RADIONICS

READYKEY® K6100 Readykey for Windows™

System Overview

17149 Ver. 5.0

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®, Windows® 95, and MS-DOS® are registered trademarks of Microsoft Corporation

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

Pentium® is a registered trademark of Intel Corporation.

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

Table of Contents

What is Readykey for Windows?

Readykey for Windows is a PC-based access control administration system, using the latest PC operating environment - Microsoft Windows.

Readykey for Windows is a completely modular system, and can be obtained in a large number of different configurations to suit individual system requirements.

For example, this version of Readykey for Windows allows a system to be split into 128 'divisions', each with up to 128 'sites' (the next section of this document describes these terms) - you simply specify when ordering Readykey for Windows the number of divisions and sites required. In addition, the number of personnel in each division may be increased from 10,000 to 18,000 by upgrading the K2100/K1100 door controller (described later) and purchasing another Readykey for Windows software module. Additional features such as Elevator Control, Attendance Reporting, Audit Trail, Serial Interface, and Photo Identification are also separate software modules available for purchase.

The software is also available in different versions, depending on the total number of doors to be controlled - 16, 32, 64, 128, and Multi-Site (over 10,000) door versions are available. Again, modules can be purchased at any time to allow the system to be easily expanded.

Once a system has been installed, new software modules can easily be added by purchasing a 'software controlled password', which can be entered directly into the software to 'enable' the new features.

Older Readykey Systems

Radionics Readykey users have used Personal Computers (PCs) to administer their access control systems for some time. The first such system was the Readykey K6000 system followed by the smaller scale K6000-AM. The K6000 system required a computer for administration, whereas the K2000-AM could be operated either directly from the door controller, or from the computer using a PC Interface Kit.

The first Readykey for Windows product provided an administration system for a system controlling up to 32 doors and 4000 personnel, connected to the computer using the PC Interface Kit. This is an equivalent of the K6000-AM system with Office Administration Kit but with double the maximum number of doors - 32.

The next Readykey for Windows development allowed a Single Site CNC (Central Network Controller) to be used to control up to 128 doors and 10,000 personnel. This was similar to the K6000 Single Site system.

Most of the features of the K6000 Multi-site system were then added, with additional facilities for up to 128 sites (including remote sites) and up to 20 administration PCs (workstations) to be used.

Version 3.0 allowed a Readykey for Windows system to be split into 128 'divisions', each with up to 128 sites. The number of personnel in each division may now be increased to 18,000, and additional features such as Elevator Control and Photo Identification have also been added.

Readykey for Windows systems can use the latest Readykey door controllers - the K2100 and K1100 as master controllers. The K2100 door controller is a direct upgrade of the previous K2000-AM and K2000-N 4-door controllers. All K2000 door controllers can be upgraded on-site to a K2100 using a K2105 upgrade kit. The K1100 is simply a two door version of the K2100, with all the additional features and benefits. Slave door controllers may be of any type - K2100, K1100 or K2000-N.

Another upgrade kit called a K2105-18K is available which allows the memory capacity of a K2100/K1100 door controller to be increased if the number of personnel in a division exceeds 10,000. This upgrade will expand the capacity to a total of 18,000 personnel, but all door controllers on the site will need to have the same capacity. A software module will also need to be purchased (K6110-18K) to enable the feature within the Readykey for Windows system.

About the Readykey for Windows documentation

This document describes the Readykey for Windows Access Control Administration system. It should be read by any person considering using Readykey for Windows or about to install the system. It is recommended that all users or potential users should read most of this overview to gain a basic understanding of Readykey for Windows, the components and ideas behind planning, designing and administering a successful access control administration system using Readykey for Windows.

The following documents describe other aspects of the system:

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

Readykey Central Network Controller Installation Manual
This document is supplied with the Readykey Central Network Controller (CNC) which may be used as the master controller on some Readykey for Windows systems.

Readykey for Windows PC Specification
This defines the type of PC you need for running Readykey for Windows.

Readykey for Windows Software Installation Manual
This describes the installation of the Readykey for Windows software for non-networked PCs including preparation of the PC.

Readykey for Windows Programming Sheets
These are designed to assist with the programming of the Readykey for Windows Software - they should be completed by the person responsible for designing the Readykey for Windows system. Once completed, they will simplify the programming of the information into Readykey for Windows.

Readykey for Windows System Programming Manual
This describes the installation and programming of a Readykey for Windows system:

- The first section summarizes the installation process, giving a brief description of each step.
- Installers new to Readykey for Windows will also need to refer to the second section, which provides a detailed explanation of each step.

On completion of reading this manual, the installation and programming of the system should be complete to a stage where a key/card with access through all doors on all sites has been achieved.

Readykey for Windows Multi-PC Installation Manual
This describes the configuration of PCs across a network to administer Readykey for Windows including preparation of the PCs and installation of the software.

Readykey for Windows Network Operational Overview and Requirements
This document describes, in depth, the network requirements needed to administer Readykey for Windows across multiple PCs within the network environment.

Readykey for Windows Alarm Graphics Datasheet,
Readykey for Windows ASCII Transaction File Datasheet
Readykey for Windows Attendance Report Datasheet
Readykey for Windows Elevator Control Datasheet
Readykey for Windows DDE Output Datasheet

Readykey for Windows Photo-ID Module Datasheet
Readykey for Windows Serial Interface Module Datasheet
Readykey for Windows Audit Trail Module Datasheet
Readykey for Windows Alarm Sound Support Datasheet

These documents describe the operation of the additional modules available. The Alarm Graphics, ASCII Transaction and DDE Output facilities are provided as standard with all Readykey for Windows systems. Other software modules may be purchased from Radionics at additional cost. You should read the appropriate datasheet(s) for any modules you have purchased or intend to use.

Readykey for Windows On-Line Help

One of the major features of Readykey for Windows is the On-Line Help facility. At any point while operating Readykey for Windows you may ask for help, by clicking a Help button or making a menu selection. The help provided will always be relevant to the area you are working in and will also allow you to jump to other subjects, or topics that may be of interest.

A lot of the detail of this overview is included in the on-line Help. Topics can also be printed if required.

Readykey for Windows User Instructions

This document describes in simple terms how to use Readykey for Windows on a daily basis, and covers routine tasks such as adding and deleting keys, searching transactions, etc.

Contents of this Overview

This overview document is designed to be used in two ways:

- As a pre-sales aid, to help you decide how Readykey for Windows can be used to the best advantage to control access in your building or buildings.
- As an introduction to a Readykey for Windows system for installers, to describe how the software works and should be used.

It has the following sections:

What is Readykey for Windows?

Describes the background to the development of Readykey's Microsoft Windows based administration system, and discusses what Readykey for Windows is all about.

System Design

This section allows you to see what can be achieved with Readykey for Windows, and will help you decide how your own Readykey for Windows system will be constructed - including what equipment will be required and how it will connect together. Topics covered in this section include:

Sites

Each division will consist of one or more sites. This section explains what a site is, and the different types of site and communication methods available.

Divisions

A Readykey for Windows system will consist of one or more divisions. Each division may be regarded as an independent part of the system.

Masters

The PC or PCs on any Readykey for Windows system communicate to the door controllers through a master - this will either be a Readykey CNC or K2100/K1100 door controller.

Multi-PC Systems

This section explains how more than one PC may be used to administer a Readykey for Windows system, and the equipment required to achieve this.

Equipment Overview

This section describes the equipment required for a Readykey for Windows system, including PC Specifications, the Readykey Equipment and how to order the Readykey for Windows software itself.

Setting Up Readykey for Windows

This section will be of particular use to somebody about to configure a Readykey for Windows system. The steps necessary to prepare for administering a new system are detailed here.

Using Readykey for Windows

The day-to-day use of Readykey for Windows is outlined here. It will give you some idea of how the system works on a routine basis.

Multi-PC Systems

This section describes how more than one workstation can be used to administer a single Readykey for Windows system using a Local Area Network, and what is required to achieve this.

Security

Discusses prevention of unauthorized use of the system as well as ensuring the physical security of your database.

System Specification

Lists the various features of the system.

Appendix A: Glossary

A list of terms used in this overview, and throughout the Readykey for Windows system.

What to read after the Overview

After reading the relevant sections of this overview, you should use the rest of the Readykey for Windows documentation in the order described below to enable you to install and complete commissioning of the system:

1. The first step is to either buy a PC or check that the PC you intend using is capable of running Readykey for Windows. The PC specification is given in the *Readykey for Windows PC Specification* datasheet.
2. The next step in installing any Readykey for Windows system is to install the software onto the PC or PCs which will be used to administer the system.

If the Readykey for Windows system is going to be administered from a single PC only, then refer to the *Readykey for Windows Software Installation Manual.* However, if more than one PC is going to be used to administer a system, via a local area network, then you should refer instead to the *Readykey for Windows Multi-PC Installation Manual and the Readykey for Windows Network Operational Overview and Requirements document.*

3. Once the software is successfully installed onto the PC(s), you can then start to configure the system and connect the Readykey hardware (CNC, PC Interface Kits and door controllers). The *Readykey for Windows System Programming Manual* will help you to do this, describing each step in detail.
4. On completion of reading the *Readykey for Windows System Programming Manual*, you will have tested all the system, and have added ID devices (keys/cards) with access through all readers on the system.
5. The *Readykey for Windows User Instructions* describe routine tasks in administering a Readykey for Windows system, including adding and deleting keys/cards, dealing with alarms, etc.
6. The *Readykey for Windows On-Line Help* is a powerful facility that allows help to be summoned at the press of the F1 key on the keyboard or the click of the mouse on the 'Help' buttons within Readykey for Windows itself. The help given will be specific to the task you are performing at the current time. You can easily search for help on other topics, and the help given on any topic can be printed if required.
7. A number of other datasheets describe a number of special facilities and the optional modules available in Readykey for Windows. These include Alarm Graphics, the ASCII Transaction File, Attendance Reports, Photo-ID Module, Serial Interface, Audit Trail, Alarm Sound Support and Elevator Control.

System Design

This section is designed to help you decide which Readykey equipment and Readykey for Windows software is required for your individual requirements.

Readykey for Windows is an extremely versatile system, with many possible configurations, to enable it to meet a wide-range of installation requirements.

This means that there are a number of decisions that need to be made to ensure that the system is designed and configured correctly. Many installations will be extremely simple in nature, controlling up to 128 doors in a single building from a single PC. This section is therefore divided into two areas - the first to help you design these 'simple' systems, the second for other higher level systems, and explaining what can be achieved, and how.

When designing the Readykey for Windows system, you should complete the *Readykey for Windows Programming Sheets* - these will then assist with the final programming and commissioning of the system.

Simple Systems

Note: These systems assume that all communications links between the PC, PC Interface Kit or CNC and door controllers can be hard-wired.

These systems assume a maximum of 10,000 personnel, or 18,000 if K2100/K1100 controllers are upgraded (see Other Systems: Personnel, described later).

These systems can be enhanced easily, by using the information in the next section. For example, a 16 door system could be administered from two workstations by using the information provided in the 'Workstations' section.

1. Up to 32 doors

A PC Interface Kit may be used to connect the Readykey for Windows administration PC to a ‘master’ K2100/K1100 door controller. This can control a maximum of 32 doors. You can connect the doors to a total of 8 door controllers (using K2100s, one master and seven slaves, four doors per controller).The Master controller is connected up to a maximum of 7 Slave door controllers via a six wire data bus (6WB), or by using a K21232 6WB/RS-232 converter which can convert the 6WB to RS-232 for other communication methods.

This type of configuration can use a total of 8 door controllers. . A simple method of determining the maximum number of door controllers (addresses) within a system is to divide the maximum number of doors allowed by four. In a 1-16 door system the maximum number of door controllers (addresses) is four. As each K2100 can control a maximum of four doors this gives a total of 16 doors if four K2100s were used. Similarly, on a 1-32 door system the maximum number of door controllers (addresses) is eight giving a maximum of 32 doors using eight K2100s. The use of K1100s (2-door controllers) will reduce the total number of doors that can be achieved

The maximum distance from the K6100-PC PC Interface Kit to the master door controller is 3000 feet/1km, using 4-core cable.

The Six Wire Bus (6WB) is a 6-core cable that can be a maximum of 3000 feet/1km overall length, with a maximum of 1500 feet/500m between any two door controllers on the bus.

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.

The K6100-PC PC Interface Kit is supplied with a desktop Readykey (proximity) reader. However, a Wiegand Interface may be used in place of the desktop reader dependent on the type of ID device being used for administration purposes.

Note: If a high transaction rate (i.e. large number of keyholders using system at certain times of day) is expected, then the use of a CNC option is recommended for enhanced performance.

2. Up to 128 doors

A Readykey Central Network Controller (CNC) is used to connect the PC to a maximum of 32 slave door controllers, via the Readykey Six Wire Bus. The total number of door controller addresses that can be used in this single CNC configuration is 32 - one for each slave door controller. If all K2100s are used, that would equal a total of 128 doors. The use of K1100s (2-door controllers) will reduce the total number of doors that can be achieved by using an address within the system configuration.

The maximum total length of the Six Wire Bus (6WB) is 3000 feet/1km, with a maximum of 1500 feet/500m between any two devices on the bus (CNC and door controllers).

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.

Other Systems

This section describes the different stages involved in designing a Readykey for Windows system. At the end of this process, you should know how the different parts of your Readykey for Windows system will operate, and what Readykey equipment and software you need to order.

Stage 1 - Personnel

The first factor to establish is how many keyholders are going to use the Readykey for Windows system. Normally Readykey for Windows allows up to 10,000 personnel and 750 visitors on a system. However, this number can be affected in several ways:

- K2100, K1100 and K2000-N controllers can be upgraded to allow 18,000 personnel. However, **all** door controllers in the division must be upgraded to achieve this increase.
- Additional divisions can be used if the Readykey for Windows system is administering access control at a number of different physical locations, and the keyholders for each site are largely unique. If divisions are used, then the maximum number of keyholders stated above for a system become **per division**.

Stage 2 - Doors

The next step is to establish how many readers are going to be used in the access control system. Generally this will be the number of physical doors being controlled.

However, some doors may be installed with two readers, one on each side, to control access in both directions through the door. In this case, the two readers will normally become two 'doors' in the Readykey for Windows system so the direction of traffic can be determined. A K2040 Reader Combiner may be used to combine two readers into one door channel if it is not necessary to determine the direction of traffic.

Readykey for Windows is sold in different versions dependent on the total number of doors being controlled: 16, 32, 64, 128, and two versions of Multi-Site (3 sites with up to 192 doors, or 128 sites with over 10,000 doors).

Stage 3 - Sites

What is a 'Site'?

A site is a set of one or more door controllers that share a common communications route to a master. Generally each site will be in a separate physical location, although, due to certain system limits, it may be necessary to deviate from this.

This section allows you to determine how many sites will exist in your Readykey for Windows system, and how each site will communicate to Readykey for Windows.

Communications Methods

Two methods of communication to sites are used in Readykey for Windows systems:

Six Wire Bus
The Six Wire Bus (6WB) is Readykey's own communications format. This uses 6 core unscreened signal cable, 22ga or 18ga. to connect the CNC and/or door controllers.

The distance between any two door controllers on the bus must not exceed 1500 feet/500m, and the overall bus length must not exceed 3000 feet/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.

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

Types of Site

There are four basic types of site available, which are described here. However, one of the types has a number of different variations.

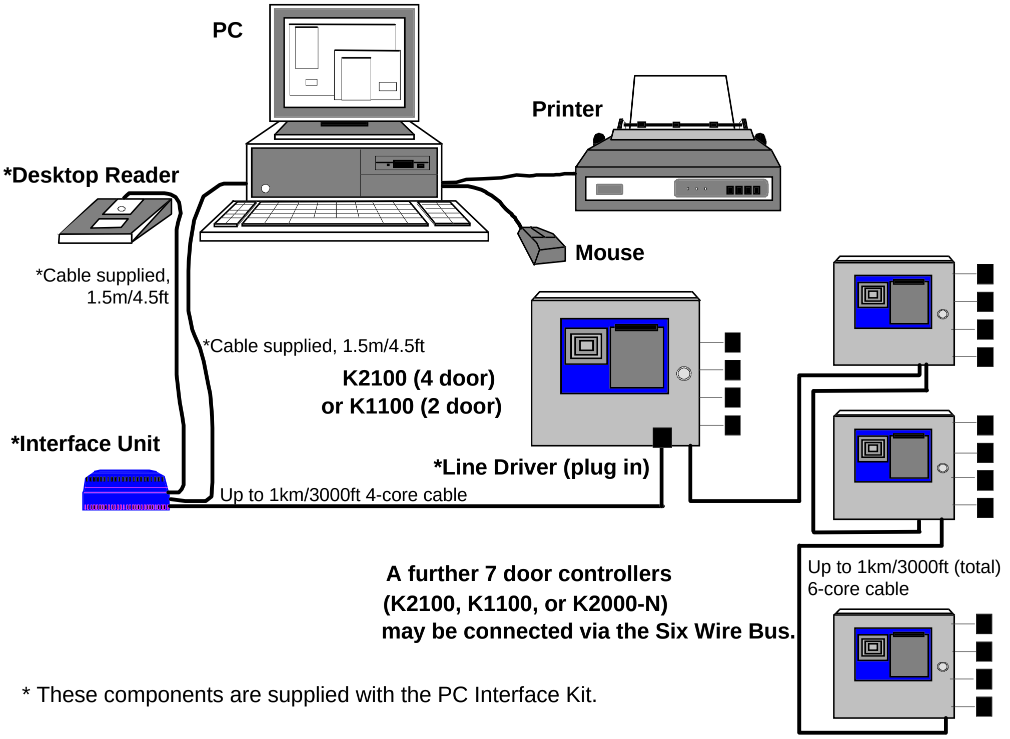
Site Type 1. PC Interface Kit connected to K2100 or K1100 Master Controller

This type of site consists of a PC Interface Kit connected to a workstation (PC) on the system. A line driver (supplied with the PC Interface Kit) is plugged into the master controller, which in this case is a K2100 or K1100. A four wire cable connects the interface kit to the line driver.

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.

Up to seven additional slave door controllers may be connected to the master controller using the Readykey Six Wire Bus. These door controllers can be of any type - K2100, K1100 or K2000-N. This type of configuration can use a total of 8 door controllers. The use of K1100s (2- door controllers) will reduce the total number of doors that can be achieved by using a door controller address.

This site type supports a maximum of 32 doors.


PC
Printer
*Desktop Reader
Mouse
*Cable supplied, 1.5m/4.5ft
*Cable supplied, 1.5m/4.5ft
K2100 (4 door)
or K1100 (2 door)
*Interface Unit
*Line Driver (plug in)
Up to 1km/3000ft 4-core cable
A further 7 door controllers
(K2100, K1100, or K2000-N)
may be connected via the Six Wire Bus.
Up to 1km/3000ft (total)
6-core cable

* These components are supplied with the PC Interface Kit.

Site Type 2. K2100 or K1100 Master Controller directly connected to PC

This type of site is similar to the one above, except that the line driver communications from the PC Interface Kit to the K2100/K1100 is not used. Instead the master door controller is linked directly to the serial port of the PC using an RS-232 link. If the distance from the PC to the master K2100 or K1100 is greater than 30 feet/15m, then this may be extended by the use of line drivers, short/long haul modems, fiber optics, etc. A 3 or 5 wire connection may be used to achieve this, depending upon configuration.

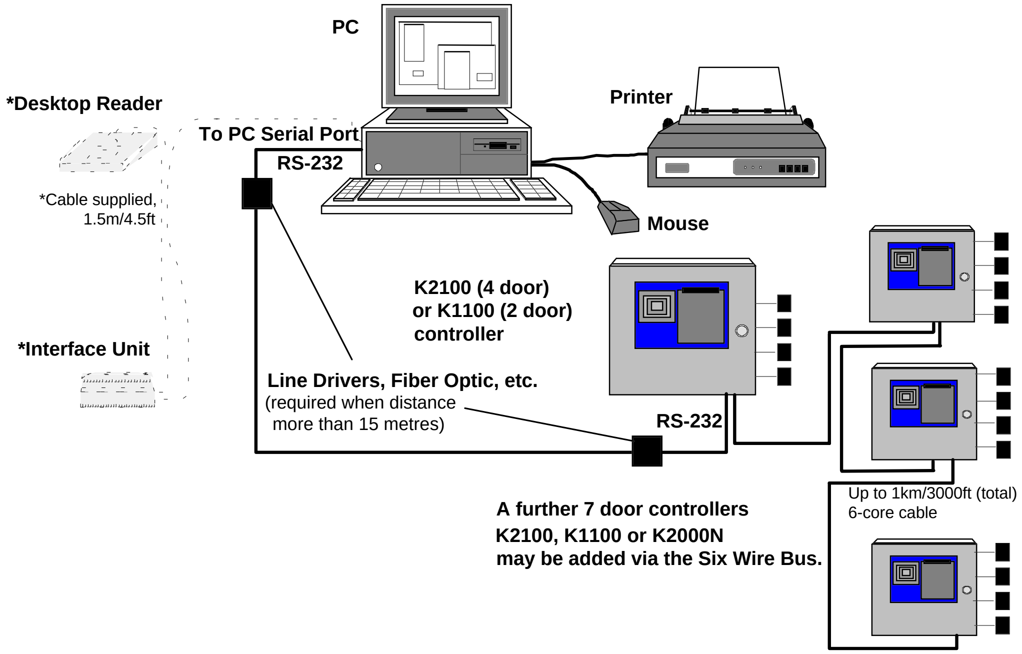
Note: It is recommended to use a six wire cable for the connection between the PC and master control, to allow for ease of future expansion.

This type of site would commonly be used if an existing RS-232 communications link were in place between the PC and the master door controller locations.

Again, this site type supports a maximum of 32 doors.

Notes:

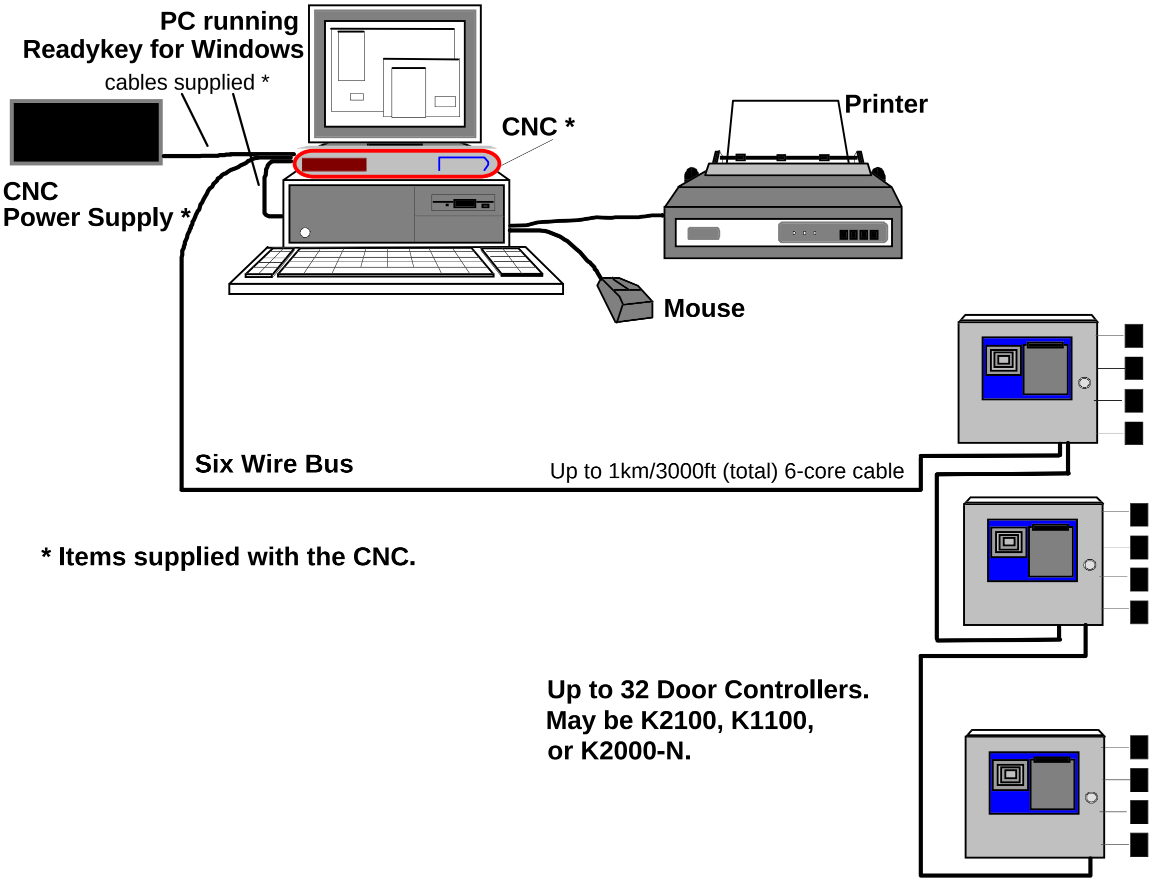
1. Dial up modems cannot be used.
2. This type of site does not provide an easy means of ID device administration. The user must either manually type into the system an ID device serial number or use the option of a PC Interface Kit. A PC Interface Kit with a desktop reader (Readykey Proximity, or Wiegand Interface with a Wiegand reader) would therefore be required, unless other sites which use a PC Interface Kit or CNC communicate to the same PC.



Site Type 3. Site using Six Wire Bus from a Central Network Controller
A Readykey Central Network Controller (K6100-CNC or K6100-CNCII) is connected to a workstation on the system.

Up to 32 slave door controllers are connected to the CNC using the Readykey Six Wire Bus (six wire cable 22ga or 18ga). These door controllers can be of any type - K2100, K1100, K2000-N. This type of configuration can use a total of 32 door controllers. The use of K1100s (two door controllers) will reduce the total number of doors that can be achieved by using a door controller address.

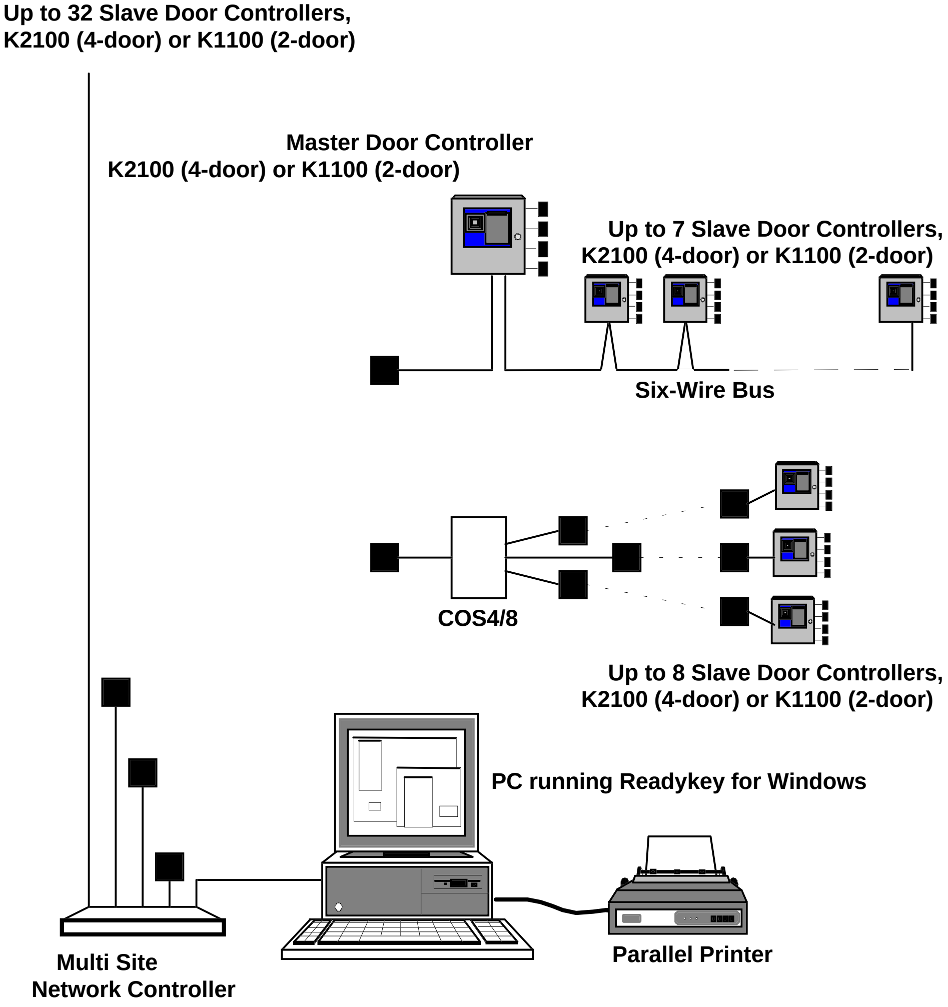
Up to 128 doors are available on a site of this type.



Note: It is possible to have as many as 4 CNCs on a single PC. However, each CNC requires one of the first four serial ports (COM1 - COM4) and each of the COM ports must have a separate IRQ number. Contact your computer hardware supplier for more information on COM ports and IRQ settings. If the COM ports are used for other equipment then this will reduce the possible number of CNCs.

Site Type 4. Site using RS-232 to communicate to Readykey CNC

A Readykey CNC has three serial (RS-232) ports any or all of which can be used for communications to a site using one or more of the four methods below. The diagram below shows the general configuration for some of these types of site.


Up to 32 Slave Door Controllers,
K2100 (4-door) or K1100 (2-door)
Master Door Controller
K2100 (4-door) or K1100 (2-door)
Up to 7 Slave Door Controllers,
K2100 (4-door) or K1100 (2-door)
Six-Wire Bus
COS4/8
Up to 8 Slave Door Controllers,
K2100 (4-door) or K1100 (2-door)
PC running Readykey for Windows
Parallel Printer
Multi Site
Network Controller

■ **Modem or Line Driver, only required when link is longer than 15m/45 ft**

Site Type 4a. Direct RS-232 Cluster

The link between the CNC and the master door controller is hard-wired, possibly using line drivers, fiber-optic, or ethernet TCP/IP communication devices, etc. Further information on suitable communication methods and equipment can be found in *Readykey Central Network Controller Installation Manual*. For Ethernet TCP/IP communication devices Lantronix Micro Serial Servers can be used.

If a K2100 or K1100 master controller is connected to the remote end of the RS-232 link, then up to an additional seven slave door controllers may be connected to the master controller using the Readykey Six Wire Bus. The slave door controllers can be of any type - K2100, K1100 or K2000-N. This type of configuration can use a total of 8 door controllers. The use of K1100s (two door controllers) will reduce the total number of doors that can be achieved.

This site type supports a maximum of 32 doors.

Site Type 4b. Direct RS-232 & Dataswitch

This is another special case of the ‘Direct RS-232’ site type. A dataswitch is used to connect up to eight door controllers at the remote site.

This type of site is commonly used on systems where all the door controllers on the site are K2000-N, since this type of controller does not support a local six wire bus connection to additional door controllers at the remote site as used in the ‘Direct RS-232 Cluster’ site type. It may also be used when the distance to the additional door controllers exceeds the limits of the six wire bus (see Communications Methods). In this case line drivers may be used from the dataswitch to the door controllers.

This site type supports a maximum of 32 doors.

Site Type 4c. CNC & Dial Up Modem Cluster

This type of site is commonly used when a door controller is at a remote location, and it is not practical, or economical, to install a wired link (either Six Wire Bus or RS-232) to the site.

If the door controller connected directly to the modem is a K2100 or K1100 controller, a local six wire bus may be established. In this case, up to an additional seven slave door controllers may be connected to the master door controller using the Readykey six wire bus. These door controllers can be of any type - K2100, K1100, K2000-N. This type of configuration can use a total of 8 door controllers. The use of K1100s (two door controllers) will reduce the total number of doors that can be achieved.

This site type supports a maximum of 32 doors.

Site Type 4d. CNC & Dial Up Modem & Dataswitch

This type of site is another special case of the ‘Dial Up Modem Cluster’ site type.

Up to eight door controllers are connected to a modem, via either a four or eight-way dataswitch. The cable distances are only limited by the type of line drivers used.

The main disadvantage of this type of site is that the dialback facility (described later) of the K2100 and K1100 controllers **cannot** be used. This type of configuration can use a total of 8 door controllers. The use of K1100s (two door controllers) will reduce the total number of doors that can be achieved.

This site type supports a maximum of 32 doors.

Dial-Up Sites - Operation

One modem is connected to the CNC and another to a door controller at the remote site. The telephone number of the modem at the remote site is specified to the Readykey for Windows system. It is possible to specify either one or two times during a 24 hour period at which the site will be automatically dialed by the CNC. Once communications are established, any database changes (updates) for the site will be transmitted and any events (transactions) which have occurred at the site will be automatically received by the CNC from the door controller.

Following any communications to the remote site, the time that the CNC will remain on line is controlled by two factors:

- If no transactions or updates are sent for two minutes, then communications will cease.
- If the maximum ‘Duration’ (configured in the Readykey for Windows software) is exceeded, then communications will be terminated, regardless of whether any transactions or updates remain outstanding.

As well as the automatic twice daily dialing of the site, an operator may ‘Force Dial’ the site at any time. This facility would be used if, for example, a key/card had been added for a visitor to a site, and the visitor wished to use the key/card before the next scheduled dialup time.

One modem at the CNC may communicate to different sites at different times of day.

An advantage of using a K2100 or K1100 controller connected directly to the modem is that transactions are reported to the PC in order of priority. High priority transactions (Unauthorized Access, Anti-Tamper etc.) are always transmitted back to the CNC and Readykey for Windows software before more routine transactions (e.g. Access Authorized, Request to Exit, etc.).

Dial back
This is a special facility that may be used if the type of controller connected directly to the modem is a K2100 or K1100. In the event of a high priority (Alarm) transaction occurring at the remote site, the door controller can be programmed so that it initiates a communications session to the CNC.

It should be noted, however, that in this case ONLY THE HIGH PRIORITY (ALARM) TRANSACTIONS ARE REPORTED TO THE CNC. Any low priority transactions will not be sent until the next routine communications session, initiated by the CNC.

It is recommended to have a dedicated modem connected to the CNC specifically for handling dialbacks, so that dialbacks can take place without being affected by any routine communications session.

Site Design

Now you are aware of the different types of site available, and how they may be used, you need to consider how these will be used in your Readykey for Windows system:

1. The first stage is to consider the 'logical' number of sites - this will be the number of physical locations in which access control will be installed. For example, a company may be installing Readykey for Windows to control access at their Head Office in Los Angeles, and at regional offices in San Francisco and Burbank. In this case, the logical number of sites would be three.
2. The next stage is to determine the communications method to each site - for the example above assume that there is a suitable fiber-optic link from the Head Office to the Burbank office, but that the PSTN will be used to communicate to San Francisco.
3. Thirdly, the number of doors to be controlled on each site need to be calculated. Let us assume that for our example there are 35 doors to be controlled at each of the San Francisco and Los Angeles offices, and 17 at the Burbank office.
4. The fourth stage is to decide the site type for each site, based on the communications method and number of doors.

   In our example, the Los Angeles office will use the Six Wire Bus from a CNC, and the Burbank office will be a 'Direct RS-232 Cluster'. However, the San Francisco office presents us with a problem, as the number of doors to be controlled (35) exceeds the number available for the 'Dial-Up Modem Cluster' site type (32).

   To solve this we need to divide the San Francisco office into two Dial-Up Modem Cluster 'sites' - one with 32 doors, the other with 3 doors (or some other combination).
5. Additional sites may need to included in the total required to meet solutions such as those in the Los Angeles solution mentioned earlier.
6. Calculate the total number of sites on the whole system.
7. Readykey for Windows is supplied with one site as standard unless the K6100-MS or K6100-MS3 has been purchased. If a second site is required then this must be ordered separately. Additional sites must then also be ordered separately up to a maximum of 128 sites total. See the section described later, Ordering the Readykey for Windows software for ordering information.

Stage 4 - Door Controllers

Your access control system will consist of a number of door controllers. When a keyholder uses their ID device with a reader, the code in the card is passed to the door controller, which then decides whether access is allowed at the current time and day.

K2100 door controllers generally control up to four readers, and the K1100 controls up to two readers.

The next stage in designing your Readykey for Windows system is to decide how many door controllers are required on each of the sites.

Calculate the number of door controllers of each type to be used on each of the sites, taking into consideration the number of doors to be controlled on each site.

Using K2000-N Controllers

The K2100 and K1100 are Readykey's latest door controllers, and allow the full features and benefits of Readykey for Windows to be used. However, the older K2000-N controllers can be used under most circumstances.

However, the following should be noted:

- Relays are not programmable on the K2000-N controllers
- The number of time profiles and time periods per division is 128 when all the door controllers in the division are K2100 or K1100 version 3.0 or higher. If any controllers in the division are K2000-Ns, then the number of time profiles and time periods will be limited to 32 of each.

Note: The first door controller connected either directly to the PC, via a PC Interface Kit, or in any of the 'non-dataswitch cluster' site types must be a K2100 or K1100.

18,000 Personnel

If the number of personnel in any division of a Readykey for Windows system is to exceed 10,000, then:

- All door controllers in the division must have the larger memory capacity, available by purchasing an upgrade kit from Radionics, (part number K2105-18K) for each controller.
- The Readykey for Windows 18,000 personnel software module (K6110-18K) must also have been purchased.

Stage 5 - Network Masters

This term is used to describe a Readykey CNC or a K2100/K1100, which is connected either directly to a PC or via a PC Interface Kit. Sometimes this term is abbreviated to 'Master'.

This should not be confused with a Supervisor key/card, which may have been defined, or a 'Remote Master', which may exist on an RS-232 'cluster' site.

It is possible to have up to 20 masters on your system. These can be all the same type or of different types. All sites communicate to a PC on the system through a master.

This stage of the system design involves deciding which sites are going to communicate to each master.

In our example, the San Francisco and Burbank sites will communicate to a CNC master installed at the Los Angeles office.

Stage 6 - Workstations

Any Readykey for Windows system may be administered from several workstations (PCs) which are connected via a Local Area Network (LAN) or Peer to Peer Network.

One of the workstations has all the Readykey for Windows application and database files installed, the others, which are to be used for system administration, have a smaller number of files.

Transactions which occur on the system may be displayed at some or all of the workstations.

Each workstation may have one or more masters connected to it. Alternatively, even if a workstation does not have a master connected to it, a PC Interface Kit will normally be installed to allow for administration at that workstation if ID devices need to be added at the workstation.

In our example, the company requires two workstations for administration of the access control system located at the Los Angeles office, one in the personnel office for staff ID device administration and the production of staff attendance reports, the second in a 24-hour manned security office for monitoring of the sites outside office hours. These two workstations will be connected via a Local Area Network (LAN)or Peer to Peer Network. The workstation in the personnel office will have the CNC master connected to it. A PC Interface Kit is connected to the workstation in the security office for acknowledgment of alarms and administration of visitor keys/cards.

Further information on multiple workstation systems and networks is contained in the section 'Multi-Workstation Systems' later in this overview. All Multi-Workstation systems must be configured according to the specifications described within the Multi-PC Installation Manual.

Stage 7 - Divisions

A Readykey for Windows system may be split into 'divisions'. A division is a database that consists of one or more sites, up to 128 sites total.

Each division will have its own personnel records, key/card and access information which will be stored in the door controllers on the site. Personnel information may be copied between divisions (databases).

Most Readykey for Windows systems will only have one division (database). However, on large systems it may be required to administer independent Readykey for Windows installations from a central point.

Using divisions can simplify the administration of Readykey for Windows systems with a large number of sites and keyholders.

For our example, we could split the system into three divisions, one for each of the offices in our example earlier. However, this would only be a sensible option if the majority of the keyholders only work at one of the offices.

Some keyholders may exist in more than one division (database) using a utility in the Personnel application to copy keyholders between divisions (databases). For example, senior management may visit each of the branch offices from time to time - they would have access and other information stored in each division (database).

System Operators may be restricted as to which divisions (databases) they can edit and view database information. It is also possible to configure the system such that only transactions for certain divisions (databases) are displayed at each workstation.

Each site may be a part of **one division (database) only**. Hence the number of divisions (databases) cannot exceed the total number of sites.

Note: Even on a multiple-division (database) system all the information is still stored centrally.

Readykey for Windows is supplied with one division (database) as standard. If a second division (database) is required then this must be ordered separately. Additional divisions (databases), a K6110-DV must then also be purchased separately. See the section described later, Ordering the Readykey for Windows software for ordering information.

Readers

There are a variety of different Readykey readers, all usually mounted next to the door and used to identify electronic keys/cards. All readers may be up to 1 km/3000 ft from the Door Controller.

Some examples of special 'readers' are given next:

- **Readykey K2001-P PIN Reader:** in addition to reading keys/cards this reader may also require a PIN number to be entered before granting access. The latest versions of this reader allow the requirement for PIN entry to be restricted to certain times by a time profile. For instance, during normal office hours a key/card only is required, outside hours a key/card plus PIN is needed. The PIN number is not programmable, the number is contained within the electronic key/card.
- **Wiegand Interface:** this special interface allows other manufacturer's identification devices to be used with Readykey Door Controllers and administration systems. The interface accepts the output from Wiegand 26 bit compatible devices, such as card readers, hands-free readers, etc. and produces Readykey key/card codes. For administration purposes the Readykey PC Interface Kit is used and a Wiegand Interface with a Wiegand reader is used in place of the desktop reader. If using a CNC-based system, or any system which has mixed Readykey and Wiegand devices, then an additional PC Interface Kit, unless the K6100-CNCII is used, can be installed on a second serial port on the PC. The Wiegand Interface is not limited to just Wiegand 26 bit format readers, it can be used for a large number of formats available on the market. Formats other than Wiegand 26 bit, must be used with a K6100-CNCII or with a PC Interface Kit with a wiegand interface and corresponding wiegand reader, to read the ID Device number into the system.

Note: A second PC Interface may require the addition of a second or third serial port to your PC.

Other Items - All Systems

- **Request to Exit:** a motion detector, switch, or push button on the secure side of the door that allows people to leave an area.
- **K2015A Alarm Event Manager:** a device that may monitor up to 8 additional alarm points. These may be fire doors, motion detectors, environmental monitoring etc. Responses may be made through 1 to 8 relays on the alarm module as well as an alarm being reported at the PC. The alarm inputs can be grouped into alarm areas in Readykey for Windows. Operators can then arm and disarm alarm-areas
- **K2050 Alarm/Access Integration Module:** a device that is used on main entrances into an alarm protected area which allows the alarm system to disarm when authorized personnel enter the building. In addition, this module will restrict unauthorized personnel from entering the building if they do not have the authority to disarm the alarm system.
- **K2051 Access Prohibitor Module:** a device used in conjunction with the K2050 module to prohibit access through other doors on the system until the alarm system is disarmed.

Equipment Overview

The previous section should have enabled you to create a plan of what your Readykey for Windows system will look like, and how the various components connect together.

This section briefly describes the equipment used on a Readykey for Windows administered access control system. For full details on installing Readykey equipment see the *K2100/K1100 Installation Manual,* the *Readykey Central Network Controller Installation Manual,* and the *Readykey for Windows K2015A Installation Manuals.*

Your Readykey for Windows system will consist of one or more sites.

The different types of site use different equipment:

- A Readykey Central Network Controller, or CNC, can control communications to up to 32 door controllers via the Readykey Six Wire Bus. This allows a maximum of 128 doors to be administered.
- A Readykey CNC can also communicate to sites via RS-232. Each site has a maximum of 32 doors.

Note: A single Readykey Multi-Site Network Controller is capable of communicating to one Six Wire Bus site and 127 dial up modem sites. Of the 127 modem sites, 32 may have eight door controllers and 95 a single door controller, unless the K6100-CNCII is used. If the K6100-CNCII is used all, remote dial up sites may be 32 doors each. For direct RS-232 connection, a total of one Six Wire Bus site and three direct RS-232 connect sites may be used.

- A PC Interface Kit directly connected to a workstation and a K2100 or K1100 master door controller. The K2100 or K1100 is the master. This configuration allows up to 32 doors to be administered using up to 8 door controllers.
- It is also possible to connect a K2100 or K1100 master door controller directly to the serial port of the workstation, without using a PC Interface Kit. However, since this does not provide a means of key/card administration, this type of site may only be used on systems where there is another means of administration - i.e. a PC Interface Kit or CNC.

Configurations which combine any or all of the above are possible. When ordering your Readykey for Windows system you will need to specify the base system desired which will incorporate the number of doors required. The number of divisions (databases), sites, and personnel you intend to use on your system. The system can then be increased at a later date by purchasing additional 'software modules and components'.

Note: Multi-Divisional (database) systems require the use of multiple sites. The second Division (database) must have an alternate means of communication to the door controllers on the site.

Further information to help you correctly order your Readykey for Windows system is in the section described later, Ordering the Readykey for Windows Software.

PC Specification

Use the following information to select a suitable PC. To confirm that it is of the right specification refer to the *Readykey for Windows PC Specification*.

Note: No information is provided here regarding the specification for a File Server. Setting up a Server-based network requires specialist knowledge from a qualified computer professional.

Here are some pointers that will help you select the best system:

- The type and speed of the processor will determine the overall performance of the system. The faster the processor the better the speed.
- Windows performs better with more RAM, the recommended minimum is 32 Mbytes when using Readykey for Windows , the more the better. Make sure when purchasing a system that there is room for RAM expansion, up to at least 64 Mbytes. It is better to spend money on increasing the memory of a PC than to improve the processing power.
- Usually the larger the hard disk the better its performance. We recommend a minimum of 1Gbyte.
- A good quality color display should be used, preferably a 'SuperVGA' monitor with a resolution of 800x600 pixels (dots). For the Photo ID module you will also need a graphics card capable of a minimum of 32,767 colors.
- If you want to use the Alarm Sound Support and receive audible confirmation for alarms then you will need a PC sound card and speakers. All Windows compatible PC sound cards are compatible with Readykey for Windows.
- Readykey for Windows requires a mouse, or other pointing device, to be used.
- Most PCs are now supplied with MS-DOS and Windows, Windows 95, Windows 98, or Windows NT4.0 already installed.

In general, the more doors and personnel you will have on your system, the higher the PC specification you should have. Factors that may affect the choice of PC for your Readykey for Windows system include:

- Number of personnel
- Total number of sites
- Number of divisions
- Whether the Photo-ID module, Serial Interface ,or Alarm Sound Support are being used, or intended to be used in the future. If they are, then you many need a PC with 2 serial and 2 parallel ports for digital cameras, CNCs, and Direct PVC printers. Check with the manufacturers of the equipment for their requirements.
- How 'busy' the system is likely to be - this will depend largely on the number of keyholders and doors, but there may be other factors - e.g. some times of day may be busier than others, etc.
- Windows version -The recommended version to use would be Windows 95, Windows 98, or Windows NT. Use Windows for Workgroups 3.11 for older PCs that cannot run a more recent version of Windows.

Recommended Specification

Note: If a PC of a lower specification is used then the performance of Readykey for Windows will be reduced and the ability to run other programs simultaneously may be restricted.

.Processor:	**IBM compatible Pentium 166MHz**
RAM:	**Minimum32 Mbytes**
Hard Disk:	**Minimum 1.0 Gbytes**
Floppy Disk:	**3½" High Density**
CD Disk Drive	**Standard CD ROM Drive, 2x speed or greater**
Display:	**Color SuperVGA (800x600) - 256 colors (32,767 with Photo ID module)**
Ports:	**1 parallel (LPT1), 2 serial (plus, if necessary, extra ports for an ID card printer, digital camera and Serial Interface)**
Mouse:	***Windows supported**
Printer:	***Windows supported**
MS-DOS:	**Version 5.0 or later**
Windows:	‡ **Version 3.1, 3.11, Windows 95 (preferred), Windows 98, or Windows NT Version 4.0**
Network Card:	***Windows supported (only required for multi-PC sites)**

*** Windows supported** means any device that is compatible with Windows. When Windows is installed you will be required to tell it what types of printer and mouse are connected. If the particular make or model is not listed by Windows then the printer or mouse will almost certainly be compatible with one of the standard types, e.g. Microsoft Serial for the mouse; Epson, IBM or Hewlett Packard for printers.

‡ **Windows Version:** If you are intending to have more than one workstation on your system, then all your workstations **MUST** be running Windows for Workgroups 3.11, Windows 95, Windows 98, or Windows NT. All workstations must be running the same Windows operating system.

Readykey for Windows will operate on PCs running Windows 95, Windows 98, or Windows NT. If Windows 95, or Windows 98 is being used, then the PC should be installed with at least 16 Mbytes of RAM. If Windows NT is being used, then it must be version 4.0, build 1381 or later, and the PC specification should meet the Microsoft requirements for NT. Consult Microsoft Corporation or your computer provider to ensure that the proper Microsoft Window NT specifications have been met on your system.

As mentioned earlier, Windows for Workgroups 3.11 provides superior performance over Windows 3.1. At present time of this documentation Microsoft Windows 95 is considered the preferred operating system and will produce the best system performance.

Multiple PC Systems

All the workstations should meet the specification given earlier. In particular, **ALL the workstations must have Windows for Workgroups 3.11, Windows 95, Windows 98, or Windows NT** installed. All workstations must be running the same type of Windows operating system.

The workstation which has the Readykey for Windows database and application files stored on it (the Readykey Server) should be a high specification PC - further information on PC Specifications for Multiple PC Readykey for Windows systems is included in *Readykey for Windows Multi-PC Installation Manual and Readykey for Windows Network Operational Overview and Requirements document*.

Printers

As stated earlier any Windows supported printer may be used. However you **must** use a dot-matrix type printer for transaction printing that gives an immediate on-line report of events, a laser printer will give one line per page! If you are using Windows NT, a laser printer may be used as an immediate on-line report of events with the NT drivers obtained from Radionics. Refer to the Readme file within Readykey for Windows for information of the NT print driver that can be obtained. A laser printer is best suited for producing historical reports on request. Overall, unless the best quality output is required, a good quality dot-matrix printer is most suitable. A printer for transaction printing should be exclusive to Readykey for Windows.

Ensure that a **PC to Printer Cable** is connected to the printer to the **Parallel Port** (LPT1) of the PC with the Security Block (Dongle) installed.

Hard Disk Space

A number of factors will affect the amount of hard disk space required on a Readykey for Windows workstation:

- Size of database - the main factor to affect this will be the total number of personnel in the system.
- Number of transactions required to be stored on the hard disk

- these are now described in more detail.

Database Size

All the information that forms part of the Readykey for Windows system is stored in a database on the hard disk of a PC. The main factor that affects the size of the database is the volume of keyholder information to be stored.

Readykey for Windows can support up to 18,000 keyholders in each of up to 128 divisions. As the number of keyholders in the system database expands, then so does the amount of disk space required.

If the Photo-ID module is also being used to store pictures of keyholders, then the amount of disk space required for each keyholder more than triples.

The table below illustrates the amount of disk space required for some typical database sizes:

Total Number of Personnel	**Disk Space Required (No Picture)**	**Disk Space Required (All Keyholders have Picture)**	**Disk Space Required (50% of Keyholders have Picture)**
4000	15 Mb	54 Mb	35 Mb
8000	30 Mb	109 Mb	69 Mb
10000	38 Mb	136 Mb	87 Mb
18000	68 Mb	246 Mb	156 Mb

Note: The above values are per division.

It is important that the number of keyholders, and whether the Photo-ID facility is being used is taken into consideration when purchasing the PC.

Transaction Storage

Every event (transaction) that occurs on a Readykey for Windows system will be stored on the hard disk of the PC which stores the system database.

All transactions are stored in files, which are usually 1.2 Mb in size, although this value can be changed. The number of transactions stored in each file will vary between 18,000 and 40,000; dependent on how busy the system is - more transactions will be stored in a file on a busier system.

When a transaction file is full, Readykey for Windows will automatically create a new one.

A number of completed transaction files are stored on the hard disk of the PC (usually six), after which the oldest will be automatically deleted to conserve disk space.

Completed transaction files can and should be copied ('archived') to floppy disk, network or tape, to allow operators to perform a transaction search at a future date of past system activity.

The more transaction files required to be stored on the hard disk of the PC, the more disk space will be required.

For the current recommended PC specification see the *Readykey for Windows PC Specification* datasheet.

Readykey Equipment

PC Interface Kits/CNCs

You may require one or more of the following, dependent on your individual system requirements. Refer to your system design:

- Readykey Central Network Controller
- PC Interface Kit with Readykey Desktop Reader
- PC Interface Kit with Wiegand Interface and Wiegand Reader

You may also need additional PC Interface Kits with a Wiegand Interface if you only have CNC(s) on your system and they are not the K6100-CNCII, but need to administer Wiegand ID devices.

Description of Components

This section describes the components of the access control system. Most operators will not need to be aware of the actual equipment being used. However it is an advantage to have an understanding of how your system is configured as this will aid troubleshooting in the future.

PC Interface Kit K6100-PC

The components of this kit are:

1. A 16.5VAC 25VA (D1625 transformer not included) transformer powered Interface Unit with connections for:
    - the Readykey desktop reader or Readykey Wiegand Interface
    - the serial port of the PC with connecting cable
    - a four wire connection to a K2100 or K1100 up to 1 km/3000 ft distance, it is recommended to use a six wire connection for future expansion
2. A Readykey desktop reader for key/card administration, operator log-in and accepting alarms. Alternatively a Readykey Wiegand Interface and a compatible Wiegand 26 bit reader may be used.

3. A Line Driver for installing at the K2100 or K1100 door controller connected to the 4 wire cable from the PC interface. It is recommended to use a six wire cable for this connection for future expansion.

Central Network Controller K6100-CNC or K6100-CNCII

The CNC comes complete with a power supply and all necessary cables for connection to the PC plus a built in reader for key/card administration, operator log-in and accepting alarms. (A PC Interface Kit with a Wiegand Interface may be required if non-Readykey ID devices are being used on a standard K6100-CNC.) The K6100-CNCII can connect directly to the wiegand reader, without the wiegand interface or PC interface kit.

Up to 32 slave door controllers can be connected to the CNC via the Readykey Six Wire Bus.

Additional master and/or slave door controllers may communicate to the CNC via the three RS-232 serial ports. Typical communication methods include line drivers, dial-up modems, fiber optics, ethernet TCP/IP using Lantronix Serial Servers, etc.

Note: Radionics have previously made different versions of the CNC - Single Site (SS CNC) and Multi-Site (MS CNC). Although both versions physically had the 3 RS-232 ports, these could only be used on the MS CNC. The SS CNC and MS CNC can only be distinguished by removing the cover and examining the labels on the software EPROMs. The SS CNC has now been discontinued, but existing SS CNCs can be upgraded by purchasing a K6005-MS Upgrade Kit.

Note: Each MS CNC will support the following:

- 1 Six Wire Bus with 32 door controllers.
- 32 Sites with up to eight door controllers, K6100-CNCII can have 127 Sites with eight door controllers each
  (Sites can be any combination of: Direct RS-232 Cluster,
  Direct RS-232 and Dataswitch,
  Dial Up Modem Cluster,
  Dial Up Modem and Dataswitch).
- 95 Sites with one door controller only (Dial Up Modem).

Hence, the maximum number of door controllers on a single K6100-CNC is:

(1 x 32) + (32 x 8) + (95 x 1) = 383 door controllers = 1532 doors.

The maximum number of door controllers on a single K6100-CNCII is:

(1 x 32) + (127 x 8) = 1048 door controllers = 4192 doors.

With a maximum of 20 CNCs on a single Readykey for Windows system, the total maximum possible number of doors is over 10,000 doors.

K2100 or K1100 Master Door Controller

A Master Door Controller is a K2100 or K1100 that communicates with Readykey for Windows either directly or via a PC Interface Kit. There may also be 'remote master' door controllers on RS-232 sites.

Any K2100 Master Door Controller controls 4 doors (2 doors on a K1100), but will also support up to 7 Slave Door Controllers.

All K2000 Door Controllers may be upgraded to a K2100 by installing a K2105 Upgrade Kit.

Slave Door Controllers

These slave door controllers may be a K2100 or K1100 operating in slave mode, or K2000-Ns.

Slave door controllers are connected to a master (either K2100/K1100 or CNC) by a six wire connection up to 1 km/3000 ft of Six Wire Bus.

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.

K2100 and K1100 controllers that are to be used as slaves may be ordered from Radionics without the front programming panel as either a K2100-LF or K1100-LF. However, a front panel will be needed initially on all door controllers for initial door controller configuration.

Readykey for Windows Software

As described earlier, Readykey for Windows is supplied in several versions and configurations based on the total number of doors on the system that may be administered, and which features are being used.

When purchasing Readykey for Windows you will receive a **Security Block,** normally called a 'dongle', that connects to your PC's printer port. This device is quite invisible to the normal operation of the printer but is interrogated by Readykey for Windows to determine the version and other modules you have purchased.

Note: Readykey for Windows will **not** communicate with Door Controllers without the Security Block. However it can be operated in **Demonstration Mode** without the Security Block installed.

Additional Modules

A number of extra modules are available for purchase for your Readykey for Windows system. These are described briefly here:

Attendance Report (K6110-A)

This facility allows calculation of the duration of a keyholder’s attendance at a site to be calculated based on the times of use of their ID device at designated readers. This feature is documented more fully as part of *the Readykey for Windows Attendance Report Datasheet*.

Division (K6110-DV)

This facility allows the addition of a separate Division (database) which will give the ability to separate keyholders across the divisions. This feature is primarily useful when used for central administration for multiple customers allowing separation by customer.

LAN Workstation (K6110-L)

This facility allows the addition of a workstation to be added to the system for multiple PC applications. The use of multiple workstations is documented in more detail within the *Multi-PC Operation/Installation Manual and the Network Operational Overview and Requirements document*.

18,000 Personnel (K6110-18K)

This module allows the number of personnel in each division to be increased from 10,000 to 18,000.

Note: This module must be used in conjunction with K2100 and K1100 door controllers, which have been upgraded using the 18,000 Personnel Upgrade Kit, part number K2105-18K. **All door controllers in the division must be upgraded -** i.e. it is not possible to have 18,000 personnel in some door controllers, and 10,000 in others.

Elevator Control (K6110-E)

Although called Elevator Control, this facility has a wide range of applications. It allows different combinations of relay outputs on K2015A Alarm Event Managers to be activated when a keyholder uses their ID device at a designated reader, dependent on the access rights of that keyholder.

One example of use of this feature would be a reader installed in a elevator. The outputs from the Alarm Event Manager are connected to the elevator electronics. When a keyholder uses their ID device with that reader then, dependent on the access group assigned to the ID device, the keyholder may be restricted to which floors they can gain access.

For more details see the *Readykey for Windows Elevator Control Datasheet*.

Photo ID (K6110-PID)

This module allows a keyholder's photograph to be captured and stored with each personnel record. This feature allows you to design and print ID cards using the personnel data and the Photo ID photographs.

The module comprises four distinct functions:

1. ***Photo ID***. This allows you to add a photo (bitmap) to each entry in the Personnel database if required.
2. ***Visual Verification***. This allows you to display an image of a keyholder when they try to access specific doors. You can then compare the picture with their appearance for visual confirmation.
3. ***ID Card Template Design Application***. This allows you to design card templates for the automated printing of Access cards. This is mainly intended for use with ID cards.
4. ***ID Card Printing***. This allows you to print, using a suitable printer, your design onto the ID cards.

For more details see the *Readykey for Windows Photo ID Datasheet*.

Audit Trail (K6110-T)

This module allows you to track changes made to the Readykey for Windows database. All changes are recorded and you can, for example:

1. Specify an operator and check what changes the operator has made over a specified time period.
2. Specify an event (e.g. Add User) and check which operators have added users over a specified time period.

For more details see the *Readykey for Windows Audit Trail Datasheet*.

Serial Interface Output (K6110-O)

The Serial Interface module allows you to connect a device to your serial port which receives messages from Readykey for Windows, for example, a camera system. You can specify which events are reported to the serial output. For example, when using a camera system, Unauthorized Entry events could be automatically reported to thecamera control system. For more details see the *Readykey for Windows Serial Interface Datasheet*.

Special Features

There are also a number of special features in Readykey for Windows which may be used. These are available on all Readykey for Windows systems - they do not need to be purchased separately.

Alarm Graphics

This facility allows a graphic picture to be attached to door and alarm inputs, so that the graphic will be displayed in the event of an alarm condition on that door or input being received by the Readykey for Windows system. For more details see the *Readykey for Windows Alarm Graphics Datasheet*.

ASCII Transaction File

This provides a means whereby personnel authorized transactions may be stored in a special file, the format of which is described in *Readykey for Windows ASCII Transaction File Datasheet*.

The contents of the file may then be interrogated by other systems, such as Time and Attendance, etc.

DDE Output

This facility also provides a means of third-party systems interrogating Readykey for Windows transactions.

However, in this case a Windows DDE (Dynamic Data Exchange) message is sent for each transaction to any other Windows-based applications that requests them.

Readykey for Windows DDE Output Datasheet provides a detailed specification for those wishing to use this facility.

Alarm Sound Support

If you do not have a PC sound card installed then you will not have Alarm Sound Support and your PC will beep when an alarm is triggered. Alarm Sound Support can either sound a siren or a voice explanation of each alarm.

For more details see the *Readykey for Windows Alarm Sound Support Datasheet*.

Ordering the Readykey for Windows Software

The Readykey for Windows software is available in many different versions - the following information needs to be available before ordering the Readykey for Windows base system software and hardware. The earlier sections of this overview should have helped you to evaluate your requirements:

1. **Total Number of Doors** on system
2. **Number of Divisions** on system (all systems supplied with one Division)
3. **Total Number of Sites** on system (all Multi-Site systems)
4. Which, if any, additional software modules are required - the following can be purchased:
   - **Attendance Report Option (K6110-A)**
   - **Additional LAN Workstation Option (K6110-L)**

- **Additional Site Option (K6110-S1)**
- **Additional Division Option (K6110-DV)**
- **18,000 Personnel Option (K6110-18K)**
- **Elevator Control Option (K6110-E)**
- **Photo ID Option (K6110-PID)**
- **Audit Trail (K6110-T)**
- **Serial Interface Output (K6110-O)**

Most of the modules listed are programmed into the Readykey for Windows dongle/security block, as described earlier. But some require additional hardware, i.e.: 18,000 personnel requires the K2105-18K installed in the door controllers.

All Readykey for Windows software is identical in operation and features, regardless of the system purchased. The security block simply restricts what the system operators can use or view.

It is then possible to purchase extra modules from Radionics at a future date. When you purchase new features, you will be issued with a password that can be entered into the Readykey for Windows software to upgrade and re-program the dongle.

For example, your system may initially have one site, one division and 50 doors. At a future date you may decide to add the Attendance Report facility. Radionics will supply you with a password to enable the Attendance Report facility.

Radionics Part Numbers and Ordering Information

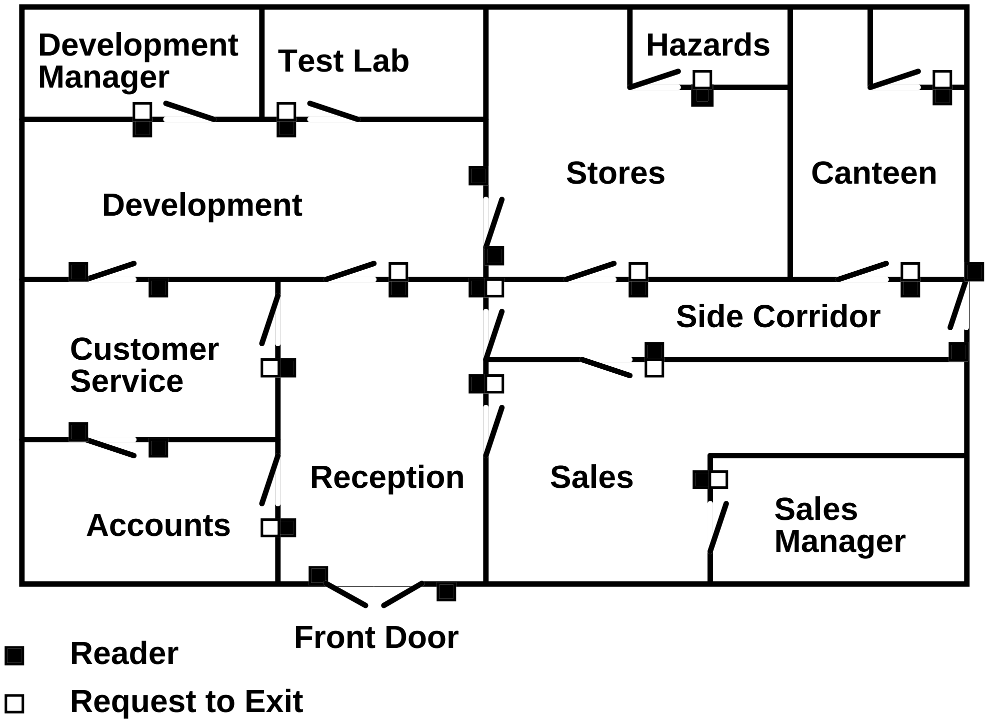
Please refer to your Radionics Product Catalog and Readykey Price list for a comprehensive list of all Radionics Readykey part numbers and pricing.

Setting Up Readykey for Windows

In order to start operating a Readykey for Windows system, you will first of all need to consider various aspects of the building or site you are about to control. The following items are listed in the order in which you should consider them.

If you plan to have a system with more than one site, then each physical ‘site’ will need to be considered individually in this way.

To help you understand the various aspects of the system a simple example site will be used throughout the remainder of this overview.



In this example you will notice that several doors have a **reader** on each side. This is to allow access to be controlled in both directions. For instance the door between Accounts and Customer Service has a reader on each side, this is because the same door is an entry door into both Accounts and Customer Service. Other doors have **Request to Exit (RTE)** motion detectors that allow any person to leave the area.

Although the example given is of a commercial building the principles can be just as easily applied to an industrial or residential application.

Areas

An **Area** is part of a building or site to which access is controlled by one or more doors (or other type of entry such as a barrier, turn-stile etc.). Any person with access to an area will be allowed in through *any* door defined as an entry door into that area. When defining doors on the system, every door must be assigned as an entry door into an area.

Consider the example above, there is a section called Customer Service with 3 possible entry points all controlled by door readers; from Reception, from Development and from Accounts. Any person given access to the area called Customer Service will **automatically have access through all three doors**.

If you have readers on doors that leave the controlled area, for instance a reader that allows people out through the front door , then you will need to define a special area called, for example, 'Outside' or 'Off-Site'. This is because when a person leaves the building they will be entering an 'area' outside.

It is important to understand the importance of areas and to consider how your particular building or buildings are to be divided into areas. In a residential application the areas may be entire blocks with access through ground floor doors or landings with access through doors on each floor.

It is possible to have an area within an area, for instance in our example there is a Sales Manager’s Office within the Sales area. The managers office will be defined as one area with access through the single door. Sales will be another area with access through two doors. This means that some people may have access to Sales only, whereas others will have access both to Sales and to the Sales Manager’s Office. Of course anyone given access to the Sales Managers Office must have access to Sales in order to reach the Office door.

Doors

A **Door** is an access point controlled by a device, such as a Readykey Reader, that will identify a key/card holder. The access point may be a door, a turnstile, a vehicle barrier etc. All doors control entry into an area.

It is important to realize that although the system uses the term 'Door', this really refers to a Readykey reader. If you have a reader on each side of a door then you need to define two 'doors'. Each 'door' (or reader) will control entry into an area. Consider the example: there is a door between Development and Stores with a reader on each side. Anybody in Stores will only be able to use that door if they have been allowed access to Development, likewise anyone in Development will only be allowed through this door if they are allowed into Stores. To achieve this control there needs to be **two** doors defined; one will be 'Stores into Development' with Development as its Entry Area, the other door will be 'Development into Stores' with Stores as its Entry Area.

Warning: A **Reader Combiner** (K2040) allows a single access point to be controlled from two locations using a single reader channel. Normally this would allow for pedestrian and vehicle use, or two different heights for different vehicle types etc. It may also allow a reader to be installed to each side of a door, but appear as only a single door at the door controller. In this case there is no indication of which reader has been used, therefore a single door is, in effect, allowing access to two different areas with no indication of which area. For this reason you are advised to use a Reader Combiner **only** when the readers are on the same side of the access point.

Time Profiles

Time profiles 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, you 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 is 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 locked again at 5:00pm, also it must 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, 24 hours a day, 7 days a week.

Access Groups

A person or visitor is given access within a building or site by allocating them an access group. An access group consists of 2 lists of areas, each of which may have a time profile allocated. A total of up to 128 Access Groups may be created, per site.

Using our example we may setup Access Groups such as:

Access Group: Development Engineers

Time Profile 1:	None	**Time Profile 2:**	Office Hours
Area List 1:		**Area List 2:**	
	Outside		Sales
	Reception		Accounts
	Canteen		Side Corridor
	Development		Customer Service

Access Group: Test Engineers

Time Profile 1:	None	**Time Profile 2:**	Office Hours
Area List 1:		**Area List 2:**	
	Outside		Sales
	Reception		Accounts
	Canteen		Side Corridor
	Development		Customer Service
	Test Lab		

Access Group: Development Management

Time Profile 1:	None	**Time Profile 2:**	Office Hours
Area List 1:		**Area List 2:**	
	Outside		Sales
	Reception		Accounts
	Canteen		Side Corridor
	Development		Customer Service
	Dev Managers Office		Stores
	Test Lab		

These examples show that all three access groups have unlimited access to Reception, Canteen and Development as the Time Profile covering those areas is 'None'. In addition the Test Engineers can get to the Test Lab 24 hours a day and the Management group has unlimited access to the Managers Office and the Test Lab.

Both groups are given limited access, during office hours, to Sales, Accounts and Customer Service with the Development Management group also being allowed access to Stores at these times.

Divisional Access Groups

These provide a method, on a multi-site Readykey for Windows system whereby a person can be given access on more than one site. An example where this might be required would be with a senior manager or housing officer who may travel from one site to another, yet only wish to carry a single ID device.

This is achieved by constructing an access group for each of the individual sites, and then combining these into a DAG (Divisional Access Group) consisting of an access group for each site. (**Note:** The assigned access group for some sites could be ‘None’.)

DAGs appear in the list of Access Groups in Personnel, Departments and Workgroups.

Up to 256 DAGs per division may be defined.

Extra Access

Readykey for Windows has a restriction of 128 Access Groups per site, and 256 Divisional Access Groups per division. On larger systems, this may not be sufficient. There may also be occasions when individual users have ‘exceptional’ access requirements, and to create a new access group or divisional access group for this single user would be inefficient.

In this case, it is possible to assign up to two additional lists of areas, each list with its own time profile, to each keyholder. Access to these areas is in addition to the **Access Group** or **Divisional Access Group** assigned.

Note: The Extra Access facility is only available on K2100/K1100 controllers with Version 3.0 or later software installed.

Departments and Work Groups

In a large or complex system many different Access Groups, up to 128 per site, may be created to allow for all the different, and possibly changing, access requirements. In addition, there may be 256 DAGs per division. When adding a new member of staff, or changing the access of an existing staff member, then it would be very cumbersome to be confronted with a very long list of Access Groups and DAGs from which to choose.

To make it easier to allocate access groups to people, Departments and Work Groups may be defined. Both these features can have a list of access groups and DAGs assigned to them. When adding a new person, by first selecting a Department and or Work Group a much reduced list of possible access groups and DAGs will be presented.

In our example we may have a Department called 'Technical'. This may cover all the development staff, Customer Service staff etc. We may include all the Access Groups shown above in this Department. We may then create a Work Group called 'Test Lab Engineers' in which we include the Access Group called 'Test Engineers'.

Departments and Work Groups make assigning access to people much easier. In addition, Departments can be used when reporting on past events.

Access Control

The advantage of setting up these structures becomes apparent when a new member of staff is appointed. Say a new test engineer starts work and needs to be issued with a key/card.

1. First of all the keyholder’s name is entered,
2. .. then a Department is selected, in this case 'Technical',
3. .. when a Work Group is selected only the Work Groups that have been assigned to the Technical Department will be displayed. In this case we will select 'Test Lab Engineers'.
4. The list of possible access groups is now restricted to the recommended access groups for a Test Lab Engineer. This may now be selected and the personnel record added to give the engineer the required access to the areas assigned.

By not selecting a Department or Work Group all Access Groups and DAGs will be presented and a selection can be made. Even if you select a Department and Work Group for a person then you can still call up all the Access Groups and DAGs and override the limited list.

Reporting

When recalling past events it is possible to limit your report to the movements of personnel who belong to one or more particular departments. This is achieved by selecting the department before running the report.

It may not be clear when looking at a simple example what are the advantages of creating Departments and Work Groups. An operator of a much larger system with hundreds, or even thousands of personnel will certainly benefit.

Personnel and Visitors

Access by personnel and visitors is controlled by allocating individuals an Access Group or DAGs (described earlier). Visitors are treated differently in that their ID devices will only be valid for a set number of days, outside which they will be denied access.

Keys/cards are added to the system by presenting them to the desktop reader , CNC, or by manually entering the key code into the system.

Using Readykey for Windows

Starting Up

Readykey for Windows is started either by an operator selecting the Readykey for Windows icon, or Start Button, from the Windows Program Manager or Start Menu, or it may be configured to start up automatically when the PC is switched on.

Logging In

Whenever Readykey for Windows is started the Login window will appear asking for a name and password. If you present an operator key, the operator name will be filled in and, if required, you must then type your password.

Every operator has a set of privileges defined that, once they have logged in, determine what items they can use, or see, within the system.

It is important to realize that at this stage Readykey for Windows is operating in the background. Before the Login box appeared a special application was started up called the Readykey Engine. This sits in the background handling all the communications between the PCs, the CNC and the door controllers. The Readykey Engine is running even when no operator is logged in. The **Alarm** application, which may also be running in the background, will be initiated and report information about alarm events as they occur.

Note: Once Readykey for Windows is running, an operator needs to go through a similar process to logging in before the system can be shut down.

Transaction Display/Printout

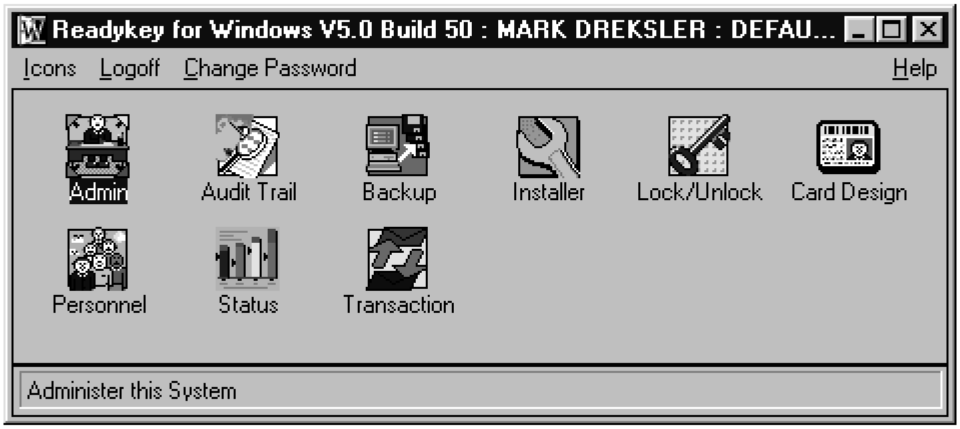
Once Readykey for Windows has started, if the **Alarm** application is running, an On-Line Transaction Display can be called up. This will show events on the screen as they occur. The system may also be configured to print some or all events as they occur.

Both these activities will occur in the background, even if other non-Readykey programs are running.

All events are stored for future viewing whether they are printed or not.

Applications

When you log in you will see another box with a certain number of icons representing all the Applications that your operator privilege allows you to use.



Administer this System

Briefly, these applications are:

Admin

When running Admin you will be presented with another set of icons, again you will only see those you are allowed to use (see Operators, described later). These represent various aspects of system administration such as setting up Access Groups, Time Profiles, Operators etc.

Audit Trail

This is a purchased module which, if present, records changes made to the system by operators. Starting Audit Trail from the icon allows you to search through all the previous operator changes by change type (for example, changes to operators, access groups, personnel records). The search also has time and date limits which can be set.

Backup

This enables the operator to make a security copy of the system database, previous events to be copied to backup disks, and the database repaired/upgraded should this become damaged or corrupted.

Alarm

Normally the Alarm application will be running permanently in the background and will not normally appear here. When a transaction is received by Readykey for Windows, the Alarm application looks at it and decides whether it is to be displayed, printed, generate an alarm event, etc. It can also arm and disarm areas which are groups of alarm inputs.

If you have a multi-workstation Readykey for Windows system, then you may wish to only have the Alarm application running on certain workstations, using other workstations purely for administration and/or reporting purposes.

Installer

Generally most operators will not need to use this application as it is concerned with configuring the hardware of the system such as Divisions, Sites, Doors, Door Controllers, Alarm Modules etc.

Lock/Unlock

The operator can manually lock or unlock any door from the workstation, overriding any time profiles that may be active.

Card Design

This icon leads to the ID Card Template Design application which is part of the Photo ID module purchased option. It allows design of ID Card Templates for use in automated key card printing from the personnel application.

Personnel

This application allows you to add, change and delete personnel and visitors. This is where you say 'who can go where and when by assigning their access group'.

Status

This allows you to examine the status of individual doors, (open, closed etc.), alarm points (isolated, active etc.), door controllers (communicating, tampered etc.) and masters (on-line to sites, etc.).

Transaction

Here you are able to recall and view or print previous events. Events can be selected on the basis of time, type of event, personnel names, certain doors etc. You can also use this application to find out which keyholders are or were in a certain area at a particular time, ., or find out which keyholders have **not** used their ID devices in a certain period.

Operators

The Readykey for Windows system is administered by **Operators**. These are people who are allocated a key/card that may be used to gain access to the Readykey for Windows system. Access to the editing system is controlled by the operator's **Password** and also by the operator **Privilege** assigned to the operator. The operator privilege defines which parts of the editing system an operator may have access to and also whether they can make changes, or just view the information.

A key/card given to an operator is not specially manufactured by Radionics. It is only an operator key/card because it has been added in to the Readykey for Windows system as such, and could also be added as a Personnel key, and hence be used to give access around a building or site.

It should be noted that by using operator privileges, an operator's view of the entire system can be limited, and that icons and menu items described in the documentation may not always be visible.

Operators may also accept alarms that occur in the system (see Alarms), again an operators privilege will determine whether they are allowed to accept alarms.

If you have more than one workstation on your system, then an operator may automatically log on or accept alarms at any workstation on the system.

Each operator can be restricted to have privileges in a limited number of divisions.

Administering Keys/Cards

Readykey for Windows has several features for making key/card administration as simple as possible. The Personnel application allows keys to be added, changed and deleted. Keys or cards can be searched for by presenting them to the administration reader or CNC. By using the Department and Work Group features the operator can quickly give the correct access group to a new person or visitor.

The Transaction application provides a means of viewing the movements of individuals or groups of people over a period of time and/or in selected areas.

Alarms

The access control system can be set up to report a variety of alarm conditions. All these alarm conditions rely on the system being installed in such a way that the alarm conditions can be detected.

Accepting Alarms

Whenever an alarm occurs a box will appear showing where, when and what type of alarm has occurred. At this stage the operator has three choices:

- The alarm may be accepted provided the operator has the privilege to do so. If this is the case then a reason is selected and the operators key/card is presented to the administration reader; a password may also be required.
- The alarm may be queued. This will be necessary if there is no operator present with the privilege of accepting alarms. When an alarm is queued it can be accepted later by calling up the Alarm application and accepting any outstanding alarms.
- The Info button may be used to display a graphic if assigned to the alarm point.

Door Alarms

For door alarms to be reported (except PIN Reader Duress), door monitoring must be set up using a door contact to determine the physical state of the door. A further advantage of setting up door monitoring is that if the door is opened and closed before the lock time has expired, any remaining lock time will be automatically canceled.

Unauthorized Access

This occurs when a door is opened without a valid key/card being presented or a Request to Exit button being pressed.

Anti-Tamper Alarm

If a reader is removed or the cable leading from the door controller to the reader/door contact is broken then this alarm event will occur. This alarm is also produced if a K2015A Alarm Event Manager is tampered.

Door Left Open

If a door is left open for more than a set time then a door left open warning will be produced.

PIN Reader Duress

This is a special alarm produced when using Readykey K2001-P PIN readers. If a key/card holder adds one to their PIN number when using the reader, an alarm is produced indicating to the operator that the key/card holder has opened the door under duress.

Door Controller Alarms

These alarms indicate conditions at the door controller itself.

Anti-Tamper Alarm

Produced if the door controller case is opened if a tamper switch is being used.

Emergency Override

A special input on the door controller which will unlock all doors on a controller in an emergency generating this alarm report.

Zone Alarms

Up to 4 K2015A Alarm Event Managers (AEM) may be installed to any K2100 door controller (2 on a K1100). Each AEM can monitor up to 8 points. The alarm inputs can operate automatically or they can be administered from the alarm application by arming and disarming alarm areas.

Alarm Activated

This event is reported when a Zone Alarm point is activated.

Reporting on Keyholders

Within the Personnel application there is a search facility that allows groups of personnel to be selected. For instance all the personnel in one department or work group could be listed and then printed.

Reporting on Events

The Transaction application allows all events to be selected and either viewed on the screen or sent to the printer. The operator can select events by date, by door, by area, by person and by department. Typical uses of this facility might be of the kind: ‘Who went into Stores during the weekend?’.   A report of which keyholders have **not** used their ID devices in a specified period can also be produced - this can be for the whole system, or for just particular doors/areas.

By using the Presence In Area facility, it is possible to find out which keyholders were in a certain area during a certain time period or currently still there.

The Attendance Report facility (available for purchase as an extra feature) provides a means of generating a report on keyholders' attendance times on a particular site.

Multi-Workstation Systems

One of the features of Readykey for Windows, is the ability for the system to be administered from several workstations which are connected via a Local Area Network (LAN) or Peer to Peer Network.

One of the workstations has the Database Engine, Readykey for Windows application and Readykey for Windows database files are installed. The other workstations, which are to be used for system administration, just have the Database Engine and Readykey for Windows application files installed.

Network Types

Readykey for Windows uses Microsoft Windows for Workgroups, Windows 95, Windows 98, or Windows NT4 to allow the access control system to be administered from more than one workstation. All workstations must be running the same Windows operating system.

Two types of network can be used. However they both use the same type of cable, connectors and require a Network Interface Card (NIC) to be installed in each workstation on the network.

For small systems, less than four PCs, a peer to peer setup is best, with the hardware connected to the PC with the database.

For large systems a server based installation works best.

Note: It is unlikely that Readykey for Windows PC-PC communication will work effectively over a Wide Area Network.

The configuration of all networking applications **must** be verified with the Readykey Technical Support department before the sale of the system.

i. Server-based

This involves having a powerful File Server PC which runs Novell Netware or Microsoft Windows NT Advanced Server. This allows connected workstations to share a common hard disk and other resources - e.g. printers.

Using this type of network, all the Readykey for Windows database, Borland Database Engine, and application files are stored on the server, but Readykey for Windows cannot be administered from this PC.

Each workstation must be running Microsoft Windows for Workgroups, Windows 95, Windows 98, or Windows NT. However, to avoid porblems, the Readykey Server should be running at least Windows 95, Windows 98, or Windows NT4. We recommend that all the workstations have the same version of Windows installed.

Notes:

1. A maximum of ten PCs can be supported on a network, which is to be used for other general business traffic. With this installation, a maximum of four PCs can support Alarm running.
2. A maximum of twenty PCs can be supported if the network is dedicated for Readykey for Windows use only. A maximum of four PCs can run Alarm.

ii. Peer-to-Peer

This is a cheaper type of network which uses ordinary PCs, each of which run Microsoft Windows for Workgroups, Windows 95, Windows 98, or Windows NT. There is no dedicated ‘File Server’. Instead any workstation on the network can allow other workstations to share access to its hard disk and printers.

In this case, the Borland Database Engine, Readykey for Windows database and application files are installed on one workstation on the network, which becomes the Readykey Server. This workstation may also be used to administer Readykey for Windows.

The Readykey Server should be running a minimum of Windows 95, Windows 98, or Windows NT4. We recommend that all the workstations have the same version of Windows installed.

Recommendations

Radionics strongly recommend using a Peer to Peer network for most small to medium sized systems.

Radionics strongly recommend that a Server-based network is used wherever possible for larger systems, as this includes a File Server that is dedicated to providing shared resources, and is inherently more reliable and will offer higher performance.

However, in circumstances where such a network is not available, a peer to peer network may be used for larger systems, with a limit of four workstations. In this case, it is recommended that the Readykey Server is dedicated to being a Readykey for Windows server, and not used for other tasks - e.g. word processing, etc.

Note: A peer to peer network with the system hardware connected to the Readykey Server is a faster running system than a File Server based network of the same size.

Readykey Server

This is a term used to describe the workstation which has the Readykey for Windows security block connected to it. The term should not be confused with a ‘File Server’ on a server-based network. On a peer-to-peer network, the Readykey for Windows database and application files will also be stored here. Ideally, this should be a high specification machine, particularly on larger systems.

You must have a Readykey Server on your system. On a Server-based network, this cannot be the file server itself.

Additional Workstations

Up to 20 workstations in total are allowed on a dedicated File Server-based network. On a Peer-to-Peer network the total number of workstations is limited to 4. Each of these may be used for full administration or solely for the display of alarms and other transactions that occur on the system. Alternatively, additional door controllers may be connected to each workstation setup up as an additional site (see Masters).

It is important to remember that any operator is allowed to log in to the system at ANY workstation.

Security Block

Your system will have a security block (dongle) connected to the parallel (printer) port on the Readykey Server.

The Readykey for Windows system interrogates the security block at workstation start up and frequent intervals to determine the type of Readykey for Windows system you have purchased. This in turn will be used to offer you different or limited choices in certain parts of the system.

It is important to note that in order to run Readykey for Windows on any workstation, the Readykey Server **must be running Readykey for Windows**. This is an important point to consider when you are designing your system.

Masters

If you have more than one master on your system, then these do not all need to be connected to the same workstation. It may be more convenient, for example if you have a number of door controllers in an outbuilding to which there already exists a network connection, to configure these as a separate 'site', and establish a master in that building. The advantage is that no additional communications cabling need be installed between the two buildings.

However, in order for any transactions from the outbuilding to be sent to any workstation in the main building, the workstation in the outbuilding must be running Readykey for Windows.

Administration

For any workstations which are not going to have a master installed, then, if you wish to use to administer keys/cards it will be necessary to either purchase and install a PC Interface Kit for this purpose or manually enter the key code values.

Transaction Routing

Every transaction that occurs on a door controller or alarm event manager is reported to a workstation via the corresponding master. The Readykey Engine on the workstation then writes the transaction to the hard disk on the Readykey server or file server.

Each workstation continuously reads the transaction file on the Readykey server and uses the transaction routing information to determine how to handle each new transaction.

Using this powerful facility, therefore, it is possible to configure a system such that transactions 'appear' on different printers and screens at different times of day. For example, you may require that during normal working hours only 'exception' reports (alarms, access denied, etc.) are printed and displayed at the workstation in the personnel office. Outside those hours, you may want all transactions to be printed and displayed at the workstation in the security lodge.

Security

Any Access Control system must be secure from anybody tampering with the access rights of personnel or altering the system in any way without the knowledge of those supervising the system.

There are two main aspects of security, one is ensuring that only authorized changes are made to the system, the other is that the data is not lost or corrupted.

Operators

An Operator is a person given the right to administer the system in some way. This may be a guard (who may accept alarms only) or a supervisor who may make changes to the way the system is configured. Every operator can be given their own set of privileges. These privileges define exactly what any given operator is allowed to do. Clearly it must be only the most responsible operators who have the ability to alter operator privileges.

Operators can also be restricted in which division(s) they can view or edit the database.

The operator keys/cards and passwords are important to the security of the system and every effort should be made to ensure their safety. Regularly changing passwords should be considered in most systems. Remember that an operator key/card can also be used to move around the building when given appropriate access. For this reason it is suggested that operators keep their keys/cards with them at all times.

It is important to realize that operator keys/cards are not special Readykey keys/cards, it is just that they have been assigned access to the Readykey for Windows database.

Remember that if you have more than one workstation on your system that any operator can gain access to the system from any workstation.

Backing Up the Database

A considerable amount of time and effort is required to set up and maintain an access control system. All this effort is stored in computer files on the PC. If backup copies of the database are not made then it can take a long time to re-create the database if the PC fails or is damaged. Regular backups, say once a week, kept in a safe place, off-site if possible, should avoid this type of problem.

Remember: all access decisions and alarm generations are carried out at the door controller. The PC plays no part in unlocking or closing doors etc., it is there to administer the system from a central point. If the PC stopped working for any reason then the access control system would go on working as normal, however no changes could be made to the system and all alarm reports would occur at the K2100/K1100 Master controller or CNC.

From the earlier section on PC Specification, Hard Disk Space, you will realize that the Readykey for Windows database can become quite large, using many megabytes of disk space.

Obviously backing up a system of this size to floppy disk would be impractical. Readykey for Windows allows the destination for a backup to be specified - so backups can be easily taken to a network file server, or to a tape drive for example.

The Readykey for Windows backup utility includes a compression facility, so that a backup of the system will take up less space than the database itself.

Note: The Readykey for Windows backup application automatically shuts down Readykey for Windows on all workstations except the Readykey Server which is running backup. Also note that third party backup facilities will **not** provide reliable backups unless **ALL** copies of Readykey for Windows are manually shut down.

System Specification

The Readykey for Windows system offers the following features:

Personnel

10,000 personnel per division
18,000 personnel per division if upgraded K2100/K1100 controllers are used and the 18,000 personnel facility is purchased.

750 visitors per division.

Real Time Personnel Trace.
Import/Export facility.
Copy personnel between divisions.

Photo-ID module (available module for purchase)

Database search and query.

Extra Access facility (allows up to two lists of areas to be included in the access of individual keyholders).

Wiegand 26 Bit card code entry/conversion.

20 Extra Information fields per keyholder.

Doors

Available in different configurations of 16, 32, 64, 128, or two forms of Multi-Site, 3 site for up to 192 doors or 128 site for over 10,000 doors.

Manual Lock/Unlock.

Anti-passback within a door controller.

Any reader can be defined as an 'Elevator Reader' to provide Elevator Control.

Network Masters

Maximum 20 per system.

Workstations

Maximum 20 per system. Transactions displayed at each workstation can be restricted to certain divisions.

Sites

Up to 128 per division.
Forced dial up of remote sites.

*Per K6100-CNC: 1 site - Six Wire Bus, Up to 32 door controllers
32 sites - RS-232, Up to 8 door controllers
95 sites - RS-232, 1 door controller only

*Per K6100-CNCII: 1 site - Six Wire Bus, Up to 32 door controllers
127 sites - RS-232, Up to 8 door controllers

Access Groups

128 per site.
256 divisional access groups per division.
Extra Access per keyholder (see **Personnel**)

Departments

128 per division.

Work Groups

127 per division.

Security

129 operators (128 + 1 supervisor)
- maximum of 32 operators may accept alarms at a CNC or door controller.

Operators may be restricted to which divisions they can edit.

Compressed backup and restore of database.
Archive of transactions to floppy.

Time Profiles

Up to 128* per division, each with up to 3 time periods

**32 if system has any K2000-N controllers.*

System Clock Synchronize to PC.

System Holiday facility.

Alarm Monitoring and Control Facilities

Door Controller Alarms: Case Tamper, Emergency Override.

Door Alarms: Unauthorized Access; Cable/Reader Tamper; PIN Reader Duress; Door Left Open Warning.

Zone Alarms: Up to 32 points per door controller by using K2015A Alarm Event Manager modules.

Relay Outputs: Up to 36 programmable relay outputs per door controller by using Alarm Event Manager modules.

Automatic alarm accept facility.

Door and alarm status display.

Alarm Graphics automatically displayed on alarm event.

Transactions

Unlimited on PC Hard Disk.
Unlimited archived.
Real Time Transaction Display
ASCII Transaction File output.
DDE Output to third party applications.

Serial Interface Output, module available for purchase.

Transaction Routing by Type, Division and Workstation.

Reports

Transaction Analysis, Unused Key/Cards, Presence In Area, Attendance Report (purchased as an option).

User Interface

Microsoft Windows multi-tasking environment.
On-line Context-sensitive Help Facility.

Appendix A: Glossary

Access Group

A list of areas to which a keyholder is allowed access. The access may be restricted to certain times by use of a Time Profile.

Area

A part of a building - typically a single room. One or more doors give access to the area.

Alarm Area

Area to which alarms inputs are assigned. This can be a real area with doors (as above) or can be an area defined specifically for attaching alarm inputs. Alarm inputs attached to an area can be viewed, armed and disarmed as a group in the alarm application.

Alarm Event Manager

A module which may be installed on the cable between a reader and door controller, allowing monitoring of eight additional points (alarm inputs) and providing eight programmable relays. This modules is called a K2015A.

Alarm Graphic

A picture which is assigned to either a door or alarm point. When an alarm occurs, the picture may be displayed to provide more information about the source of the alarm. An example would be a site plan, showing the location of the door.

Anti-Passback

The limiting of an ID device’s use in one direction without first having been used in the opposite direction. For example, if an ID device has been used for entry it cannot be used for re-entry until it has been used for exit.

Anti-Tamper

A means of detecting unauthorized disconnection of cables or removal of covers from security equipment.

Archive

Every transaction that occurs on the system is written to a file stored on the hard disk of the PC, so that searches can be performed at a later date. Periodically, a new file is created. The system will only retain a set number (usually six) of files on the hard disk, after which, the oldest will be deleted. These old files are called archives, and should be copied to a floppy disk and stored in a safe place.

Audit trail

History of operator changes to the Readykey for Windows database and settings. Module available for purchase.

Auto Accept

Every alarm that occurs in the system must be accepted at the workstation by means of a valid operator key/card or name. It is possible to set up the system so that if the workstation is unattended for any period of time any alarms received are automatically accepted.

Backup

The Readykey for Windows system consists of a large database of information - doors, personnel, etc. In order to safeguard the information against PC failure or other disaster, it is recommended that a copy (backup) of the database is taken at regular intervals, in order to minimize disruption in the event of any problems.

Block Add

If a large number of keyholders are to be entered into the database, it may be more convenient to enter all the names, access groups, etc. first, then to assign the keys/cards at a later date. The Personnel application includes a special ‘Block Add’ utility for this purpose.

Card

An ID device containing a unique code. This device is flat in appearance and of the same size as a credit card. The technologies of this type of device could be magnetic stripe, bar code, barium ferite, etc.., the controller then decides whether to release the lock.

Card (proximity)

An ID device containing a unique code. This device is flat in appearance and of the same size as a credit card. The device is held near to a reader to allow the code to be read, the controller then decides whether to release the lock.

Channel

A term used to describe the connections on a door controller for a single door - i.e. reader, locks and request to exit and door contact inputs.

CNC (Central Network Controller)

A piece of Readykey hardware which allows Readykey door controllers to be administered from a workstation running suitable Readykey software.

Clock Synchronize

All Readykey door controllers and network controllers maintain a real time clock. This is used to time ‘stamp’ transactions as they occur, and also to determine when time profiles begin and end. Twice a day, at midday and midnight, these clocks are synchronized to the clock in the PC automatically. It is also possible to manually perform this operation for special cases - e.g. ‘Daylight Savings Time’ adjustment.

Dataswitch

An item of equipment which allows up to four or eight Readykey door controllers to communicate via a common RS-232 connection. Normally refered to as a Code Operated Switch.

DDE (Dynamic Data Exchange)

DDE is a Microsoft Windows facility that allows information to be transferred between different Windows-based applications. Readykey for Windows uses DDE in two ways:

i. To allow third-party applications to use the transactions generated on a Readykey for Windows system - e.g. building management, time and attendance, etc.

ii. A special form of DDE, NetDDE is used to allow more than one PC to simultaneously administer a Readykey for Windows system over a network.

Department

Used for keyholder management. A large keyholder database may be divided into departments for searching and reporting. A department may consist of one or more workgroups.

Dial-back

A term used to describe the process whereby a K2100 or K1100 controller initiates a communications session via a pair of modems to a Readykey MS CNC to report an alarm condition which has occurred at a remote site.

Division A division can be regarded as a collective name for a number of sites in the ‘system’. The database can be split by using multiple divisions.

Divisional Access Group Used on a Readykey for Windows system where there is more than one site to allow access to be given to keyholders on more than one site within a division.

Door Although this term is usually used to refer to a physical door at which a Readykey reader is installed, it is useful to remember that sometimes each physical door may have a reader installed on both sides - in this case it would be referred to as two ‘doors’ in the context of the Readykey for Windows system.

Door Contact A device, usually a magnetic switch, which may be installed on a door to monitor whether the door is open or closed.

Door Controller A microprocessor based unit from which up to four doors may be controlled. The door controller reports to and is administered by the PC(s). The door controller makes the decision as to whether access is to be allowed.

Door Open Time If a door has a means of monitoring its state (closed or open) installed, then it is possible to configure the system to produce a transaction if the door is held open beyond a specified time. **Note that the door open time begins from the instant the lock time expires, NOT at the time the door was initially opened.**

Dongle See ‘Security Block’.

Download A means of ensuring that the database held in a door controller is identical to that stored on the PC. This operation is only normally performed during the installation of a new door controller, and is normally preceded by an initialize operation.

Engine A special Readykey application that runs all the time on Readykey for Windows systems in the background. This application handles all communications between the other Readykey applications and the Readykey hardware.

Emergency Override In the event of a fire or other emergency, it would be usual for all doors on the system to be automatically unlocked. Each Readykey door controller provides an input for this purpose. In addition an emergency override facility is available on individual doors.

Entry Area Each site is divided into a number of areas. Each area has one or more doors that restrict access to the area. An entry area is assigned for each door. This is the area that a keyholder would enter by presenting their key/card to the Readykey reader on the secure side of the door, and then entering the area by use of the door.

Events (see Transaction) System activity that generates messages to the reporting device.

Exit Out Of Hours

If a person has access to an area for a limited time only (controlled by a time profile), and the door has a reader installed on both the inside and the outside, then it is feasible for a keyholder to become ‘locked’ on the inside of an area. By selecting this option for any channels which correspond to a reader on the secure side of a door, then keyholders will be still able to leave the area, but a special exception transaction would be recorded.

Fail Safe/Fail Secure

These terms are used to describe the two common types of locks available.

Fail Safe locks (also sometimes called ‘Power to Lock’) require a permanent power to keep the door locked. This type of lock would normally be used if safety was most important - i.e. in the event of equipment failure the door would become unlocked.

Fail Secure locks (also called ‘Power to Release’) require a power to unlock the door.

Hexadecimal

A numbering system that is commonly used in PC-based applications. The system uses the digits 0 to 9 and the letters A to F to count from 0 to 15 (A=10, B=11, C=12, etc.).

A hexadecimal system is used in Readykey for Windows to store the keycodes for keyholders.

History

The alarm ‘History’ queue lists any alarms that have cleared and been accepted. Normally alarms only remain in this queue for seven days, after which they will be deleted. To search for alarms over a longer period, the Transaction application may be used.

Holiday

This is a special override which would normally be used to prevent doors normally automatically unlocked by a time profile from being left unlocked during public holidays.

Icon

A small picture, used in Microsoft Windows to represent a program.

ID (identity) device

May be a card or some form of ‘electronic key’. Each ID device has a unique security code which is read by the reader.

Initialize

An operation to clear all information from a door or network controller. Usually followed by a download.

Key/Card

A Readykey electronic identification device containing a unique code. This device is held near to a Readykey reader to allow the code to be read, the door controller then decides whether to release the lock.

Key Code

A term used to describe the unique code stored within a Readykey electronic key. This code is programmed by Readykey at manufacture and cannot be changed.

Line Driver

A piece of equipment which can be used to increase the distance RS-232 data can be sent beyond 30 feet/15m . Line drivers are always used in pairs, one at either end. The cable between them is commonly four core unscreened. Sometimes called a Baseband Modem.

Lock Time

The time that a door will be unlocked following a valid key/card being presented at a reader or a request to exit button being pressed. Note that this time may be shortened if a door contact is installed and the door opens and re-closes before the lock time expires.

Log In

An operation by which an operator gains access to the system, usually performed by presenting their operator key/card to the desktop reader or CNC, followed by possibly typing a password.

Log Off

The operation by which an operator ends their Readykey for Windows administration session. No further changes to the system are possible without an operator logging in again. Note that logging off does not stop Readykey for Windows operating in the background - alarms and other transactions will still be received and reported.

Master

A K2100/K1100 or CNC which will enunciate alarms and also store transactions and updates from and to any slave controllers connected to it.

Modem

A device which allows any device with an RS-232 interface to communicate over a telephone (PSTN) line. Modems are always used in pairs.

Multi-Site

A system which allows more than one group of Readykey door controllers to be administered from the same central location.

Operator

A keyholder who is allowed to make changes to the Readykey for Windows database and accept alarms.

Password

A word which must be entered by an operator when logging in to prevent unauthorized access to the system.

PC Interface Kit

A piece of hardware which allows a keyholder to log on to a Readykey for Windows system by presenting their key/card at a desktop reader. Can also be used to connect a Readykey for Windows system to a master K2100/K1100, without the need for a CNC.

Personnel

One type of keyholder - typically a tenant or employee who carries a Readykey key/card.

PIN Reader/PIN Number

A PIN reader is a special type of Readykey reader which is commonly used where an additional level of security is required. To gain access through a door, the keyholder must present their key/card, followed by typing their 4-digit number. The PIN number is derived from the key/card code and cannot be changed.

Point

An additional input, provided by a K2015A Alarm Event Manager, which permits additional equipment to be monitored.

Privilege

Controls whether system operators are allowed to view/ modify the different parts of the Readykey for Windows database.

Reader

A device installed adjacent to a door, which reads the stored code when a Readykey key/card is held close to it by a keyholder, and transmits to the door controller. The reader also incorporates an ‘access authorized’ LED.

Report

A printed list of information about a part or all of the system.

Request To Exit

A motion detector or switch, normally mounted on the secure side of the door allows exit from the area, without need for a key/card to be presented. Operation of this generates a ‘Request to Exit’ transaction.

Restore

An operation whereby a backup of a database is copied from a floppy disk to the hard disk of the PC. This would normally only be required if the Readykey for Windows had become corrupted for any reason, or if the Readykey for Windows system was being moved to a different PC.

This operation should be followed by an initialize and download, to ensure that the database on the PC is identical to that in the door controllers.

RS-232

A universal standard communications format. This format is used by multi-site Readykey for Windows systems to allow remote door controllers to communicate to a MS CNC via line drivers, modems, etc.

Security Block

A device which is connected to the parallel (printer) port of a PC on the Readykey for Windows system. On a multi-workstation system, the security block should be connected to the Readykey server.

Single Site

A collection of Readykey door controllers which are connected together using the Readykey six wire bus. The maximum number of door controllers is dependent on the Readykey for Windows system purchased.

Site

A group of one or more door controllers which are in the same physical building, and share a common communications route to the master.

Six Wire Bus

A Readykey communications protocol for connecting Readykey door controllers together and to the master. The bus uses standard 6 core 0.22mm^2 security cable. The maximum distance between any two items on the bus is 1500 feet/500m. Overall maximum bus length is 3000 feet/1km.

Status

A special Readykey for Windows application which can be used to find the current condition of Readykey hardware - e.g. door controllers, doors, inputs on Alarm Event Managers, etc.

Timeout

In order to protect the security of the PC database, every operator who wishes to make a change to the system must first log in. If the operator leaves the PC unattended for any length of time, but still is logged in, then the system will automatically log the operator off if a length of time equal to the timeout passes without any keyboard or mouse activity.

Time Period

A means of defining a limited time during which access may be controlled. Consists of a start time, end time, and one or more days.

Time Profile
A group of up to three time periods, which may be assigned to an access group to restrict a keyholders access to within the defined time limits. May also be assigned to a door to unlock the door during the defined time.

Transaction
Any event that occurs on a Readykey for Windows system is called a transaction. All transactions which originate from a door controller are reported to the PC, and stored on the hard disk for later analysis. In addition, the Readykey for Windows system then decides the fate of each transaction - display on screen, printer, generate an alarm, etc.

Unaccepted Alarm
An unaccepted alarm is one which has not yet been acknowledged by an operator presenting a valid key/card.

Unauthorized Access
A special kind of transaction which occurs when a door is opened without a valid key/card being presented to the Readykey reader, or the request to exit switch being pressed.

Uncleared Alarm
An alarm event which may have been accepted by an operator, but the condition that initially caused the alarm is still outstanding. An example would be an unauthorized access alarm which has been accepted, but the door is still open.

Update
Any changes that are made to the Readykey for Windows database are automatically sent to all relevant door controllers in the form of ‘updates’. This is a small ‘packet’ of information that the door controller can understand, and use to adjust its own database accordingly. An example would be a new keyholder being added - this would require the keycode and access information to be sent to the door controllers.

Visual Verification
This is a software feature that allows an operator to compare a person’s appearance with that in a personnel database. This module is supplied with purchase of the Photo ID Module.

Visitor
A keyholder who is only allowed access for a limited number of days. The system will automatically restrict the keyholders access to the allowed dates.

Workgroup
Used for keyholder management. A large keyholder database may be divided into departments and workgroups for searching and reporting. Each department may have one or more workgroups.

Workstation
A PC that is used to administer Readykey for Windows. All systems have one workstation. However, Readykey for Windows may be administered from more than one workstation simultaneously.