R A D I O N I C S

READYKEY® K6100 Readykey for Windows™

Network Operational Overview and Requirements

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

Trademarks

Background

Readykey for Windows is the Microsoft Windows based PC software which may be used to monitor and administer the Radionics Readykey access control system. The purpose of this document is to describe how it is possible to use several PCs on a Local Area Network (LAN) to perform one or more functions.

The Access Control System

The Radionics Readykey access control system consists of electronic keys and cards, door readers, door controllers and the optional Readykey for Windows PC administration software. The keyholder's unique identification can take the form of proximity key fobs or cards, magnetic stripe cards, or other types of Id devices. The door readers are located on one or both sides of a door, or other access point. These readers read the unique code in each Id device and pass the code to a nearby door controller. The door controller compares the code with information stored in its own local memory. If the keyholder is allowed through the door at that time on that day then the door controller will operate the lock to open the door.

It is important to realize that all the operations described earlier occur within the dedicated electronics and cabling of the access control system. *At no time is a PC or network communications involved in the routine operation of controlling access through protected areas.* The purpose of the PC software is to provide an easy way of programming and monitoring the system. Typical routine tasks carried out at the PC include:

- Issuing new Id devices
- Deleting existing keyholders or Id devices, perhaps if lost or stolen
- Modifying existing records when a keyholder's access requirements change
- Manually locking and unlocking doors
- Monitoring of Alarm or Emergency conditions of protected areas within the system
- Analyzing and reporting on past events, e.g. tracing use of a particular Id device

As well as such routine operations the PC software is also used for the configuration of the system hardware. This would normally be done by installation or maintenance personnel familiar with the components, rather than a normal system operator.

PC Communications

This section gives a brief description of the devices that connect to each PC's serial port. For further information consult the Readykey for Windows technical documentation.

Communicating with Door Controllers

The first requirement of any PC based system, whether a single PC or networked PCs, is to communicate with the access control hardware. This is achieved through the PC serial port. Usually only one port is required, but it is possible to communicate with more than one group of door controllers from the same PC. Note: that if you expect to use more than one serial port, then you may need to install additional ports on the PC being used.

It is through the serial port that:

A. All changes made to the system are sent to the door controllers,

B. All events that occur at the door controllers are received back at the PC.

There are two types of ordinary methods that the PC can communicate with the door controllers:

The PC Interface Kit or RS-232 Direct Serial Link

These methods allow up to 8 door controllers to be administered. The PC interface kit will consist of an AC powered box with connections for the PC serial port, the first door controller (up to 3000ft away) and a desktop reader. The desktop reader of the PC interface kit is used for reading proximity keys or cards into the system unless supplemented with a wiegand interface unit and a different type of Id device reader. For the method using the direct RS-232 Link, the first door controller must be located within 50ft. of the PC.

The Central Network Controller (CNC)

The CNC is used on larger systems. It allows up to 32 door controllers to be administered through a local port. It also has three RS-232 serial ports that allow the use of dial-up modems to control remote sites. The CNC contains a proximity administration reader built into it's front panel.

Key or Card Administration

Id device administration includes:

- Adding new Id devices to the system
- Searching for a the holder of a key or card by presenting it to the administration reader or typing the unique coding for the Id device used
- Logging into the system with a key or card
- Accepting alarms with a key or card

A PC Interface Kit may also be used on its own for key or card administration. Usually this will be the case when:

1. To provide a proximity reader for reading keys or cards into the system connected to a workstation.
2. The system may use non-proximity keys, such as magnetic stripe, in which case a supplemental wiegand interface and reader is required when a CNC is the Master.

PC Operating System

Readykey for Windows can operate with any of the following operating environments on **a single, non-networked** PC:

- MS-DOS 5.0 and above *plus* Microsoft Windows 3.1
- MS-DOS 5.0 and above *plus* Microsoft Windows for Workgroups 3.11
- Microsoft Windows 95

Readykey for Windows can operate with any of the following operating environments on a **networked** PC:

- MS-DOS 5.0 and above *plus* Microsoft Windows for Workgroups 3.11
- Microsoft Windows 95

Note: *The current version (3.x) of Readykey for Windows does **not** work solely under Microsoft Windows NT. Microsoft Windows NT can be used as the File Server, as long as the PC's operating Readykey for Windows are running Windows for Workgroups or Windows 95.*

Networked systems will also require the following:

- A network interface card (NIC) supported by Windows for Workgroups or Windows 95.
- Client software for attaching to other network servers such as Novell Netware or Microsoft Windows NT.

Please note that it is still essential that Microsoft Windows for Workgroups or Microsoft Windows 95 is used ***even on server based systems*** *- described later.*

PC Specification

Shown here is the ideal PC specification for a typical Readykey for Windows installation. Like any Windows software the more RAM your system contains the better. Higher hard disk capacities usually reflect higher hard disk performance. This is especially important if the PC is to be Peer to Peer server. Beyond this there are no particular special requirements for the PC.

Note: there is no point putting more than 32 Mb RAM in a Windows for Workgroups PC, as this operating system will not use more than that amount.

All the minimum specifications below assume the following throughout:

14" SVGA Display (800x600)
3½" Floppy Drive
Keyboard
Mouse

Network Interface Card

MS-DOS 5.00 or above (recommended MS-DOS 6.22) plus Microsoft Windows for Workgroups 3.11 or Microsoft Windows 95

Ideal Specifications

Peer to Peer File Server

133 MHz Pentium Processor
32 Mb RAM or more
1 Gb Hard Disk or more

Standalone PC or Network Workstation running Alarm

100 MHz Pentium Processor
16 Mb RAM or more
500 Mb Hard Disk or more

Network Workstation that does not run Alarm

75 MHz Pentium Processor
8 Mb RAM or more
500 Mb Hard Disk or more

Absolute Minimum Specification

This specification will allow Readykey for Windows to run but its performance will be poor. It may be suitable as an occasional workstation.

66 MHz 486DX2 Processor
8 Mb RAM or more
200 Mb Hard Disk or more

Network Services Required

This section describes how Readykey for Windows may use a network and the services that need to be available over the network.

Data Storage

Before describing the network options, it will be useful to understand how Readykey for Windows stores and manages its data.

Whatever the network configuration, there is only **one** copy of the data stored anywhere in the system. It is not possible to have two or more copies of the data in different locations, unless for backup purposes, without a possibility of data corruption.

There are two types of data stored by the system. The first type is the database, which contains all the data relating to the hardware configuration and keyholder access. The second type is the transactions, that is the storage of all the events that have occurred within the system. Described later, there will be a more detailed description on how Readykey for Windows works and operation of the different applications.

The files are stored and maintained using the Btrieve filing system. These files can only be accessed from the Readykey for Windows program, and are not accessible from outside programs. Other programs using the Btrieve filing system may not operate on the same PC using Readykey for Windows.

The Database

Whenever changes are made to the database through the PC, an update is generated which is communicated through the serial link to the door controllers. For example, when a keyholder is added to the system the database is modified, then a record is added to the update queue. This queue is constantly processed and the necessary information sent to all or some of the door controllers and central network controllers on the system.

Transactions

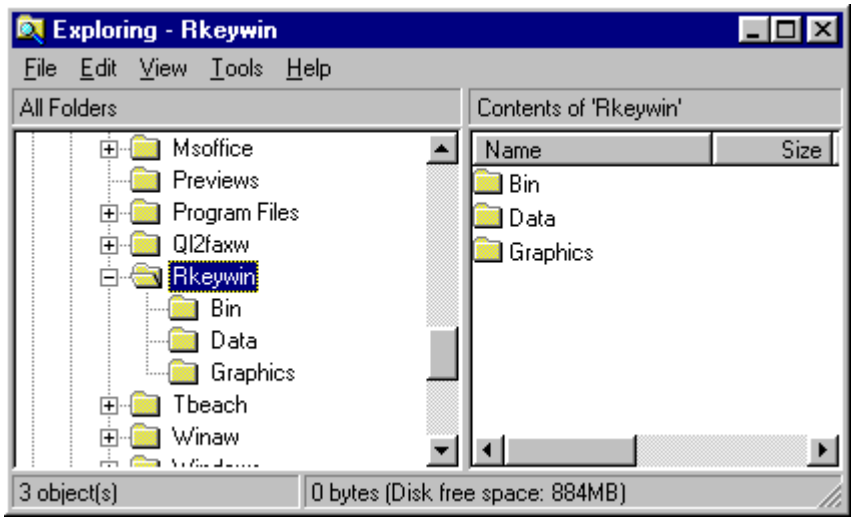
The Readykey for Windows software constantly monitors the door controllers and central network controllers and gathers events from them. These events are stored within series of numbered files on the DATA directory. Each file grows until it is approximately 1.2 Mbytes in size, and then a new file is started. An application is provided within Readykey for Windows to allow completed files to be copied (archived) to floppy disk storage. The most recent six transaction files are kept in the DATA directory for faster analysis.

Directory Structure

All Readykey for Windows systems are installed into the same directory structure. This process is controlled entirely by the installation program. Do not be tempted to move files around once the system is installed. At installation you can choose the location and name of the base directory. In a standalone or workstation installation the default is C:\RKEYWIN.

Whatever the type of installation both workstations and servers must have the same directory structure. The main difference will be that only **one** DATA directory contains the Database and Transactions.

No files are located in the base directory. All files are stored in one of the sub-directories, as follows:



The BIN directory

This contains all the executable programs plus some configuration files, such as LOGIN.INI and ALARM.INI. On a file server based system this is where the shared programs are stored.

The DATA Directory

All the data used by the system, with some minor exceptions, is stored in the DATA directory. This is a sub directory of the directory into which Readykey for Windows was installed. Although all workstations have a DATA directory, only one stores the main database.

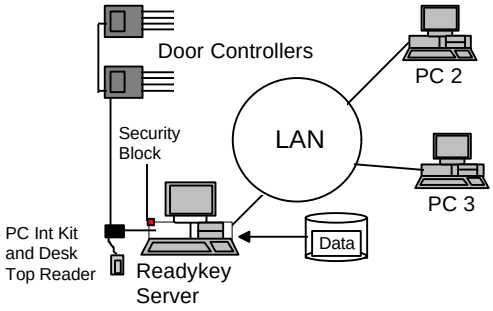
The GRAPHICS Directory

This subdirectory is used to store images that may be used in the Alarm application.

Network Types

There are two ways in which Readykey for Windows can operate over a LAN:

Peer to Peer

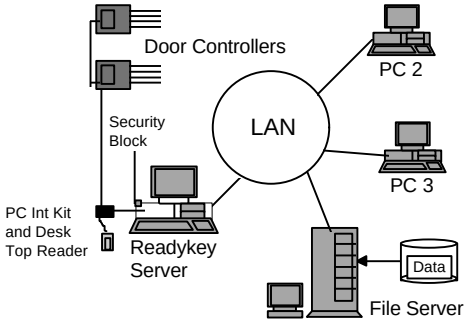


In a peer to peer arrangement all the data is stored on one PC, the 'Readykey Master Server'. This PC will have the Security Block (Dongle) installed on the LPT1 parallel port. This is not always the PC that communicates directly with the door controllers. This PC then shares its Readykey for Windows base directory with Read/Write access to all of the workstations attached to the system.

Up to three additional workstations can then connect to this shared directory. The Readykey Master Server PC must be switched on and operating the Readykey for Windows software for any of the other PC workstations to run Readykey for Windows.

Peer to Peer configurations demand an enormous amount resources to be drawn from the Readykey Master Server. Considerations to dedicate the Readykey Master Server soley for this purpose is strongly recommended.

Server based



In a server based system, each PC running Readykey for Windows is connected to a dedicated file server. Typically this file server will be running a Network Operating System (NOS) such as Novell Netware or Microsoft Windows NT Server. The file server acts purely as a storage area for the Readykey for Windows programs and data, no Readykey for Windows programs will run solely on the server. The Security Block (Dongle) cannot be connected to the file server, neither can the server communicate with door controllers directly.

One of the PCs connected to the file server will have the Security Block connected to its parallel port and may also communicate directly with the door controllers. This will be the Readykey Master Server PC. The Readykey Master PC must be switched on and operating the Readykey for Windows software for any of the other PC workstations to run Readykey for Windows.

Network Services

There are two main requirements of the network when operating Readykey for Windows on a network. The first is the ability for each workstation to be able to connect to the shared directory. The second required service is the Network DDE. This is a feature of Microsoft Windows networking that enables applications on different PCs to communicate with each other.

Shared Directory

This may be on a PC (peer to peer) or file server (server based). A connection can usually be made with File Manager under Windows for Workgroups, or Network Neighborhood, Explorer or My Computer under Windows 95. The connection can be made either to a shared directory on the Readykey Server, or a file server directory.

In a peer to peer system, the Readykey Server shares its base directory using File Manager in Windows for Workgroups, or Network Neighborhood, Explorer or My Computer in Windows 95.

Network DDE (NetDDE)

NetDDE is a service that allows applications to communicate between PCs over a network. In order for NetDDE to work, the network protocol and network devices must allow the NetBIOS protocol to operate between all the PCs running Readykey for Windows. This is enabled differently for each operating system under Windows for Workgroups or Windows 95.

Windows for Workgroups

Ensure that one of the following protocols has been installed in Network:Network Setup**.** This is shown in the Network Drivers section.

- IPX/SPX compatible transport with NetBIOS
- NetBEUI
- TCP/IP-32b

The first two are standard protocols supplied with Windows for Workgroups, the third, TCP/IP-32b, is available separately from Microsoft. The same protocol should be installed on all PCs using Readykey for Windows. Usually only one is necessary, but Windows for Workgroups network Setup usually installs the first two automatically to be default.

Use **Control Panel:Network:Startup** to ensure that Network DDE is enabled.

Windows 95

Use **Control Panel:Network** and check that one of the following protocols are installed :

- IPX/SPX compatible protocol
- NetBEUI
- TCP/IP

If IPX/SPX is installed then you should also ensure *that NetBIOS support for IPX/SPX compatible protocol* is also installed. If not, then select Properties of IPX/SPX compatible protocol and select *NetBIOS support* under the NetBIOS tab.

Readykey for Windows places the following line in the WIN.INI file:

```
Load=NETDDE.EXE
```

This ensures that NetDDE is loaded and available as soon as the PC starts up.

Note: This line is only installed on a new installation within Windows 95. This line will need to be manually added if the orignal Readykey for Windows installation was performed within Windows for Workgroups.

How Readykey for Windows Works

It is first necessary to understand how Readykey for Windows uses shared files and NetDDE to allow more than one PC to monitor and administer the system.

Readykey for Windows uses several different application programs to perform the various functions within the system. An example this type of application would be the Personnel (PERSONEL.EXE) application which is called up from the main Login applications when required. There are three main applications that will usually need to run continuously.

LOGIN.EXE

This application is the first to be run when Readykey for Windows is started. Its first task, within in a multi-PC system, is find the Security Block to obtain the stored configurations. It will check the local PC's parallel port to see if one is installed locally. If not found it will communicate (using NetDDE) with the Readykey Master PC - which will have the Security Block installed.

If the Security Block cannot be found then a message will displayed to that effect. The most likely reasons for this are:

- The Readykey Master PC is not running Readykey for Windows
- The workstation PC cannot communicate with the Readykey Master PC through the network with the NetDDE. (see Troubleshooting)

Once the Security Block is found then the PC will check that the number of concurrent PCs operating Readykey for Windows has not been exceeded. If not then the operator will be able to login.

ENGINE.EXE

While Login starts, the Readykey Engine application is started at the same time. This is the application that deals with communications between the PC and the access control system hardware. The Engine uses NetDDE communications to communicate with the Engines on other PCs.

ALARM.EXE

It monitors all events that are received into the transaction files and decides which action to perform. The way each event is handled is determined by the Transaction Routing configuration that is set up (this is in the Admin application). Alarm is required if you want to view or print on-line events as they happen.

Installing Readykey for Windows

There are several alternatives when installing Readykey for Windows, each with several steps. These steps are fully documented in the K6100 Readykey for Windows Software Installation Manual. This section gives some extra detail as it applies specifically to networked installations.

Peer to Peer Installation

These are the steps required to establish a Peer to Peer base Readykey for Windows system. A maximum of up to four PCs (or workstations) total, including the Readykey Master Server is allowed.

Network Requirements

Before attempting to install Readykey for Windows, establish that each PC can operate and communicate correctly connected to the Window for Workgroups or Windows 95 network.

1. Ensure that the Windows networking has been set-up correctly on each PC. It is recommended that all the PCs are in the same Workgroup. An example would use the Workgroup name *RKEYWIN*, and use a Computer Name for each PC such as *RKey1*, *RKey2* etc. **Warning:** Do **not** use spaces in the Workgroup name or Computer Name - this can cause known problems with Windows networking.
2. Now view the RKEYWIN Workgroup with File Manager under Window for Workgroups or Network Neighborhood under Windows 95, and browse each PC in the Workgroup.
3. Check that NetDDE is active by using the Windows CHAT application found in the Network program group under Windows for Workgroups. Each PC should be able dial and communicate with all the others on the network and get a response.

Installing the Readykey Master Server

1. Connect to the first PC, which will become the Readykey Master Server, the security block to the LPT1 parallel port which is required for the system to be operational.
2. Install Readykey for Windows, following the K6100 Readykey for Windows Software Installation Manual, and select the Standalone PC option.
3. Select the directory in which Readykey for Windows will be installed, the default will be C:\RKEYWIN.

After Readykey for Windows has been installed it is important to treat this as a single PC system at this stage. Confirm the communications with the access control hardware and normal keyholders operating *before* attempting to get further workstations installed. Standard system setup procedures are described within the Installation manuals provided with the Readykey for Windows software package.

While completing this process of installation use the Installer:Workstations application to create each workstation that will be used on the system. Record the number of each workstation (number 1 is already set-up as Default Workstation) and give it a meaningful Name that will be utilized later for reference.

The following settings have been made to the WIN.INI file on the Readykey Master Server:

```
[Btrieve]
options=/m:48 /p:3584 /b:16 /f:80 /l:20 /n:12

[PAC Windows]
TRMPath=C:\RKEYWIN
SRVPath=C:\RKEYWIN
```

Installing Workstations

Once the system is operating correctly on a single PC then prepare to install Readykey for Windows into additional workstations on the other PCs to be connected to the networked system.

1. The first step is to share the RKEYWIN base directory. Do this using **File Manager** under Windows for Workgroups or **My Computer** under Windows 95. The Sharing rights should be set to establish Read/Write capabilities that can be password protected if you wish. Then start the Readykey for Windows application and leave running in the background.
2. Each of the other PCs should then be able to make a connection to the Shared RKEYWIN directory. This will be given a drive letter normally “R:”, if not used. If the Readykey Master Server has only allowed the ability to share the RKEYWIN directory, then the workstations will only see the three RKEYWIN sub-directories on Drive R:
3. Install Readykey for Windows on one of the workstations. Select either *Local Program Files* or *Shared Program Files*. Local Program Files, which is recommended, will make the system respond faster and reduce network traffic.
4. When asked for the directory into which to install Readykey for Windows for a Local Program Files installation select the C:\RKEYWIN directory which is the default. You will then be asked for the location of the shared installation and Enter R:\RKEYWIN. This document assumes that the Readykey Server is sharing it’s C:\RKEYWIN directory, otherwise specify the according shared directory source, and the workstation has connected to it as drive R:, or corresponding drive location on custom installations.
5. Enter the PC Number, which was requested when you set up the Workstations within the Installer applications - described earlier.

The following settings have been made to the WIN.INI file on the workstation:

```
[Btrieve]
options=/m:48 /p:3584 /b:16 /f:80 /l:20 /n:12

[PAC Windows]
TRMPath=C:\RKEYWIN
SRVPath=R:\RKEYWIN
```

Once the installation has been completed start up the Readykey for Windows program on the workstation. If everything has been set-up and installed correctly, then Readykey for Windows will communicate and the system will be able to login. If not then see the Troubleshooting section later in this document.

Repeat the process until all the workstations are installed.

Server Based Installation

Network Requirements

Before attempting to install Readykey for Windows, establish that each PC can operate and communicate correctly on the Windows for Workgroups or Windows 95 network. You should also ensure that it can communicate with the File Server as well. If this is a Windows NT Server then the network software provided by Windows for Workgroups or Windows 95 is sufficient.

If a non-Windows server is being used then the client software for that network needs to be installed.

1. Verify that each PC can connect to the file server. To do this each PC (or user) will need to have an account set-up that allows access to the file server. This account must allow full read/write access to the shared RKEYWIN directory normally located within drive R:
2. Then make sure that Windows networking has been set-up correctly on each PC. It is recommended that all the PCs are in the same Workgroup. An example would use the

Workgroup name *RKEYWIN*, and use a Computer Name for each PC such as *RKEY1*, *RKEY2* etc. Do **not** use spaces in the Workgroup name or Computer Name - this can cause known problems with Windows networking.

3. Now view the Workgroup in File Manager under Windows for Workgroups or Network Neighborhood under Windows 95, and browse each PC in the Workgroup.
4. Check that NetDDE is active by using the Windows CHAT application found in the Network program group under Windows for Workgroups. Each PC should be able dial all the others and get a response.

Installing the File Server

The first step in setting up a file server based system is to create one or more user accounts on the file server. The next step is performed during the installation process creating a directory, RKEYWIN by default, and its three sub-directories on the file server. To do this the user logged into the file server must have the rights to create a directory. Subsequently, once the directory is created, user accounts need only have read/write access to the RKEYWIN directory itself.

A drive will normally be mapped to the shared directory on the file server. This may be done from the login script for Novell Netware, or in File Manager using the Reconnect at Startup option. For this example we will assume drive R: is the file server drive.

1. Install Readykey for Windows and select the File Server Installation option.
2. Select the directory in which Readykey for Windows will be installed, e.g. R:\RKEYWIN.
3. The installation process will then copy files to the file server.

This process **only** copies files to the file server. No Program Group or Icons are created on the workstation, neither are any files copied to the workstation itself. The next step is to perform a workstation installation on the same PC.

Installing the First Workstation

1. Install the security block on LPT1 of this Readykey Master PC.
2. Install Readykey for Windows. Select either *Local Program Files* or *Shared Program Files*. Local Program Files, which is recommended, will make the system respond faster and reduces network traffic.
3. When asked for the directory into which to install Readykey for Windows select C:\RKEYWIN which is the default. You will then be asked for the location of the shared installation. Enter R:\RKEYWIN. This document assumes that the workstation has been mapped and using it as drive R:, otherwise specify the shared directory source and corresponding drive location.
4. Enter the PC Number, this will be 1 as this is the first workstation that will become the Readykey Master Server.

After Readykey for Windows has been installed it is important to treat this as a single PC system at this stage. Confirm the communications with the access control hardware and normal keyholders operating *before* attempting to get further workstations installed. Standard system setup procedures are described within the Installation manuals provided with the Readykey for Windows software package.

Then start the Readykey for Windows application and leave running in the background.

As part of this process you should use Installer:Workstations to create each workstation that will be used on the system. Record the number of each workstation (number 1 is already setup as Default Workstation) and give it a meaningful Name that will be utilized later for reference.

The following settings have been made to the WIN.INI file on the workstation:

```
[Btrieve]
options=/m:48 /p:3584 /b:16 /f:80 /l:20 /n:12

[PAC Windows]
TRMPath=C:\RKEYWIN
SRVPath=R:\RKEYWIN
```

Installing Further Workstations

Once the system is working correctly on a single PC you can then install additional workstations.

1. Install Readykey for Windows on one of the workstations. Select either *Local Program Files* or *Shared Program Files*. Local Program Files, which is recommended, will make the system respond faster and reduce network traffic.
2. When asked for the directory into which to install Readykey for Windows for a Local Program Files installation select the C:\RKEYWIN directory which is the default. You will then be asked for the location of the shared installation and Enter R:\. This document assumes that the Workgroup is sharing the R:\RKEYWIN directory, otherwise specify the according shared directory source, and the workstation has connected to it as drive R:, or corresponding drive location on custom installations.
3. Enter the PC Number recorded from when you set up Workstations - described earlier.

The following settings have been made to the WIN.INI file on the workstation:

```
[PAC Windows]
TRMPath=C:\RKEYWIN
SRVPath=R:\RKEYWIN
```

Once the installation has been completed start up the Readykey for Windows program on the workstation. If everything has been set-up and installed correctly, then Readykey for Windows will communicate and the system will be able to login. If not then see the Troubleshooting section later in this document.

Repeat the process until all the workstations are installed.

Troubleshooting

The are many potential problems that can prevent the installation and operation of Readykey for Windows on a network. Most of these problems are caused by a failure of one of the two network services, read/write access to a shared directory or drive, and NetDDE between workstations.

Some simple questions to ask when troubleshooting are:

"Has it ever worked?", If the answer is “Yes” then investigate what has changed since the system last worked. If the answer is No, then you must take a step by step approach to ensure that all the services needed are in place.

"Does it fail every time?", If Yes then review the following message to see which ones may apply.

Unable to Find Security Block

If this happens on the PC with the Security Block, then it may be that the LPT1 parallel (printer) port has failed. See if it is possible to print to the printer port. If it has never been possible to find the Security Block, check the BIOS settings of the PC. Some PCs allow a variety of different modes of operation for parallel port. Try setting the mode to 'AT compatible' rather than 'Bi-directional' or 'ECP'. Note that these terms may vary from PC to PC.

If this happens on a workstation then there first check that the PC with the Security Block is switched on and running Readykey for Windows.

If the PC with the Security Block is running Readykey for Windows, then it is possible that NetDDE is not operating between the two PCs. Use Windows Chat to try and communicate between the two PCs.

If NetDDE is not operating, the check:

- The two PCs are using the same network protocols that support NetBIOS, i.e. NetBEUI, IPX/SPX with NetBIOS or TCP/IP.
- If using Windows for Workgroups, ensure that Network DDE is enabled under Control Panel: Network: Startup)
- If using Windows 95 then check that NetBIOS is selected in Properties when using IPX/SPX.
- If using Windows 95 then check that the `Load=NETDDE.EXE` command is used within the WIN.INI.

File not Found Error

You may see this error when first starting Readykey for Windows on a workstation. This will be due to a failure to see the shared files. This might be because:

- You are not logged into to the file server.
- You are logged in to the file server but not with the right account to access the shared directory.
- The file server, or Readykey Master Server in a peer to peer system, is not operating or switched off.
- Due to a network fault the shared files are not available.
- The settings in WIN.INI are incorrect.

To check most of the above use File Manager under Windows for Workgroups or Network Neighborhood under Windows 95 to attempt to view the shared files. If they are visible then check the `SRVPath=` setting in WIN.INI under `[PAC Windows]`to see that it indicates the correct path.

Permission Error

This is due to not having the correct rights to write to the shared files. Check that the sharing rights have been set correctly (within Windows for Workgroups or Windows 95) or that your user account (Windows NT, Novell Netware) allows you to write to a file.

Various File Errors

There are several file errors that can be received when starting Readykey for Windows, that result from incorrect Btrieve settings. These can often occur if a database such as Microsoft Access, often installed as part of Microsoft Office, has been installed. Such products often set their own Btrieve parameters in the WIN.INI file.

Ensure that the following settings are found in WIN.INI:

```
[Btrieve]
options=/m:48 /p:3584 /b:16 /f:80 /l:20 /n:12
```

Make sure there is only one `[Btrieve]` heading and that there is only one `Options=` line. It is acceptable to have other lines in this section, provided they start with something other than `Options =`, e.g. `access_options=`.

Setting up a Clean System

Sometimes a particular PC can be unreliable or, for no obvious reason, will just not run Readykey for Windows or connect to the network. Over time Windows systems may accumulate a lot of system software and configuration file (.INI) settings that can become incompatible or unstable. In these cases it may be worth starting again and setting up the PC from scratch.

The following describes a technique for setting up a DOS/Windows for Workgroups PC for connecting to a Novell Netware system.

Preserving existing system

Before making any changes to the system, existing configuration files should be copied to a backup directory. For the purposes of these instructions we will call it the `c:\bak_`*`mmdd`* where *`mmdd`* is the current month and day, e.g. 0705. The following files and directories should be copied to `c:\bak_mmdd:`

`c:\config.sys`
`c:\autoexec.bat`
the `c:\net` or `c:\net` directory

In addition you should **rename** the `c:\windows` directory to `c:\win_`*`mmdd`*.

CONFIG.SYS and AUTOEXEC.BAT

The configurations below are the bare minimum needed to operate MS-DOS, Windows for Workgroups 3.11 and Novell Netware. You will need to add any extra commands and drivers to support other hardware (e.g. CD-ROM) or software.

Assumptions used below are as follows:

MS-DOS is located in directory C:\DOS
Windows for Workgroups is located in directory C:\WINDOWS
Netware files are located in C:\NET

CONFIG.SYS

This file contains the minimum necessary to run MS-DOS, Windows for Workgroups and the Netware VLM client. Notice that EMM386 is NOT used. Windows for Workgroups does not require this to be loaded, only use it if you need to load DOS files into high memory.

```
device=c:\dos\himem.sys
dos=high
device=c:\windows\ifshlp.sys
shell=c:\dos\command.com /p /e:1024
stacks=9,256
files=255
lastdrive=z
```

For U.S. systems do not use a `Country=` statement, for other countries set the number, and codepage as required.

AUTOEXEC.BAT

This file also loads the real mode ODI network drivers, the VLM shell and logs the user into the Netware server. This requires the files shown below to be in the c:\net directory.

```
prompt $p$g
path c:\dos;c:\windows
set temp=c:\temp
c:\windows\net start
cd \net
lsl
```

<Network adapter driver, e.g. ne2000 >

```
ipxodi
c:\windows\odihlp.exe
vlm
f:
login
```

For U.S. systems do not use a `keyb` statement, for other countries set the country, and codepage as required.

NET Directory

This directory should contain the following files. These are the most recent files available at the time of writing (from Novell VLMUP4).

```
LSL      COM         18,285  04/17/95  10:30
IPXODI   COM         39,748  08/08/95  14:27
VLM      EXE         37,763  10/02/95  16:15
LSL      MSG          3,551  04/17/95  10:29
IPXODI   MSG          4,334  02/01/95  13:23
DOSRQSTR MSG          9,624  06/16/95  12:37
NETX     VLM         17,390  11/21/95  15:39
GENERAL  VLM          4,958  10/02/95  16:18
AUTO     VLM          4,559  10/02/95  16:17
BIND     VLM          4,793  10/02/95  16:17
CONN     VLM         10,994  10/02/95  16:16
FIO      VLM         18,378  10/02/95  16:18
REDIR    VLM         15,258  10/02/95  16:18
IPXNCP   VLM         10,521  10/02/95  16:16
NDS      VLM          8,597  10/02/95  16:17
PRINT    VLM          8,181  10/02/95  16:18
NMR      VLM          9,874  10/02/95  16:17
NWP      VLM          6,661  10/02/95  16:17
PNW      VLM         10,140  10/02/95  16:18
SECURITY VLM          8,011  10/02/95  16:17
TRAN     VLM          1,562  10/02/95  16:16
RSA      VLM         19,633  09/26/95  10:05
NMR      MSG            620  06/05/95  13:19
```

NET.CFG

The FRAME statement should reflect the ethernet frame type in use on the network. Default for Netware 3.12 and 4.x is `Ethernet_802.2`, for Netware 3.11 and before it is `Ethernet_802.3`.

```
Link Driver 3C5X9
    FRAME=ETHERNET_802.3

Netware DOS Requester
    Preferred Server=
    First Network Drive=F
```

Windows for Workgroups

Windows for Workgroups should be installed on the workstation either from original floppies, CD-ROM or an administrative network installation.

In **Network Setup**:

Under Networks..., both Microsoft Networking and one other network should be set up. **Other** should be set to *Novell Netware (Workstation Shell 4.0 and above).*

Under Sharing..., set ‘I want to share my files...’. This is important as it also enables Network DDE to operate.

Under Drivers..., install the Network adapter (3COM Etherlink III). The protocol *IPX/SPX Compatible Transport with NetBIOS* only should be selected. Remove NetBEUI if it has been installed.

Once installed, make sure the following files are copied to `c:\windows\system`.. These are the latest (at the time odf writing) supplied by Novell.

```
NWCALLS  DLL       147,616  10/20/94  11:56
NWGDI    DLL        82,064  05/17/94  10:25
NWIPXSPX DLL        41,456  10/18/94  14:55
NWLOCALE DLL        43,088  09/20/94  12:16
NWNET    DLL       225,264  10/18/94  16:35
NWPOPUP  EXE         4,592  09/30/94  10:58
VIPX     386        23,855  05/23/94   9:51
VNETWARE 386        15,645  10/13/95  11:04
VPICDA   386        11,063  01/30/91  10:58
NETWARE  DRV       165,792  02/23/95  13:44
NETWARE  HLP       419,701  08/29/94  13:15
NWUSER   EXE         5,072  10/28/93   8:12
```

The following file corrects a problem with Windows for Workgroups when using 3COM network interface cards. This file is supplied by Microsoft as WG1004.EXE and should be copied to `c:\windows\system` directory.

```
MSODISUP 386        19,295  03/09/94  15:11
```