master' controller.

Up to seven additional 'slave' door controllers can then be connected to the master via the Six Wire Bus.

RS-232

RS-232 is a standard communications format. Normally this has a limit of 30ft/15m. However, a variety of equipment (modems, fiber optic drivers, line drivers etc.) may be used to extend this distance.

CNC

The CNC has 3 ports for RS-232 communication to door controllers. The communication from the PC to the CNC is also RS-232. If a dial-up modem is connected to a port, then the same modem may be used to communicate to different sites.

PC Interface Kit

The PC Interface Kit communicates to the PC via RS-232. The administration reader and link to the Master K2100/K1100 door controller connect to the PC Interface Unit, which in turn connects to the PC.

Special line drivers are used to boost the RS-232 signal from the PC Interface Unit to the door controller. One of the line drivers is incorporated into the Interface Unit itself, the other plugs into the K2100/K1100 RS-232/Printer port.

Direct Connection - PC to Master Door Controller

It is possible for a Master K2100/K1100 door controller to be connected to a PC directly, without using a PC Interface Kit or CNC, via RS-232.

PC Serial Ports

Most PCs are supplied with two **Serial Ports**. Usually one will have a 25-pin male connector, and the other a 9-pin male connector, although sometimes both connectors will be of the same type. One of the ports will be assigned as **COM1:** the other will be assigned as **COM2:**. It is possible that there will be no external markings on the PC indicating what the port assignments are, refer to the documentation that came with the PC system for identification.

Some PCs have a special port, usually a small DIN connector, for a **Bus Mouse**. This is a normal mouse that connects directly to the PC's internal bus without using a serial port. This type of mouse is ideal if you need to use two serial ports for Readykey equipment. For example, if you are using non-Readykey ID devices on a CNC-based system, with Wiegand compatible readers instead of Readykey readers, then you may need a port for the PC Interface Kit with Wiegand Interface as well as a port for the CNC.

It is recommended that you install the mouse in **COM2:**, or use the special bus mouse port, and install the CNC/PC Interface Kit in **COM1:**.

Technically the mouse and CNC/PC Interface Kit must use different IRQ levels. If you have problems with the serial ports then ensure, using suitable diagnostic software, that the mouse and CNC/PC Interface Kit are not sharing the same IRQ number. Normally the COM1: serial port is assigned IRQ 4, COM2: is assigned IRQ 3.

Cables are supplied with the CNC and PC Interface Kit for connecting them to the PC. The cables supplied with the CNC, have a 25 pin male connector at one end for connection to the CNC, whereas the cables supplied with the PC Interface Kit have a 5-way terminal block at one end.

At the other end both have a 9-pin female connector. Use the cable that matches the PC serial port you are using or purchase an adapter from a local computer store to match up to the serial COM port connection on your PC.

Additional PCs

Readykey for Windows may be administered from more than one PC simultaneously across a Local Area Network (LAN) or Peer to Peer Network. It may be convenient, if more than one master is being used, to connect these to different PCs across the LAN, and hence reduce the amount of cabling and communications equipment required to connect the door controllers to the masters.

Installation of a CNC

Refer to *Central Network Controller Installation Manual* (supplied with the CNC) for details of how to connect the CNC to the PC and door controllers.

CNC to PC Baud Rate

The speed at which the CNC communicates with the PC is selected by a switch, SW 2 switch number 7, inside the CNC or accessible from underneath the case on new CNCs. Readykey for Windows communicates with the CNC at 9600 baud. This is unlike the earlier K6000 system which communicated at 19200 baud.

It is essential to make sure that this switch is set to OFF, i.e. towards the front of the CNC for Readykey for Windows to operate correctly.

Note: New CNCs supplied by Radionics will be correctly configured to operate with Readykey for Windows.

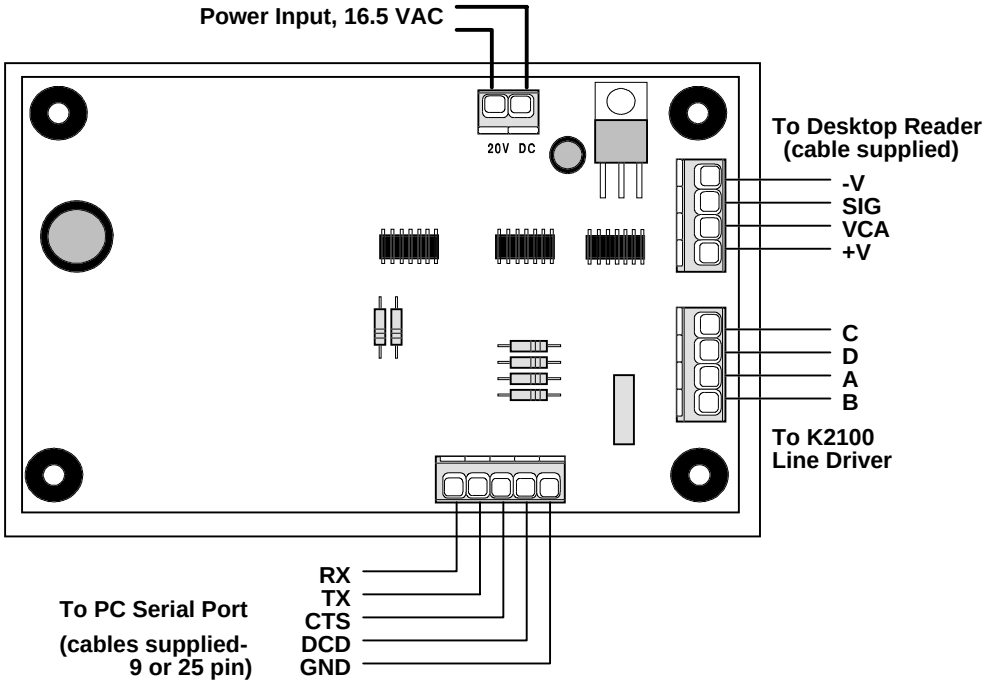
Recent versions of the CNC display the CNC to PC baud rate ('Host Baud') during the power up sequence. In earlier versions of the CNC it is necessary to inspect the switch position to determine the baud rate. Further information on the CNC switch settings is included in the *Central Network Controller Installation Manual.*

Installation of a PC Interface Kit

A PC Interface Kit allows the PC to be connected, via a serial port, to the K2100 or K1100 door controller. The door controller may be up to 3000ft/1km away using 4-core signal cable.

Note: It is recommended to use a six wire cable between the PC Interface kit and Master door controller. This will allow for a ground reference, if necessary, or ease of future expansion.

The kit includes a PC Interface Unit, a Line Driver, cables for connecting the PC Interface Unit to the PC, and a desktop reader for administering Readykey keys/cards. A Wiegand Interface may be used in place of the desktop reader with the corresponding wiegand reader for administration of non-Readykey ID Devices. The PC Interface Unit requires a 16.5VAC 25VA transformer, purchased separately from Radionics by ordering a D1625, to power the PC Interface Unit.

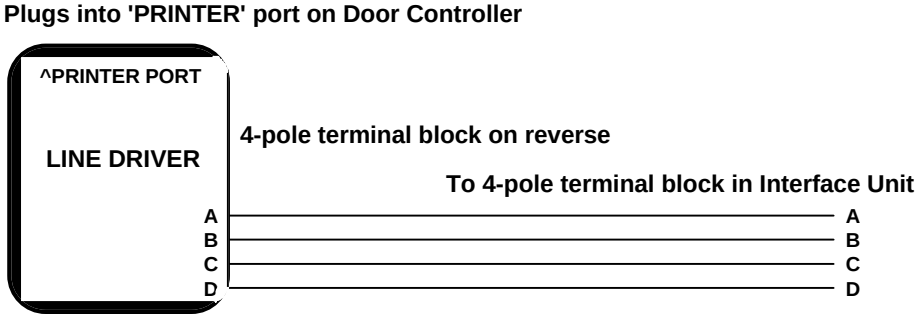


Interface Unit

Installing the Line Driver

The cable for connecting the PC Interface Unit to the Line Driver is **not** supplied with the PC Interface Kit.

Use multi-stranded, unshielded, 4-conductor 0.22mm²/24AWG signal cable. Radionics recommends that you use a 6 conductor wire for this connection, is case of future upgrades or lack of earth ground connection.



Up to 1000m/3000ft, use 4-conductor, 0.22mm²/22AWG signal cable

Line Driver, Wiring Diagram

IMPORTANT: For effective communications you must ensure that both the PC and the K2100/K1100 Door Controller are properly earth grounded. This normally will be already done by the AC mains connection.

The line driver should be plugged directly into the K2100/K1100 **'RS-232/PRINTER'** port, the 5-way socket at the bottom right of the circuit board.

The connection to the Interface Unit is made by connecting the terminals, labeled **A B C D**, to the corresponding terminals in the Interface Unit, using the 4-pole terminal blocks provided.

Note that the Line Driver is always required, regardless of the distance between the PC Interface Kit and the K2100/K1100.

Connecting a K2100/K1100 directly to a PC

As an alternative, a K2100/K1100 master controller may be connected directly to a workstation, without using a PC Interface Kit:

Use 0.22mm² 4-core unscreened signal cable, maximum length: 15m

PC Serial Port	PC Serial Port		K2100/K1100
25-way male	**9-way male**		**5-way Terminal Block**
RX 2	RX 3	- - - - - -	TX
TX 3	TX 2	- - - - - -	RX
GND 7	GND 7	- - - - - -	GND

Note: Line drivers, or other RS-232 communications equipment may be used to extend the distance between the PC and the K2100/K1100. However, dial-up modems may **NOT** be used. The distance between the PC and 'Master' door controller cannot be more than 50 feet in this configuration, unless other devices such as Line Drivers have been used to extend this distance.

Programming Multi-Division Systems

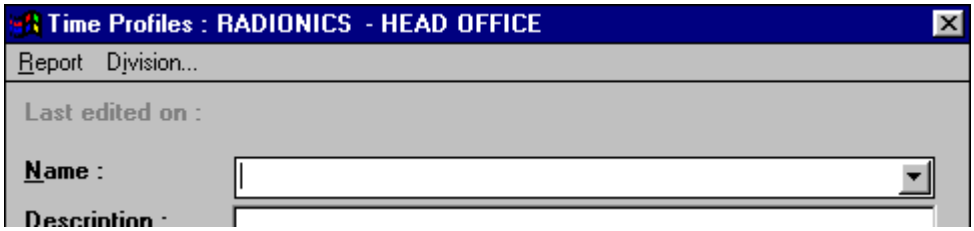
Introduction

For multi-division Readykey for Windows systems, much of the information you set up from this point needs to be programmed for each division individually.

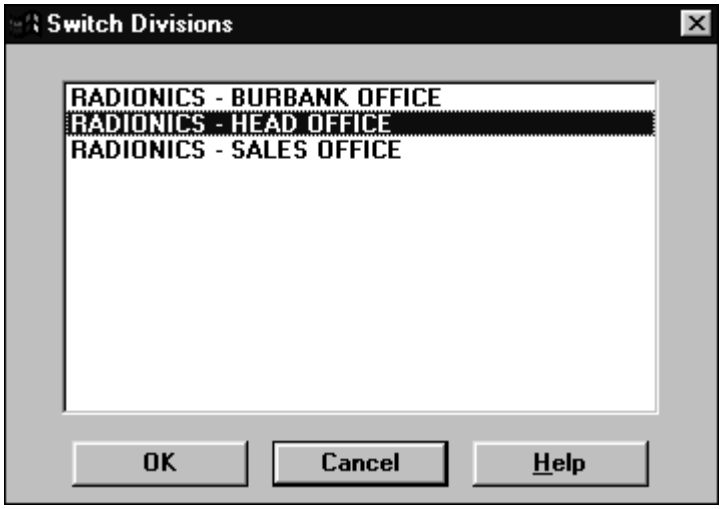
It is strongly recommended that you concentrate on commissioning each division individually.

Switching Divisions

If you have defined more than one division, then a special menu **'Division...'**will appear in most screens in Readykey for Windows to allow you to switch between divisions, as shown below:



Clicking on this menu will bring up the screen below:



- select the division you now wish to view / edit, then choose **OK.**

The name of the division currently being edited is shown on the title bar of 'division-dependent' parts of Readykey for Windows - see the sites example above.

Once you have changed to a different division, then that will remain the 'active' division throughout the Readykey for Windows software until you choose another division. For example, if you choose to edit the 'RADIONICS INC. - CHICAGO SALES OFFICE' division in **Installer: Sites**, then that will become the 'active' division in all other parts of the software until you switch divisions again.

You should also be aware that a small number of applications of Readykey for Windows are **division independent** (global to the system) - the most obvious are **Installer: Workstations** and **Installer: Masters**, but there are others too.

There are also two special cases - **Alarm** and **Operators.** How these are configured for multi-division systems is described later.

Installer: Sites

The total maximum number of sites available on your system is programmed into the Readykey for Windows security block - additional sites may be purchased if required.

Readykey for Windows supports up to 128 sites per division. This screen is used to set up the sites in each division - which master it communicates with and how it communicates. For sites that involve a dial-up link using modems and the PSTN, then the telephone number of the modem at the site, the automatic dial-up times and duration are also configured here.

One site is provided as part of the default data. This is part of the default division and communicates to the default master via the six wire bus. This site may be optionally amended or deleted.

It is a good idea to add sites one at a time, ensuring all door controllers on the site communicate with the CNC before adding the next site.

The different types of site available are described in *Readykey for Windows System Overview.*

As each site is programmed in Readykey for Windows, the communications method being used needs to be programmed. The 'Comms Type' setting in **Installer: Sites** is used for this purpose.

The different **Comms Type** settings available are:

a. Six Wire Bus

This setting should be made when the site is either:

- Local K2100/K1100 master connected to a workstation via a PC Interface Kit.
- Local K2100/K1100 master connected directly to a workstation
- Slave K2100/K1100 controllers connected to a CNC via the Six Wire Bus.

b. Direct RS-232

A single door controller of any type communicating with a CNC via a direct RS-232 link.

Note: This type of site is not described in the *Readykey for Windows System Overview* - it is a special case of the Direct RS-232 Cluster type, with just a single door controller.

c. Direct RS-232 and Dataswitch

Up to eight slave door controllers communicate with a CNC via a fixed RS-232 link and either a 4-way or 8-way dataswitch (COS-4 or COS-8).

d. Direct RS-232 Cluster

A K2100 or K1100 controller (set to System Type 2) communicating with a CNC via a direct RS-232 link. Up to seven additional slave controllers of any type may be connected to the K2100/K1100 using the Six Wire Bus.

e. Modem

A single door controller of any type communicating with a CNC via dial-up modem.

Note: This type of site is not described in the *Readykey for Windows System Overview* - it is a special case of the Modem Cluster type, with just a single door controller.

f. Modem and Dataswitch

Up to eight slave door controllers communicate with a CNC via dial-up modem and either 4-way or 8-way dataswitch (COS-4 or COS-8).

g. Modem Cluster

A K2100 or K1100 controller (set to System Type 2) communicating with a CNC via dial-up modem. Up to seven additional slave controllers of any type may be connected to the K2100/K1100 using the Six Wire Bus.

CNC Limits

The K6100-CNC allows a total of 32 RS-232 sites with more than one door controller (types c, d, f and g). An additional 95 sites with a single door controller may be added on each CNC - the special cases of site types b and e are offered for these. To add additional sites with more than one door controller, further CNCs must be added or a K6100-CNCII must be used to replace the existing K6100-CNC.

The K6100-CNCII allow a total of 127 RS-232 sites with more than one door controller (types c, d, f, and g).

Although sites from different divisions may communicate via the same CNC, Readykey for Windows will check as sites are being added, to ensure the above limits for a single CNC are not exceeded.

The CNC displays site information using ‘Site Numbers’. Readykey for Windows uses names only to describe sites. When adding sites of types b or e, these will be automatically given CNC site numbers between 34 and 128.

Door Controllers

Before adding any sites to the Readykey for Windows database, you should ensure that the door controllers are correctly configured and communications equipment and cabling are in place. This is so that when sites are added into the Readykey for Windows system, communications can commence immediately. The following types of door controller may be used on a Readykey for Windows system - K2100, K1100, K2000-N. The list offered will include a number of variations on these - referring to software version numbers, etc. Some features of Readykey for Windows will only be available for certain types of door controllers - see the list under **Installer: Divisions**, described earlier.

Door Controller Settings

Each door controller must have certain settings made in order for it to communicate with Readykey for Windows. The settings made in the door controller will depend on the type of door controller being administered and the method of communication being used.

A table of all the relevant settings for the different controllers/site types is given in the **Quick Start** section of this manual, under **Installer: Controllers**.

Dialback

The K2100 and K1100 controllers offer a facility whereby high priority transactions occurring at a dialup site (type e or g only) can initiate a communications session with the CNC.

Programming of dialback is done at the K2100/ K1100 which is connected directly to modem at the site. No programming or settings for this facility are required in Readykey for Windows.

Configuring Optional Hardware

This section describes some additional features of the Readykey for Windows system that you may be using. These are:

- Controller Relays (K2100 and K1100 controllers)
- K2015 Alarm Modules and K2015A Alarm Event Managers

Both these are defined within the **Installer** application.

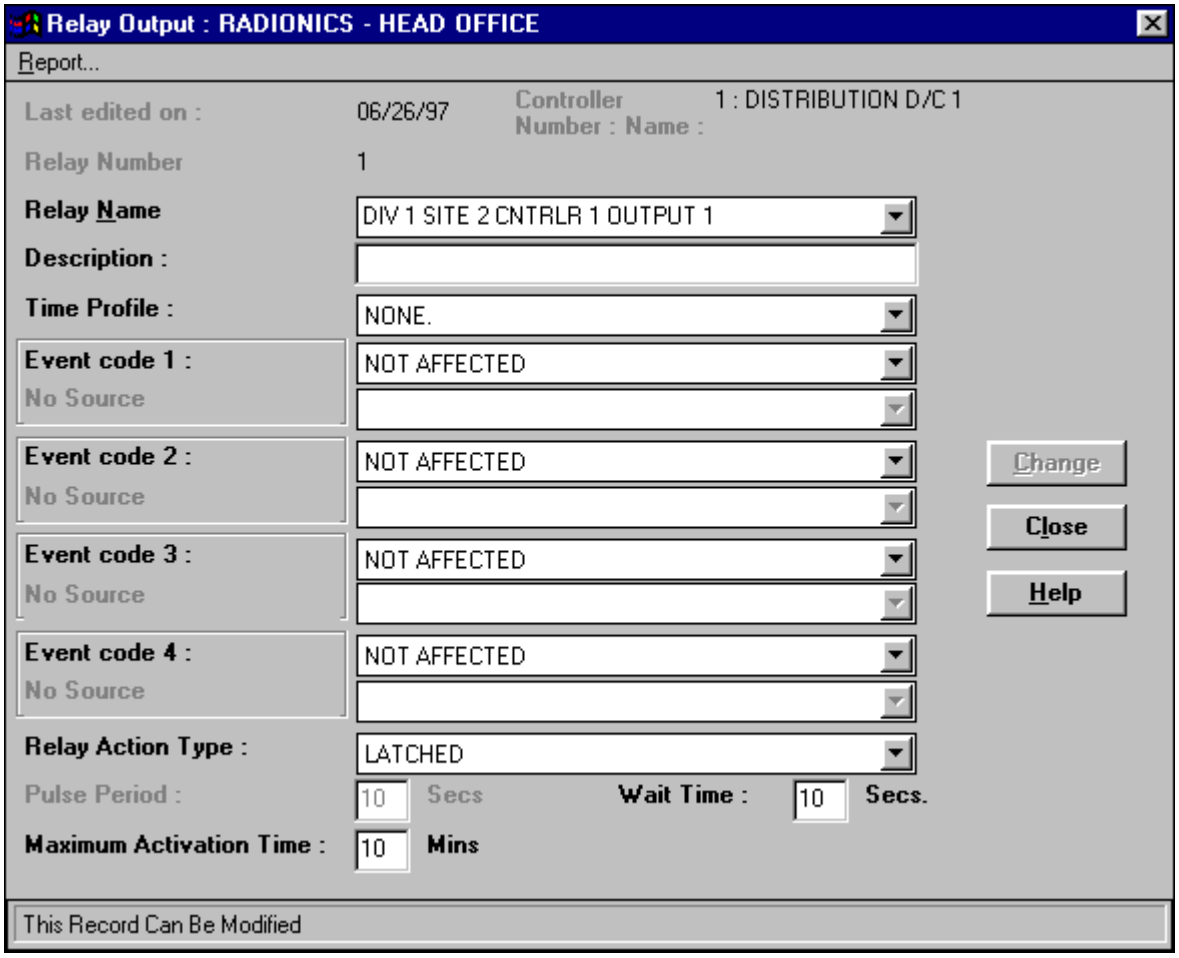
Programming On-Board Relays (K2100 and K1100 only)

The K2100 and K1100 have four on-board relays which may be programmed to activate for certain events. If the relays are not programmed, then they behave as follows:

Relay Number	Activates with....
1	Unauthorized Access (any door)
2	Time Profile 1
3	Door Left Open (any door)
4	Case Tamper

From the **Installer** sub-applications, double-click the **Controllers** icon.

Choose **Outputs...**.



Up to 4 different events may be attached to each of the 4 on-board relays. The dialog box above shows the settings for one relay.

By default the **Relay Name** is set to ***controller x output y,*** where ***x*** is the Door Controller number and ***y*** is the relay number. Use the drop down selection box to select the relay you want to modify. You should enter a more meaningful name in this field as the name you enter will appear on reports when the relay is set or reset.

A useful **Description** should be added to help describe the relay's function.

The **Time Profile** is an overall Time Profile, the relay will only respond to events when the Time Profile is active. If no Time Profile is assigned then the relay will always respond.

Event Codes

There are 14 different **Event Codes** that can be set to activate the relay. Some of the events also have a **Source.** The source title will change depending on the type of event.

The types of event, with their sources are:

Event	Reset	Source	Notes
Not affected		none	
Door alarm	**A**	Door Name	Unauthorized Access
Door tamper	**A**	Door Name	Cable or Reader Tamper
Door controller tamper	**A**	none	
Alarm module tamper	**A**	Alarm Module	
Access authorized	**L**	Door Name	See Note 1
Access denied	**L**	Door Name	See Note 2
Door opened	**C**	Door Name	
Door left open	**C**	Door Name	
Time profile	**T**	Time Profile	See Note 3
Door controller override	**C**	none	Emergency Override
Door alarm/tamper	**A**	Door Name	Alarm or Tamper
Alarm zone activate	**A**	Alarm Input	Zone Alarm
Manual zone enable	**C**	Alarm Input	See Note 4
Auto zone enable	**C**	Alarm Input	See Note 4

Reset

The reset codes above refers to when an activated relay is reset.

A **A** when the alarm is accepted, e.g. unauthorized access followed by alarm accepted.
C **C** when the condition is cleared, e.g. door open followed by door closed.
L **L** active for the duration of the Lock Release Time.
T **T** the relay follows a time profile.

Notes

1. This includes Access Authorized, Entry Authorized, Exit Authorized.
2. This includes No Access: Unknown ID, Level, Time, Visit Time, Locked Out, Passback, Incorrect PIN (Personal Identification Number).
3. **Time Profile** is secondary to the overall time profile above for the relay. The relay will activate with whichever time profile is entered in **Source**.
4. The relay will activate whenever an Alarm Module Input is enabled either manually or automatically (by time profile).

Relay Action Type

When a relay is active it changes over from 'normally closed' to 'normally open'

Here you can select from:

Latched **Latched** where the relay will stay active until either the condition is cleared (see Reset above) or the **Maximum Activation Time** expires. You may also set a **Delay Time** before the relay will activate.

Momentary **Momentary** which will activate for the length of the **Pulse Period (seconds)** after expiry of the **Delay Time.**

Set/Reset **Set/Reset** where the relay will stay active until the next occurrence of the event, in which case it will change back. (Note: there are no pulse or delay settings in this case).

Pulsing **Pulsing** in which the relay will pulse according to the setting of **Pulse Period (1/10th seconds)**, after expiry of the **Wait Time**, until either the condition is cleared (see Reset above) or the **Maximum Activation Time** expires.

The settings for each relay action type described above are:

Pulse Period	**Period** in 1/10ths of a second for pulse, whole seconds for momentary. When the relay type is Pulsing the relay will pulse (switch on and off) according to this value. When the relay type is Momentary the relay will operate for the number of seconds
Wait Time	**Time** - the number of seconds before which the relay will activate. If the condition is cleared before the expiry of the wait time then the relay will not activate. A Wait Time value of "0", will activate the relay immediately upon the event occurring. The maximum Wait Time is 99 seconds.
Max. Activation Time	**Time** the maximum time (in minutes) that the relay will be active. A pulse period, whether momentary or pulsed, will always be allowed to finish. Set a time of 0 (zero) minutes for the relay to be active until reset. A Maximum Activation Time value of "0", will activate the relay permanently upon the event occurring until accepted either by a Master or PC Operator. The maximum value for the Maximum Activation Time is 99 minutes.

Some Examples

You may wish to switch on a security light or camera whenever somebody attempted to use their key outside office hours. In which case you would:

1. Set the overall **Time Profile** to cover the time period you wish the relay to operate,
2. Enter an **Event Code** of Access Denied for each door (**Source**) you wish to monitor,
3. Set the relay **Action** required to operate the device.

Activate a buzzer when a door is left open:

1. Set the overall **Time Profile** to 'none',
2. Enter an **Event Code** of Door Left Open for each door (**Source**) you wish to monitor,
3. Set the **Relay Action Type** to latched, with no Wait Time (delay). The buzzer will sound from the time the door left open is detected (lock release time + door left open time) until the door is closed.

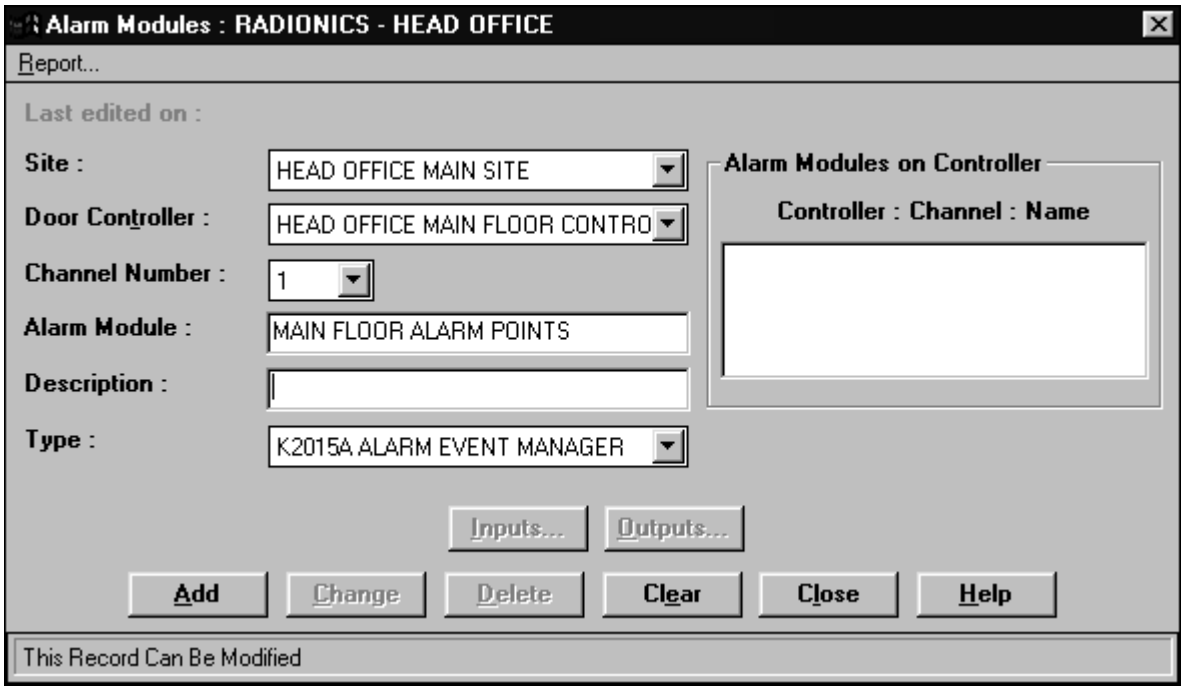
K2015A Alarm Event Managers

Here you can set all the features for any K2015A Alarm Event Managers (or the earlier K2015 Alarm Modules) you have installed.

See the *K2100/1100 Installation Manual* and *K2015A Alarm Event Manager Installation Data Sheet* for full information on installing these devices.

Readykey for Windows is the system that uses all the features of the K2015A Alarm Event Manager, including responding to Tamper (open) and Trouble (short) events on the monitored inputs and grouping alarms into areas to allow arming and disarming of areas by the operator.. Also, only Readykey for Windows allows programming of all 8 output relays.

From **Installer**, choose **Alarm Modules**:

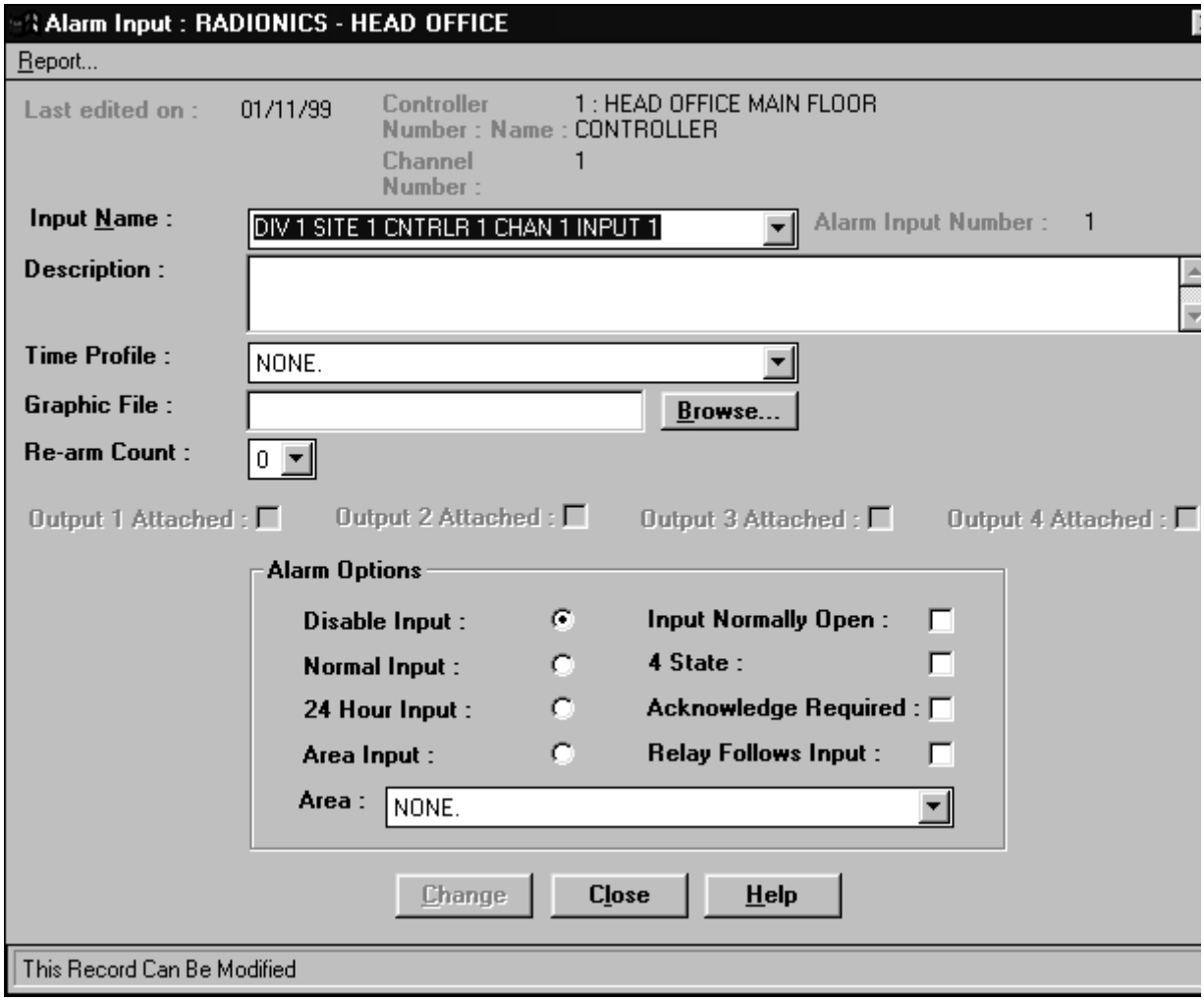


Installing a K2015A Alarm Event Manager or K2015 Alarm Module

1. Make sure the correct **Division** is selected.
2. Select the **Site** and **Door Controller** from the lists.
3. Select the **Channel Number** to which the device is connected from the list.
4. Enter an **Alarm Module** name, and useful **Description** if required.
5. Select the **Type** of module, either a *K2015 Alarm Module* or *K2015A Alarm Event Manager*.
6. Choose **Add**.
7. The Alarm Module is now added to the system and you can program the **Inputs** and **Outputs**.

Programming Inputs

1. Choose **Inputs...** from the **Alarm Modules** dialog.



2. Select an Alarm **Input Name**, if this is the first time the input has been used then replace the dummy name (e.g. DIV 1 SITE 1 CNTRLR 1 CHAN 1 INPUT 1*)* with something more meaningful.
3. Add a **Description**, this description will be displayed in the Alarm application when you select an alarm event and choose **Info.**
4. The **Time Profile** sets the time **when the input is isolated** (shunted), i.e. if you apply a time profile of 9:00-5:00, Mon-Fri to the input, then the input will **not** respond during this time period.
5. **Alarm Graphic**

   If there is a graphic file name, in the form *filename.bmp*, then a picture or diagram will be available in the **Alarm** application when an alarm is activated. Files must be stored in the directory \xxx\GRAPHICS, where xxx is the directory in which Readykey for Windows was installed, usually RKEYWIN.

   This picture may be displayed in the **Alarm** application by selecting the **Info..** button.

   Choose the **Browse..** button to select a picture or diagram.

6. The **Re-arm Count** is the number of times the input will respond in any arming period. If the number of responses exceed this number then an event will be generated and no further responses will be produced. Set this value to 0 to ensure the input always responds and re-arms the protected point. **Warning:** Only use a value greater than "0" when a Time Profile is assigned to the input. Once the re-arm value is exceeded the point will remain 'Shunted/Isolated' until the Time Profile becomes active and later re-activates the point.

7. **Alarm Options**

   a. **Disable Input**, this disables the input and prevents an alarm event being produced; however, see **Relay Follows Input** below.

   b. **Normal Input**, this sets the input to generate an alarm event (provided the **Time Profile** allows).

   c. **24 Hour Input**, this input cannot be disabled and will always produce an alarm event.

   d. **Area Input**, this sets the alarm input to an alarm area. Select the alarm area in the list box below the button. If this is set then the alarm inputs can be armed and disarmed manually in the alarm application.

   e. **Input Normally Open**, (K2015A Alarm Event Manager only) indicates whether the input is normally open or normally closed.

   f. **4 State,** (K2015A Alarm Event Manager only) indicates whether the input is supervised or not. The 4 states are Normal, Active (Alarm), Shorted or Open (Tamper).

   g. **Acknowledge Required,** any relay response will remain active until an operator accepts the alarm. If this is not selected then the relay will reset when the condition clears.

   h. **Relay Follows Input**, when this is set any relay response will be activated when the input is activated, and reset when the input is reset. **This will be the case even when the input is disabled**. This is intended for use when the input is not an alarm input but a plant or environment monitor.

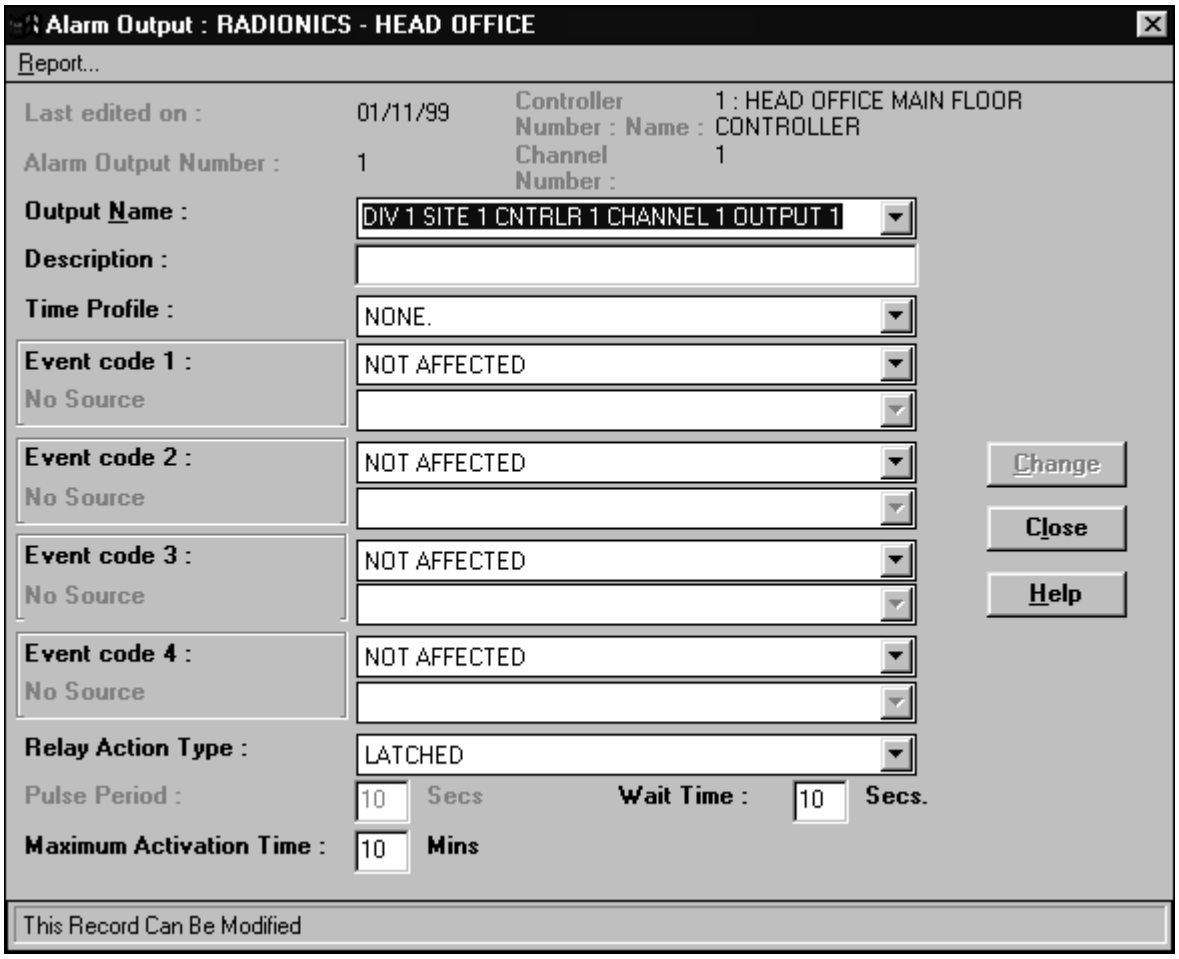
8. **Output Attachments**

   Note: These apply to K2000-N door controllers only.

   Each input can activate one or more of the relays on the same alarm module. These are always momentary.

Programming Outputs

1. From the Alarm Modules dialog, choose **Outputs...**



   If you have programmed the on-board relays of the K2100 or K1100 you will realize that this screen is very similar.

2. In this case select the **Output Name** from the list. Change it to a more meaningful text than the default. Add a **Description,** if required.

3. The **Time Profile** you assign at this point will determine when the relay will respond to events. If you select 'none' then the relay will always respond. If you select a time profile that works from 9:00 - 5:00, Monday to Friday, then the relay will only respond between those times - **whatever the event codes you set below.**

4. **Event Codes**

   There are 15 different **Event Codes** that can be set to activate the relay. Some of the events also have a **Source.** The source title will change depending on the type of event.

   The types of event, with their sources are:

Event	Reset	Source	Notes
Not affected		None	
Door alarm	**A**	Door Name	Unauthorized Access
Door tamper	**A**	Door Name	Cable or Reader Tamper
Door controller tamper	**A**	None	
Alarm module tamper	**A**	Alarm Module	

Access authorized	**L**	Door Name	See Note a
Access denied	**L**	Door Name	See Note b
Door opened	**C**	Door Name	

Event	**Reset**	**Source**	**Notes**
Door left open	**C**	Door Name	
Time profile	**T**	Time Profile	See Note c
Door controller override	**C**	None	Emergency Override
Door alarm/tamper	**A**	Door Name	Alarm or Tamper
Alarm zone activate	**A**	Alarm Input	Zone Alarm
Manual zone enable	**C**	Alarm Input	See Note d
Auto zone enable	**C**	Alarm Input	See Note d
Alarm Zone Tamper	**A**	Alarm Input	See Note d
Alarm Zone Trouble	**A**	Alarm Input	See Note d
Elevator Control	**L**	Elevator Name	See Note e

Reset

The reset codes above refers to when an activated relay is reset.

- **A** when the alarm is accepted, e.g. unauthorized access followed by alarm accepted.
- **C** when the condition is cleared, e.g. door open followed by door closed.
- .**L** active for the duration of the Lock Release Time.
- **T** the relay follows a time profile.

Notes

a. This includes Access Authorized, Entry Authorized, Exit Authorized.

b. This includes No Access: Unknown ID, Level, Time, Visit Time, Locked Out, Passback, Incorrect PIN.

c. **Time Profile** is secondary to the overall time profile above for the relay. The relay will activate with whichever time profile is entered in **Source**.

d. The relay will activate whenever an Alarm Module Input is enabled either manually or automatically (by time profile).

e. The relay will be activated dependent on the Access Group assigned to the keyholder. See the *Readykey for Windows Elevator Control Datasheet*.

5. **Relay Action Type**

When a relay is active it changes over from 'normally closed' to 'normally open'

Here you can select from:

Latched **Latched** where the relay will stay active until either the condition is cleared (see Reset above) or the Maximum Activation Time expires.

The relay will only activate after the **Wait Time** has expired..

Momentary **Momentary** which will activate for the length of the Pulse Period (seconds) after expiry of the **Wait Time**.

Set/Reset **Set/Reset** where the relay will stay active until the next occurrence of the event, in which case it will change back. (Note: there are no pulse or wait settings in this case).

Pulsing **Pulsing** in which the relay will pulse according to the setting of Pulse Period (1/10th seconds), after expiry of the Wait Time, until either the condition is cleared (see Reset above) or the Maximum Activation Time expires.

The settings for each relay action type described above are:

Pulse Period	**Period** in 1/10ths of a second for pulse, whole seconds for momentary. When the relay type is Pulsing the relay will pulse (switch on and off) according to this value. When the relay type is Momentary the relay will operate for the number of seconds
Wait Time	**Time** - the number of seconds before which the relay will activate. If the condition is cleared before the expiry of the wait time then the relay will not activate. A Wait Time value of "0", will activate the relay immediately upon the event occurring. The maximum Wait Time is 99 seconds.
Maximum Activation Time	**Time** the maximum time (in minutes) that the relay will be active. A pulse period, whether momentary or pulsed, will always be allowed to finish. Set a time of 0 (zero) minutes for the relay to be active until reset. A Maximum Activation Time value of "0", will activate the relay permanently upon the event occurring until accepted either by a Master or PC Operator. The maximum value for the Maximum Activation Time is 99 minutes. **Note:** If you select Elevator Control as the Event Code then the Maximum Activation Time is measured in seconds.

Some Examples

You may wish to switch on a security light or camera whenever somebody attempts to use their key outside office hours. In which case you would:

1. Set the overall **Time Profile** to cover the time period you wish the relay to operate,
2. Enter an **Event Code** of Access Denied for each door (**Source**) you wish to monitor,
3. Set the relay **Action** required to operate the device.

Activate a buzzer when a door is left open:

1. Set the overall **Time Profile** to 'none',
2. Enter an **Event Code** of Door Left Open for each door (**Source**) you wish to monitor,
3. Set the **Relay Action Type** to latched, with no wait time. The buzzer will sound from the time the door left open is detected (lock release time + door left open time) until the door is closed.

Appendix A: Troubleshooting

This section provides a list of the most likely problems which you may experience when commissioning your Readykey for Windows system.

If none of the given solutions resolve the problem, please contact Radionics Customer Service for assistance, telephone (800) 538-5807.

Note: Radionics Technical Support can only provide assistance to Authorized Readykey dealers. Please contact your installing Readykey dealer for assistance if you are not Authorized dealer.

Error Messages displayed when starting Readykey for Windows

Security Block not found

Check that the Readykey for Windows Security Block is installed in the parallel port of your PC. This will be a 25-way female D-type connector on your PC.

Confirm that the parallel port is operational by connecting a parallel printer to it and printing a text file - the Readykey for Windows Readme file could be printed using the Write application (supplied with every copy of Microsoft Windows).

Cannot Initialize Port

An Engine Error will occur if no Readykey hardware can be found in a serial port or another application is currently using the specified port of your PC. If this message occurs during initial start-up, then click on OK and ignore the message - you will set the system up correctly at a later stage.

However, if the message persistently reappears, you should check that the CNC/PC Interface Kit/K2100/K1100 is plugged into the correct serial port on your PC (either COM1: or COM2:), and that the port specified in **Installer: Masters** is correct. Confirm also that the CNC/PC Interface Kit/Door Controller is powered, and the connections from the serial port on your PC to the Readykey hardware.

You should also check that the serial port is working, and that it is not being shared with any other devices.

No Polling Indication on Door Controllers

This symptom can have a number of causes:

- Security block missing or insufficient number of sites programmed.
- The CNC/PC Interface Kit being incorrectly connected to the PC and door controller.
- A dial-up site is not on-line to the CNC.
- The Readykey for Windows system being incorrectly programmed.
- The door controller itself being incorrectly configured.
- Connection to the door controller from the CNC incorrectly connected.

Security Block Missing/Incorrect Number of Sites

A Readykey for Windows dongle (security block) must be connected to the LPT1 parallel port of the PC for communications to take place with the CNC and door controllers.

Readykey Hardware to PC Communication Problem

If a CNC displays `MONITORING` then the CNC is connected correctly to the PC. If the CNC displays a different message, then you should check the following:

PC to CNC cable

Check the cable between the PC and the CNC for continuity and shorts. Refer to the Central Network Controller Installation Manual for cable specifications.

PC Serial Port Operation

Close down Readykey for Windows and restart. Watch for error messages as Readykey for Windows starts. Refer to the error messages troubleshooting section above.

CNC to PC Baud Rate

The CNC must be configured to communicate to Readykey for Windows at 9600 baud. This is in contrast to the K6000 system which communicated to the CNC at 19200 baud. Recent versions of the CNC display the baud rate setting (Host Baud) at power up. In earlier versions, it is necessary to remove the CNC cover and inspect the setting of Switch Block #2 and verify switch 7, which should be set to OFF, i.e. towards the front of the CNC. All new CNCs are supplied to communicate with Readykey for Windows.

CNC Not Initialized

When the CNC is initialized, it learns about how many door controllers are connected to it, and hence which to poll. The initialization process also clears any information that may be in the CNC. To initialize the CNC, in **Installer: Masters** choose **Initialize**. If the PC reports 'Initialize Complete', then the CNC should now display `MONITORING.` If the Initialize operation fails, then confirm the CNC is communicating with the PC, as earlier in this document.

Non-CNC Sites

Confirm the wiring as described in the appropriate documentation from the PC to the PC Interface Kit (if used), and from the PC Interface Kit to the master door controller. If the master door controller is displaying a polling indication, but others on the same site are not, verify the six wire bus wiring, and the settings programmed in the door controllers and Readykey for Windows.

Dial Up Site not On-line

Use **Installer: Force Dial** to check the current status of communications to any dial-up sites. Force dial the site if necessary, by selecting the site from the list and choosing **Dial**.

If the site does not appear in the list, then check the settings in **Installer: Sites**, particularly the **Comms Type.**

Readykey for Windows Incorrectly Programmed

Incorrect Port Number in Installer: Masters

You should verify that the **Port** setting in **Installer: Masters** corresponds to the COM port on your PC to which the master is connected. If the COM ports are not labeled, then either try connecting the CNC to the other port, or select a different **Port** setting in **Installer: Masters**. When you set the port number to a different value you should close down Readykey for Windows and restart.

Incorrect Master Type in Installer: Masters

The Engine is responsible for all communications between the PC, the CNC and the door controllers. However, the Engine communicates to different types of master in different ways.

You should ensure that the **Master Type** is correctly set for your system.

Door Controller added

Confirm that the Door Controller has been added in **Installer: Controllers**. Confirm that the settings (address, type, etc.) in the door controller are correct.

Door Controller enabled

Confirm the door controller has been enabled in **Installer: Controllers**. It may be occasionally necessary to disable the controller - choose **Change**, then re-enable the controller, again choosing **Change.**

Door Controller Incorrectly Configured

System Start

The door controller should have had a 'System Start' operation performed before any settings were made. If this is not the case, then carry out this procedure as described in *K2100/K1100 Installation Manual*.

System Type and Door Controller Type

Make sure that a K2100 or K1100 door controller is set to the correct System Type 3 for a slave and System Type 2 for a master. Press the '**?**' key on the door controller. The controller should bleep and indicate a display similar to:

```
2100 Mn  Vx.yz 1
```

If the controller does not bleep and show such a display, then the controller is probably not a K2100 or K1100.

Refer to the chart on page 17 for information on correct door controller settings.

Address

Make sure the address of the door controller is correctly set, and also that no two controllers on the same site have the same address. Use Engineering Mode on the K2100 or K1100 to confirm this setting.

Reset Door Controller

Occasionally it may be necessary to press the 'Reset' button on the door controller before communications begin. The controller should bleep. If it does not, then ensure the controller is powered.

Connections to the door controller

Six Wire Bus

Check the six wire bus connection between the door controllers and the master for continuity and short circuits. It may be a good idea to add door controllers one at a time to the six wire bus, ensuring each is communicating correctly before adding the next door controller.

RS-232

Check that the cables which connect the door controller to the CNC/PC Interface Kit/PC Serial Port and to any communications equipment are wired in accordance with the *Central Network Controller Installation Manual*. Wiring of the PC Interface Kit is described earlier in this document.

If possible, eliminate third party communications equipment by connecting the door controller directly to a CNC.

Test Key/Card will not allow access

No transaction displayed when key/card presented

If no transaction appears on the On-line Transaction Display when the key/card is presented to a reader, then you should verify that the transaction is being received at the PC. To confirm this, double-click on the Engine icon. Several lines of information will be displayed. The number shown for 'Transaction File Size' should increase by 1 each time a key/card is presented to a reader. If it does not, then verify the connection between the PC, the CNC and the door controllers. For remote sites, ensure the site is on-line.

If however, the 'Transaction File Size' does increase, then the transaction is being received at the PC. Use **Admin: Trans Routing** to verify that **ALL** transactions have a cross in the 'Display' box. Also ensure that the **Enable Routing Frame** box contains a cross.

If you have more than one workstation or division, then you will need to create transaction routing information for the second and subsequent divisions.

No Access: Unknown ID

If the On-line Transaction Display reports **No Access: Unknown ID** when an ID device is presented, then the ID device is unknown to the door controller.

Verify that the key/card exists in the **Personnel** application by presenting the ID device to the CNC reader in **Personnel**. If present, the test ID device record should be displayed.

If you have more than one division, then confirm that the ID device has been added to the correct division.

If the ID device is in Personnel, then verify communications with all door controllers. Ensure the CNC display does not reflect that updates are being stored in the CNC for the door controllers on the site. If no updates are waiting to be sent, use **Status** to verify communications to the site before performing a download to the door controllers, using the **Initialize and Download** function in **Installer: Utilities**.

No Access: Locked Out

This message means that the ID device is recognized by the door controller, but no access group has been assigned to it on the site. Within the **Personnel** application, make sure an **Access Group** is assigned to the ID device. Choose **Change** after making any changes to the record.

If the ID device has a DAG assigned, verify the programming of the DAG has an access group assigned for every site.

No Access: Level

This message means that the key/card has been recognized by the door controller, and has access to some areas of the system, but not into the area entered from the door reader at which the key/card was presented. There could be two reasons for this:

Access Group

In **Admin: Access Groups** select the test access group for the site. Make sure all the areas defined on the site are in the **Access List 1** box. Choose **Areas...** to make any changes to the entries in the **Access List 1** box. Choose **Change** when you have made any changes to the Access Group record.

Doors

In **Installer: Doors** make sure that each door has the correct **Entry Area** assigned. Choose **Change** after making any changes to each door record.

No Access: Date

This transaction will appear if the keyholder has been programmed with Start and End Dates in **Personnel**, but either:

1. today's date lies outside the dates specified, or
2. the date stored in the door controller is incorrect, or
3. the date entered is in the incorrect format.

This problem can be resolved as follows:

1. In the **Personnel** application, search for the keyholder, and amend the dates as required.
2. Confirm the PC time and date is correctly set - use **Control Panel: Date/Time** from the Windows Program Manager. When the date and time have been correctly set, use the **Clock Synchronize** utility in the **Installer** application to update the clocks in the door controllers.
3. Readykey for Windows uses the Windows **Control Panel: International/Regional** settings to determine the date format for the country where Readykey for Windows is installed.

Commonly this will be:

- DD/MM/YY - for most European countries,
- MM/DD/YY - for the United States and Canada,
- YY/MM/DD - for Scandinavia and Japan.

Make sure the dates entered in the **Personnel** application are in the same format.

No Access: Time

This message will be displayed if the keyholder's Access Group has been restricted by a Time Profile allowing access only between specific times. Ensure that the Access Group assigned to the keyholder is correct or that the correct Time Profile is assigned to the Access Group. Select a Time Profile value of 'None' if it is desired to allow all keyholders assigned to the Access Group 24 hour a day entry all days of the week.

No Access: Alarm Armed

This message may be displayed if this system is using the K2050 Alarm/Access Integration module. The Access Group assigned to the keyholder is only granted access into the area when the intrusion alarm system has been disarmed. Ensure that the proper Access Group has been assigned to the keyholder.

No Entry: Passback

This message will be displayed if the system is using the Anti-Passback feature of Readykey. The keyholder has attempted to violate the Passback restriction by not going through the Exit reader before re-entering the area. This restriction may be time controlled to allow 'Forgiveness' after a period of time, or no 'Forgiveness' at all. The keyholder must first use the 'Exit' reader before 'Entry' will be granted.

No Exit: Passback

This message will be displayed if the system is using the Anti-Passback feature of Readykey. The keyholder has attempted to violate the Passback restriction by not going through the 'Entry' reader before re-entering the area. This restriction may be time controlled to allow 'Forgiveness' after a period of time, or no 'Forgiveness' at all. The keyholder must first use the 'Entry' reader before 'Exit' will be granted.

MSD - Microsoft Diagnostics

If you experience problems with the PC itself or Readykey for Windows system on a PC running MS-DOS and Windows 3.1/Windows for Workgroups 3.11, Radionics' Customer Service Department may ask you to forward an 'MSD Report'. MSD is a diagnostics program supplied by Microsoft as a part of Windows and MS-DOS (Version 6.00 and above), which produces a report of your PC specification and its setup. This information is sometimes invaluable in troubleshooting problems.

To obtain an MSD report:

1. Close down Readykey for Windows. Close down Windows itself.
2. At the MS-DOS C:\> prompt, type **MSD** and press **Enter**.
3. You will now be presented with a screen of information. To produce a report of the information, press **ALT** followed by **F**. This will bring down a list of options from the **File** menu at the top of the screen. Press **P** to choose **Print Report**.
4. In the **Report Information** screen, press the spacebar once to put a cross in the **Report All** option. If you have a parallel printer connected to LPT1: on your PC, then press Enter. Alternatively, press the **TAB** key until the cursor is in the 'Report to' section, use the arrow keys to select the required destination, and then press **Enter**.
5. In the 'Customer Information' screen, type your name in the **Name** box. Press **TAB** to move to the **Company Name** box. Type your company's name and press **Enter**.
6. The report will now be generated automatically. As this happens, the **Page** number in the lower left hand corner will count upwards. The report may be over 25 pages long! When it has finished, press **F3** on the keyboard to leave MSD and return to MS-DOS. If you have produced a report to a file, then copy the file (called 'REPORT.MSD') from the current directory to a floppy disk.

Appendix B: Using non-Readykey ID Devices

Most Readykey for Windows systems will use Readykey electronic keys or proximity cards with Readykey readers to form the basis of the access control system.

However, it is possible to use Wiegand compatible readers and ID devices as an alternative.

Two methods for administering non-Readykey ID devices are supported in Readykey for Windows:

- Readykey PC Interface Kit with Wiegand Interface may be used. The workstation will need to have a vacant serial port.
- Manually entering the codes into the Readykey for Windows **Personnel** application.

ID Device Codes

Different types of ID device have codes in different formats. Readykey proximity devices have codes which consist of eight hexadecimal characters (numbers 0 to 9; letters A to F).

The codes of many non-Readykey ID devices will consist of a 'site code' (sometimes called a 'facility code') and a sequence number. The number of digits in the site code and sequence numbers vary between formats.

Readykey for Windows allows a number of different ID device types to be used on a single system. The codes of the ID devices are always stored in the Readykey format in Readykey for Windows and the door controllers. Readykey for Windows automatically handles the 'translation' between formats.

In the **Personnel** application, the facility exists to add and view the codes of the ID devices in different formats. The default type of ID device is programmed, for each division on the system, in **Installer: Division** - this is the type of ID device automatically selected when the **Personnel** application is started, or when the current division is changed.

However, it is possible to have different ID devices within a single division - you should be aware that the type of ID device issued to a keyholder is not stored in the **Personnel** database, only the code itself. Hence, if the current ID device type is changed, the codes for all ID devices will be displayed in that format, regardless of the type of ID device actually issued to that keyholder.

Note: Changing the ID Device Type of an existing record, may corrupt the actual keycode. Do not make such a change to an existing record, unless under direction of Radionics Technical Support.

If mixed ID devices are in use on a Readykey for Windows system, then it is probably a good idea to use one of the 20 Extra Information fields in **Personnel** to keep a record of the actual ID device type in use.

The Supervisor Key code and that of any system operators is **ALWAYS** displayed in, and can only be entered in, a Readykey format - see the note below under 'Manually Entering Codes'.

Using a PC Interface Kit

You should assemble the PC Interface Kit as described earlier. The PC Interface kits are supplied with cables to connect to the various components of the PC Interface Kit and PC. Use the 9 pin female D-type connector to connect to your PC. Use one that matches the PC serial port you are using to connect the PC to the Interface Kit. If you are using a 25 pin connection, purchase an adapter from your local computer supplier. The line driver supplied with the kits is not used unless communicating to door controllers.

If you are using a PC Interface Kit with Wiegand Interface, then connect a Wiegand reader to the Wiegand Interface, and the Wiegand Interface to the PC Interface Kit, as described in the documentation of the wiegand interface. The Wiegand Interface needs to be configured for connection to the PC Interface Kit via an on-board jumper - refer to the K2012 Wiegand Interface datasheet for details.

Use **Installer: Workstations** to configure Readykey for Windows to recognize the PC Interface Kit - this process is described in the Quick Installation section of this document - see page 10.

Manually Entering Codes

These codes can be directly entered into Readykey for Windows, which will then 'translate' them into the Readykey format. The different formats available and their translations are stored in a special Readykey for Windows file on the PC hard disk. To enter a Sensor 2601 (Wiegand 26 Bit) format, enter in a 3 digit 'Site Code' (facility code) followed by a dash "-". Then enter the 5 digit Serial Number (card number).

It should appear within the Key Code field as follows:

- 012-01200

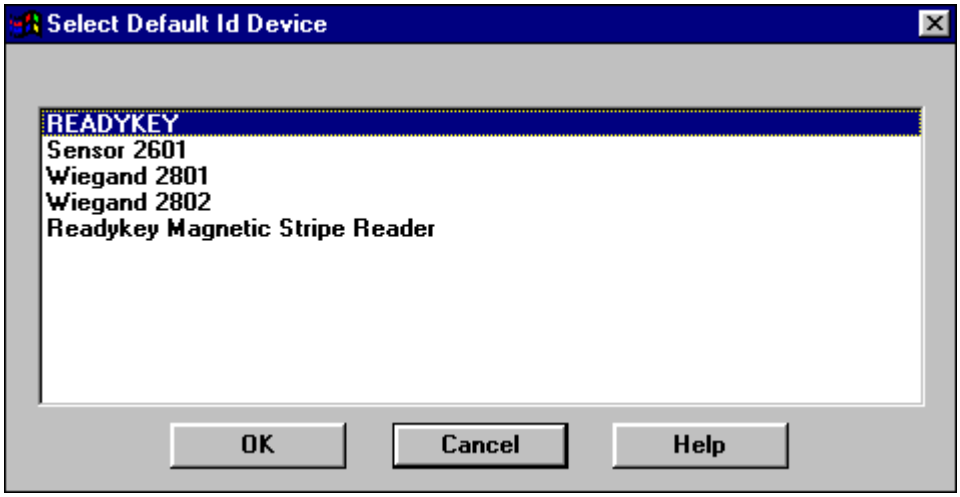
The above value would be entered for a Site Code value of 12, and a Serial Number value of 1200.

Note: If the format is not Wiegand 26 Bit, or not known, the ID Device Type should remain as Readykey and the wiegand ID Devices will need to be read into the system using the Wiegand Interface and PC Interface kit.

Personnel

When the **Personnel** application is started, or the current division changed from within **Personnel**, the 'Default ID Device' for the division is selected (using the setting programmed in **Installer: Divisions**).

The current ID device setting is displayed at the right hand side of the Status Bar at the foot of the **Personnel** screen, and can be changed by selecting the **ID Device...** menu from the main **Personnel** screen:



- select the ID device type to become the current type from the list, and choose **OK**.

Adding ID Devices

Adding keyholders with non-Readykey wiegand 26 bit ID devices is very similar to that of adding Readykey proximity cards and keys. However, instead of presenting the card/key to the administration reader to read the code, the site and sequence codes of the ID device should be entered manually in the **Key code** box, separated by a '-' (minus) sign.

When the rest of the keyholder information has been entered in the usual way, if the entry in the **Key code** box is valid, then choose the **Add** button.

Notes:

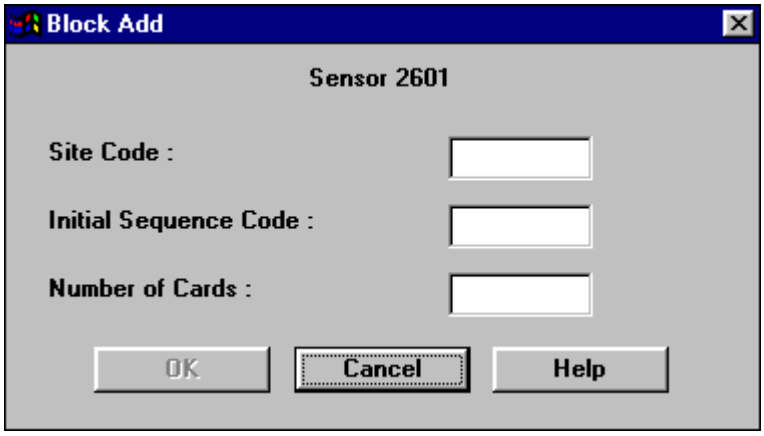
1. The **Add** button will be grayed out and unavailable unless the code of the device is valid.
2. If the format is not Wiegand 26 Bit, or not known, the ID Device Type should remain as Readykey and the wiegand ID Devices will need to be read into the system using the Wiegand Interface and PC Interface kit.

Block Add

Unlike Readykey proximity ID devices, which have seemingly 'random' codes, the site code of non-Readykey devices will often be the same, whilst the sequence codes will be in a range, from one value to another. The site and sequence codes are normally programmed to the customer's requirements when the ID devices are ordered.

When non-Readykey ID devices are being used, the **Block Add...** utility allows a large number of ID devices to be added quickly by specifying the site code and range of sequence codes.

Selecting the **Block Add...** item from the **Utilities** menu in **Personnel**, when the current ID device type is not Readykey, will bring up the following screen:



- enter the **Site Code**, the **Initial Sequence Code** and **Number of Cards** in the boxes and choose **OK**. If the values entered are valid, Readykey for Windows will start to add keyholders to the **Personnel** database for the current division. The following screen will indicate progress.

- Cancel may be chosen at any time to abort the process.

If any duplicate codes are found a warning message will be issued.

When all the keyholders have been added, you will be returned to the main **Personnel** screen.

The added keyholders will have been given a **Last Name** based on their Site and Sequence code. This will generally be of the form:

TTT-QQQQQ, where **TTT** is the (3 digit) site code, and **QQQQQ** the (5-digit) sequence code. The number of digits in each part of the above may vary from format to format. Note the '-' separating the two parts.

It is now a simple task to search for the added keys and **Change** it to the correct **Last name**, **First Names**, **Department** and **Workgroup** (if used) and **Access Group** as the keys/cards are issued.

Note: When the current ID device format is Readykey proximity, the **Block Add...** utility works differently - it searches the current division for keyholders without an assigned ID device - each of these will then be displayed in turn to have a key/card assigned. The operator needs to present a key/card to the administration reader, and choose **Change**. The next keyholder without an assigned ID device will then be displayed. When all keyholders have a **Key code** assigned then 'Block Add Mode' will end automatically.

Further information on using the **Block Add...** facility in Readykey for Windows is included in the On-line Help.

Note: If the format is not Wiegand 26 Bit, or not known, the ID Device Type should remain as Readykey and the wiegand ID Devices will need to be read into the system using the Wiegand Interface and PC Interface kit.

Defining Formats

The formats displayed are stored in a special file, CARDCONV.INI, in the Readykey for Windows BIN directory.

This file contains the names of the ID devices, and the 'translation' information.

The following ID devices are supported as part of the default CARDCONV.INI file:

- Sensor 2601 (Wiegand 26 Bit)
- Wiegand 2801 (Casi-Rusco Wiegand 28 Bit Format 1)
- Wiegand 2802 (Casi-Rusco Wiegand 28 Bit Format 2)
- Readykey Magnetic Stripe Reader (Readykey European ISO Magnetic Stripe)

Note: If the format is not Wiegand 26 Bit, or not known, the ID Device Type should remain as Readykey and the wiegand ID Devices will need to be read into the system using the Wiegand Interface and PC Interface kit.

Operators / Supervisor

As stated above, the code of ID devices assigned to system operators and the supervisor is always displayed in, and can only be entered in, a Readykey format.

Therefore, if no PC Interface Kit with suitable administration reader is in use on the system, then ID devices cannot be used to log in to Readykey for Windows.

In this case, it will be necessary to create system operators without an ID device assigned. At least one of these should be assigned 'Supervisor' privileges, as the Supervisor key (**Installer: Global** and **Admin: Global**) may not be used.

Appendix C: Upgrading from a K6000 System

If you are installing a Readykey for Windows system in place of an existing K6000 or K6000-AM system, then you can partially convert the database of that system to the new Readykey for Windows format.

You should first of all install Readykey for Windows as described in the Readykey for Windows Software Installation Manual. Once you have installed the software, you can then convert the old database.

Before upgrading the database, however, you should:

1. Verify the integrity of the K6000 or K6000-AM database.
2. Configure certain parts of the Readykey for Windows system.

It is possible to upgrade multiple K6000 and/or K6000-AM databases into a single Readykey for Windows system, either into separate divisions, or merge them into one division.

Note: It is important to remember that the upgrade utility only provides a partial conversion. A detailed description of how each aspect of the K6000/K6000-AM database is handled by this utility is given at the end of this section - 'The Conversion Process'.

Verifying Existing Databases

Before attempting to upgrade a K6000 or K6000-AM database, you should first of all run a special utility, provided with the K6000 or K6000-AM software, that checks the database integrity.

To do this you need to close down Readykey for Windows, leave Windows itself and return to the DOS **C:>** prompt.

1. Type `CD \P6000` and press **Enter** (for a K6000 system), or `CD \2000AM` and press **Enter** (for a K6000-AM system).
2. Type `P6UTIL SORT` and press **Enter** (for a K6000 system), or `P2UTIL SORT` and press **Enter** (for a K6000-AM system).

The utility will now check the database and report on any duplicate or corrupt keys. Make a note of any keys or personnel it reports.

Note: Readykey for Windows will not accept the same key in both the Personnel and Visitor files. This is possible in K6000 or K6000-AM databases. Check, as far as possible, that there are no such keys/cards. If any are found, then the Readykey for Windows upgrade will reject these keys/cards.

Configuring Readykey for Windows

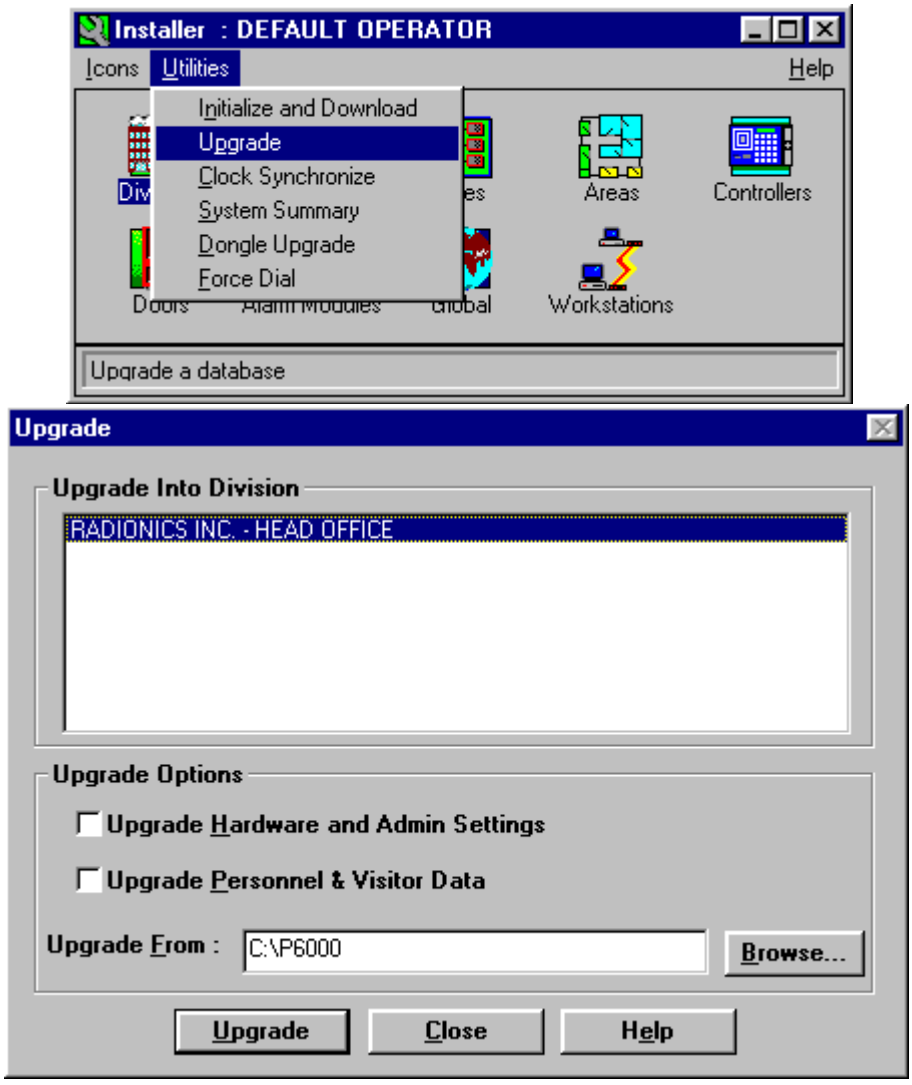
Note: The term 'DOS system' is used throughout the following to refer to the K6000 and K6000-AM systems.

Before attempting to upgrade a K6000 or K6000-AM database into Readykey for Windows, you should first Define the divisions in Readykey for Windows - the K6000 or K6000-AM database information is assigned to a division in Readykey for Windows. Multiple K6000 or K6000-AM systems may be upgraded into either a single or different divisions.

Follow the instructions in the Quick Start section of this document regarding programming division information before proceeding.

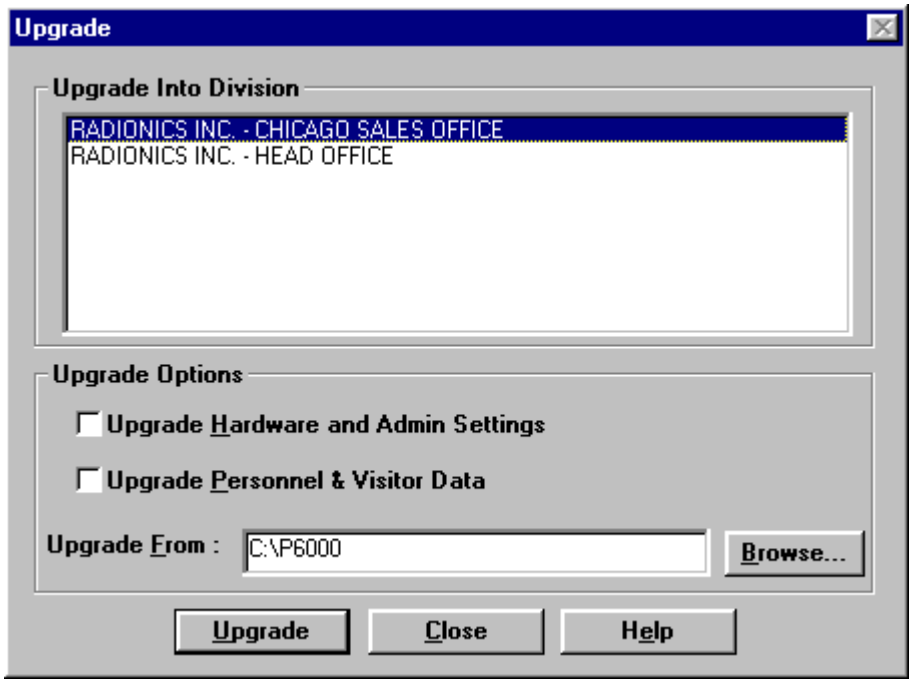
Upgrading the Database

The Upgrade utility is in the **Installer** application. From the **Utilities** menu, choose **Upgrade**.



Upgrade Into Division

Select the division into which the K6000 or K6000-AM system is to be upgraded, by clicking on it with the mouse.



Upgrade Options

The parts of the DOS system database that get upgraded to Readykey for Windows are dependent on the Upgrade Options chosen.

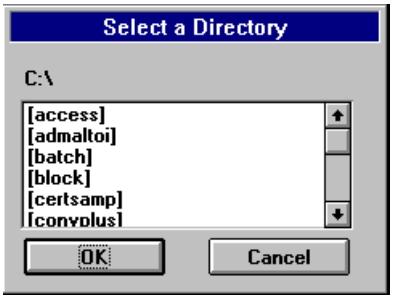
Upgrade Hardware and Admin Settings - converts the information listed below ('The Conversion Process') in the **Installer** and **Admin** sections.

Upgrade Personnel & Visitor Data - reads the keyholder (Personnel & Visitor) information from the DOS system and adds it in the Readykey for Windows **Personnel** application.

Upgrade From

You need to tell the Upgrade utility the source of the DOS database. The default setting is `C:\P6000`, but this can be changed.

Enter the path to the K6000 or K6000-AM database (normally C:\P6000 or c:\AM2000), or choose **Browse...** to view all directories and drives available:



- select the source path of the DOS database and choose **OK**. The selected drive and directory will now be displayed in the **Upgrade From** box.

Starting the Upgrade

Choose **Upgrade**.

The upgrade will then proceed. You will see an indication of progress in the Status box, along with a **% Complete** value.

Warning Messages

You may receive warning messages during the upgrade process, if for example duplicate keyholder information is found. You will be given options of what action to take - these will usually be to either abort the upgrade process, or continue, skipping the problem information.

It is important to carefully note any messages given - this information will need to be checked in Readykey for Windows when the upgrade process has completed.

The Conversion Process

There are many differences between a Readykey for Windows database and a K6000/K6000-AM database. The following describes what information has been converted and what remains to be completed manually.

The following assumes a knowledge of how Readykey for Windows and the K6000/K6000-AM (DOS) systems operate.

Installer

Divisions

The DOS systems only consisted of one division. When using the Upgrade utility, it is possible to upgrade multiple DOS systems into different divisions of a single Readykey for Windows system.

The divisions required should have been created first using **Installer: Divisions**.

Masters

The number of masters in the DOS and Readykey for Windows systems will be compared. If a K6000 database contains two masters and the Readykey for Windows system only one, then an additional CNC master will be created.

Note: The K6000-AM system only supported one 'master' - a K2000-AM (or K2100 in System Type 1). This will be programmed as a K2100 by the upgrade utility in Readykey for Windows. A K2000-AM door controller itself will also need to be upgraded. The system type of a K2100 controllers will need to be changed from 1 to 2.

Sites

Note: This section applies to K6000 systems only - the K6000-AM system only supports one site. A single Six Wire Bus 'site' will be used in Readykey for Windows for K6000-AM systems.

A site will be created in Readykey for Windows for every site in the K6000 system, using the same site name. Communication information will also be transferred - telephone number, baud rate, dial up times, site type, etc.

If there was only one CNC in the K6000 system, then all sites will be assigned to this. If there was more than one, the user will be presented with an option of which sites to assign to which CNC master.

Areas

No areas will be created. This information needs to be added in accordance with the system design, following completion of the upgrade.

Controllers

Controllers will be created as required on each site in Readykey for Windows to support the number of readers (doors) on each site in the DOS system. The *Controller Type* setting in Readykey for Windows will be set to 'K2000-N' or 'K2100' for controllers, dependent on the type of Alarm Module Sensor Records being used in the DOS system - this will need to be checked against the actual hardware installed and amended as necessary.

Note: This setting will restrict the availability of certain features in the Readykey for Windows system, particularly the number of personnel, time profiles and time periods.

Controllers will be named according to their address. All controllers will support four doors - if any K1100 controllers are in use, then these will need to be changed, after the 'dummy' doors on channels 3 and 4 have been deleted (see below).

Doors

Doors will be created in Readykey for Windows for every door that existed in the DOS system. If any K1100 controllers exist then 'dummy' doors will have been created in Readykey for Windows for channels 3 and 4.

Door information (Lock Release Time, Door Open Time, Time Profile, Lock Mode, PIN Reader Time Profile, etc.) will be transferred.

No Entry Area in the Readykey for Windows system will be assigned. This will need to be amended according to the system design plan, once the areas have been created.

Alarm Modules

An Alarm Module will be created in the Readykey for Windows system for each door in the DOS system that had Lock Mode 5 set.

All Alarm Modules will be defined as K2015 Alarm Modules, not K2015A Alarm Event Managers.

Inputs

Alarm Module Inputs will be created, enabled, and be assigned the same time profile as programmed in the DOS system.

Outputs

The outputs on Alarm Modules on K2000-N controllers will be configured as they were in the DOS system.

Global

No information will be programmed/changed.

Workstations

No information will be programmed/changed.

Admin

Operators

System operators will be transferred, if possible, from the DOS system. The number of operators transferred will depend on the number of operators that exist already in the Readykey for Windows system. If the number of operators in the DOS system plus those in the Readykey for Windows system already exceeds the Readykey for Windows limit then a choice will be offered to add as many as possible, or all to ignore all the operators from the DOS system.

No privilege information will be set up, but any operators added will be able to access the division the DOS database is being upgraded to.

Departments / Workgroups

No department/workgroup information will be created - these facilities are unique to Readykey for Windows and will need to be programmed, if desired.

Areas / Doors

Areas will need to be created, see appropriate sections in **Installer,** described earlier.

Time Profiles / Time Periods

Time Profiles and Time Periods will be created in the Readykey for Windows system to match those programmed in the DOS system.

The Time Profiles/Time Periods will be given numeric-based names, using the number of the Time Profile/Time Period from the DOS system.

Readykey for Windows supports either 32 or 128 time profiles/time periods per division, dependent on the type of door controllers in use. The DOS systems supported 32 time profiles and 32 time periods per site - only time profiles and time periods from site one will be upgraded.

If the number of Time Profiles or Time Periods that already exist in the Readykey for Windows system, plus the number in the DOS system exceeds the limit, then the upgrade will be aborted.

Access Groups

Access Groups in Readykey for Windows may be considered to be equivalent to Access Codes in the DOS systems.

However, in the DOS systems, the Access Codes consisted of a combination of Access Levels and Time Profiles. Access Levels in turn consisted of combinations of Door Groups.

In Readykey for Windows, each Access Group consists of either one or two lists of Areas, each list with an optional Time Profile.

Because of these differences, the upgrade utility will not create any Access Groups.

Divisional Access Groups (DAGs)

This is a feature unique to Readykey for Windows. The K6000 system used a method of allowing a different Access Code to be assigned to each keyholder for each site. Readykey for Windows uses DAGs to combine Access Groups for different sites; DAGs are then assigned to keyholders.

No DAGs will be created by the upgrade utility. This will need to be setup manually, see the Divisional Access Group section of this document for detail how to configure.

Holiday

The System Holiday information (Holiday Record 1) from the DOS system will be transferred.

Transaction Routing

No information will be set up. This will need to be setup manually, see the Transaction Routing section of this document for details to configure.

Keyholders (Personnel/Visitors)

Personnel and Visitors from the DOS system will be added to the Readykey for Windows system. Visitor Start and End Dates will be transferred.

The DOS systems allowed the same keyholder to exist in both the Personnel and Visitor databases - the upgrade utility will detect and reject these - a warning will be produced for any found.

The whole name for each keyholder from the DOS system will be transferred to the **Last Name** field in Readykey for Windows. Duplicate last names will be avoided by the upgrade utility by appending a number to the end of the last name.

No Departments or Workgroups will be assigned - these are unique to Readykey for Windows.

No Access Group will be assigned to any keyholder. This will need to be setup manually, see the Personnel section of this document for details on changing the personnel assignment.

Finishing Off

When the upgrade has been completed, you may wish to repeat the process for other K6000 or K6000-AM systems, upgrading them into either the same or a different division in Readykey for Windows.

You should now verify and complete the programming of the Readykey for Windows system, using the detailed steps given in the Quick Installation section of this document.

The following items at least will need to be checked and programmed:

1. **Installer: Masters** and **Installer: Sites** - check and modify assignments of masters to workstations and sites to masters.
2. Establish communications between masters and workstations - change the System Type of K2100 'master' controllers from 1 to 2 (any K2000-AM controllers will need to be upgraded to a K2100 by purchasing a K2105); change the CNC 'Host Baud' rate from 19200 to 9600, using SW 2 switch number 7 in the CNC (refer to *Central Network Controller Installation Manual*).
3. **Installer: Controllers**. Communications to each controller need to be re-established.
4. Define the areas on each site using **Installer: Areas**.
5. The information programmed for each door, using **Installer: Doors** is correct, and assign an 'Entry Area'.
6. Time Periods and Time Profiles (if used) in **Admin: Time Profiles**.
7. Create **Access Groups** and **Divisional Access Groups (DAGs)** as required in **Admin: Access Groups** and **Admin: DAGs**.
8. Assign the correct Access Group or Divisional Access Group to each keyholder in **Personnel**.
9. Configure the privileges of each system operator in **Admin: Operators**.

