Doors™ in a Network Environment

Application Note

Doors™

1.0 Purpose of this Document

Doors is designed for use in stand-alone computer applications; no network functionality has been built into the program. However, with the prevalence of local area networks (LANs) in the workplace, certain sites have the need to access the *Doors* software from multiple computer workstations over a LAN.

The use of *Doors* in a LAN allows more than one workstation to access the *Doors* databases and the access control network. Certain *Doors*/Badging operations may also be performed over a LAN.

This Application Note is written for applications where the access control network directly communicates with the host workstation, either through an RS-232 serial connection or via modem. It addresses what can and cannot be done using the *Doors* program in its current version. There are very specific restrictions and limitations to *Doors* and Badging operations over a LAN and these must be recognized to ensure the integrity of the *Doors* databases and to ensure proper operation of the *Doors* program.

NOTE: There are access control/LAN applications that allow the access control network to become an IP addressable part of the network. These IP addressable applications require the use of a LAN-50 or LAN-100 Ethernet communication module. IP addressable applications are ***NOT*** *covered in this document (refer to either the LAN-50 Ethernet Communication Application Note – P/N 01881-003 or the LAN-100 Ethernet Communication Application Note – P/N 01881-001).*

This Application Note does not discuss LAN setup or configuration, as there are just too many system and network specific variables to be properly covered in this document. Please consult your Network Administrator for network configuration related information.

1.1 Applications Covered

There are three *Doors* network applications covered in this document.

1. Sharing the *Doors* Databases – allowing users on multiple workstations to perform administrative database tasks.
2. Controlling *Doors* from Workstations – using third-party software to run the entire *Doors* program from a remote workstation.
3. Operating *Doors* Badging Functions – creating and printing badges.

NOTE: Badging is a fee based, installable addition to the standard Doors program. Not every Doors installation will have the Badging feature enabled.

1.2 Limitations

At this time there is no way to directly and concurrently control access control networks from multiple workstations without using some kind of third-party software. The current version of the *Doors* program is designed to work with only one controlling workstation and to communicate with only one access control network at a time.

2.0 Sharing the *Doors* Databases

One way to use *Doors* in a network is to install the *Doors* software on a host workstation that can be shared by multiple users at remote workstations. Once *Doors* is installed, these remote workstations can run the *Doors* program and performing administrative tasks by being granted access to the *Doors* folder on the host workstation via the operating system's folder sharing feature.

The host workstation **must** be connected to the access control network, and because of this physical connection it is the only workstation that can directly communicate with and control the access control network. The following tasks can **only** be performed from the host workstation:

- manually lock or unlock doors
- upload/update information to the access control network
- download information from the access control network
- event monitoring

Sharing the *Doors* program allows remote workstations to perform the following tasks:

- access the *Doors* databases
- perform administrative tasks
  - generating reports
  - block enrolling cards
  - setting up time zones
  - setting up access groups

Figure 1 on page 3 provides a diagram of how this shared *Doors* application works.

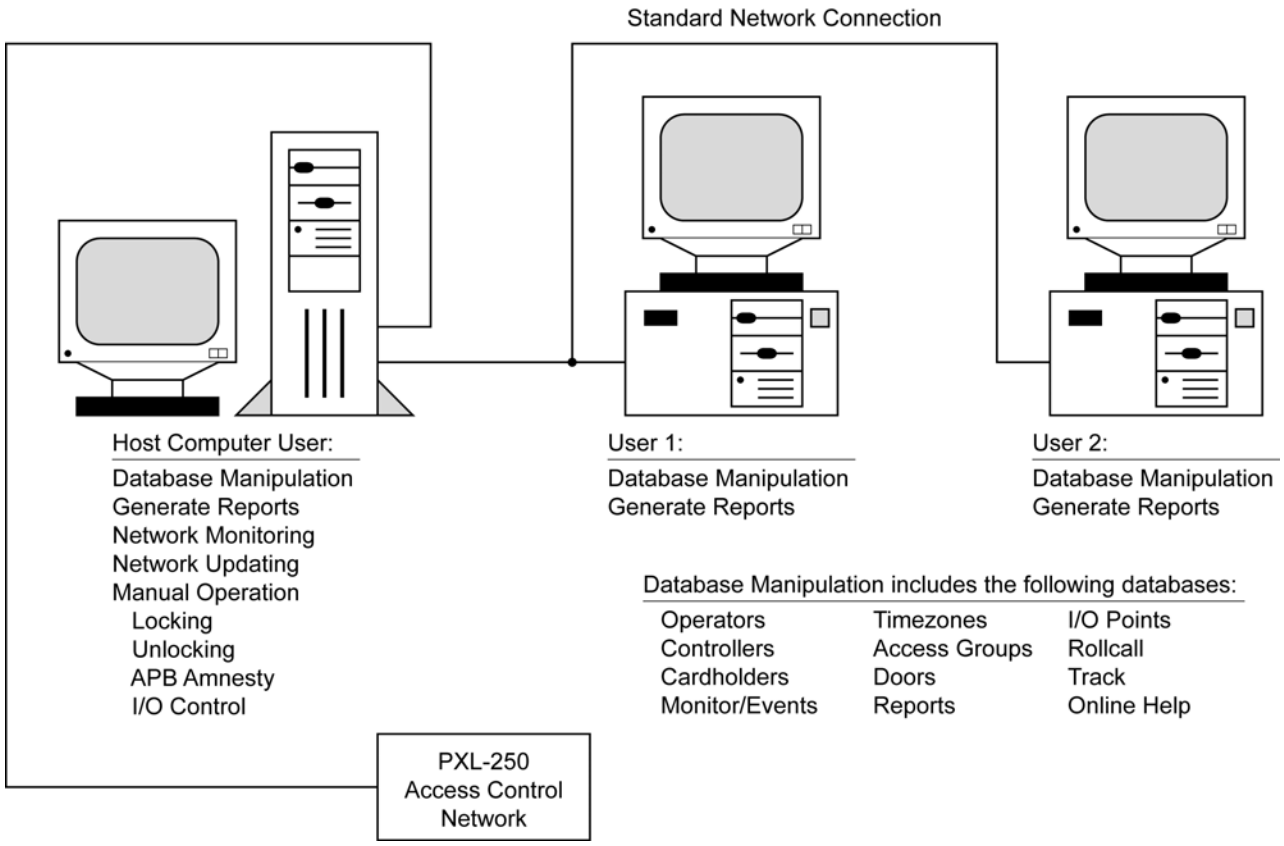

Figure 1: Sharing the Doors Databases

2.1 Sharing the *Doors* Kerisys Folder

Perform the following steps to allow users on remote workstations to access the host workstation and run the *Doors* program to perform administrative database tasks.

1. Install the *Doors* software onto the designated host workstation.
2. Using Microsoft Explorer, locate the folder in which the *Doors* software has been installed; "Kerisys" on a default installation.
3. Right-click on the folder name and the folder properties window appears. Click on the Sharing Tab (see Figure 2 on page 4).

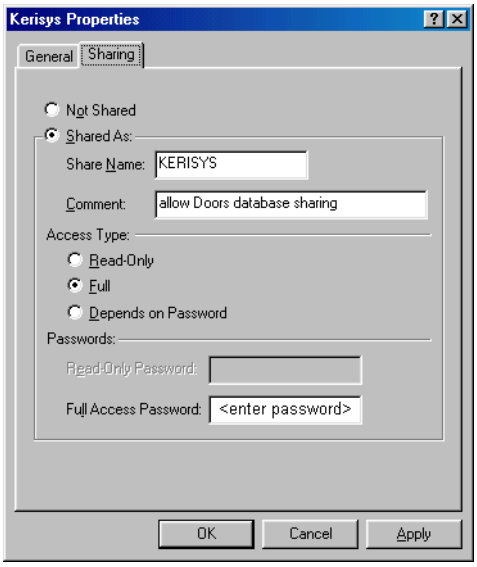

Figure 2: Sharing Tab for the "Kerisys" Folder

4. Click the **Full** radio button under Access Type to allow sharing with the *Doors* databases.
5. Click in the **Full Access Password** field and enter an appropriate password. This password must be made available to all workstations that will be sharing the *Doors* databases.
6. Click the **OK** button and the "Kerisys" folder is now shared. This can be identified by a change in the folder icon; a small hand is shown holding the folder (see Figure 3).

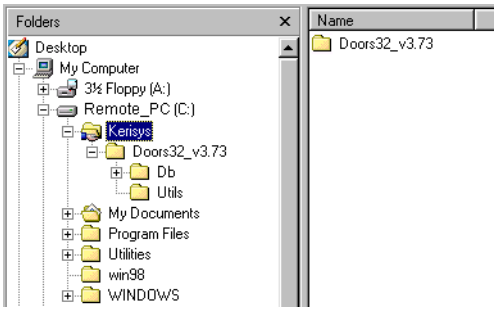

Figure 3: Shared "Kerisys" Folder

2.1.1 Creating Shortcuts at the Remote Workstations

Once folder sharing is enabled, a shortcut must be created at each of the remote workstations. This shortcut must point to the shared "Kerisys" folder on the host workstation. This shortcut provides the access path from the remote workstation to the host workstation to allow the remote workstation to run the *Doors* program and perform administrative database tasks.

*NOTE: Do **not** install the Doors software on each remote workstation. This will create unique databases on each workstation that cannot be shared between workstations. By creating a shortcut on each remote workstation to the shared Kerisys folder on the host workstation, each remote workstation uses the single Doors installation on the host workstation.*

1. Use Windows Explorer on the remote workstation to locate the “Kerisys” folder on the host workstation. Click on the folder name (see Figure 4).

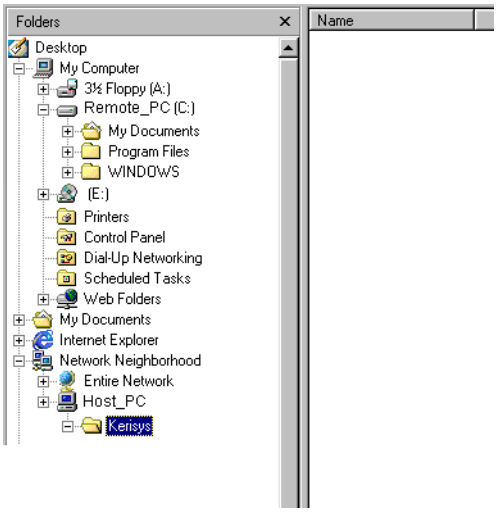

Figure 4: Locating the “Kerisys” Folder on the Host Workstation from the Remote Workstation

2. A dialog box appears requesting the network password (see Figure 5 on page 6). Click in the password field, enter the password created during the folder sharing process (see Section 2.1 on page 3),

NOTE: Just below the password field (see Figure 5 on page 6) is a check box allowing you to save the network password in the remote workstation’s password list. This is a convenience feature as it does not require you to memorize the password for future access to the Doors databases. However, it also grants Doors database access to anyone who uses that remote workstation. For complete database security, memorize your password and clear the check box.

3. Click the OK button.

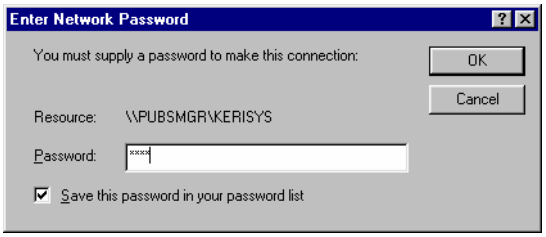

Figure 5: Enter Network Password

4. Use Windows Explorer on the remote workstation to locate the "doors32" program file in the "Kerisys" folder on the host workstation (see Figure 6).

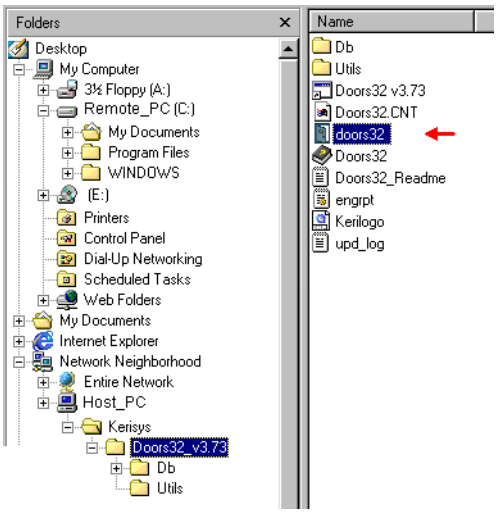

Figure 6: Locating the "doors32" Program in the "Kerisys" Folder

5. Right-click on the "doors32" program file. A pull-down menu appears. From the pull-down menu, click on "Send To" > "Desktop (create shortcut)" (see Figure 7 on page 7).

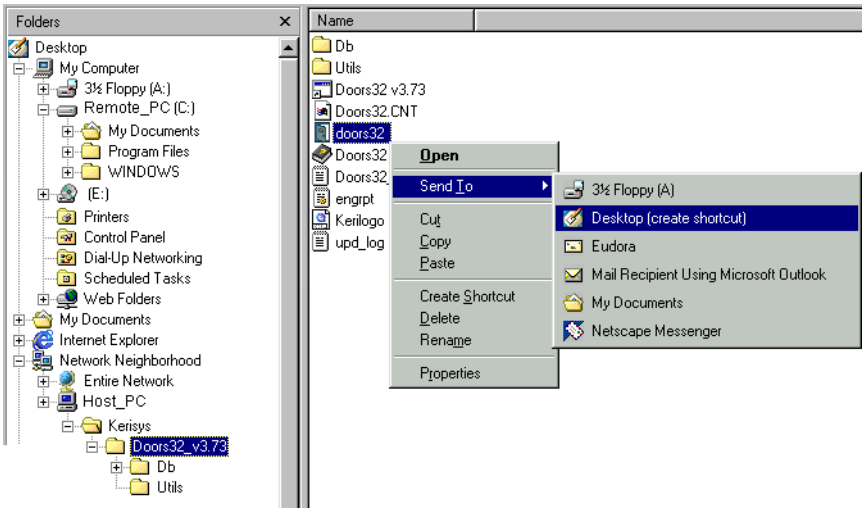

Figure 7: Send To Desktop Pull-down Menu Option

6. A shortcut acknowledgement message appears. Click on the OK button (see Figure 8).

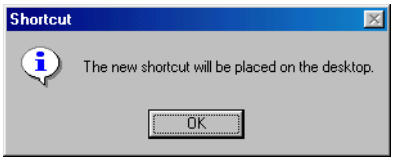

Figure 8: Acknowledge the Shortcut

The shortcut now appears on the workstation desktop (see Figure 9).

Figure 9: The *Doors* Shortcut on the Remote Workstation Desktop

2305 Bering Drive
San Jose, CA 95131 USA
(800) 260-5265 (408) 435-8400 FAX (408) 577-1792
Web: www.kerisys.com E-mail: sales@kerisys.com

2.1.2 Starting the *Doors* Program from a Remote Workstation

1. To start the *Doors* Program from a remote workstation, simply double-click on the *Doors* shortcut. The *Doors* program opens and the remote user can then begin to perform database or report work.

*NOTE: Remember, **only** the host workstation (the one physically connected to the access control network with the Doors program installed) can perform the commands that require direct communication with the network (such as manually locking or unlocking doors, uploading/ updating information to the access control network, downloading information from the access control network, event monitoring).*

*NOTE: Presentation card enrollment **must** be performed at the host workstation as presentation enrollment requires direct access to the access control network and the enrollment reader to complete this task.*

2.1.3 Warnings when Sharing *Doors* Databases

There are no notifications to indicate a database has been changed since the last time a user opened that database. If User-A and User-B have the same database open and User-B makes changes to that database, User-A must close the database and then reopen it to see any of the changes made by User-B.

More than one copy of a database can be open at the same time, which means that more than one user can be editing the same database. If User-A and User-B have the same database open and both are making changes to that database, if User-A saves one set of changes and then User-B saves a different set of changes, the changes made by User-B (the last set of changes saved) will **overwrite and undo the changes** made by User-A.

These warnings are made because whenever a database is opened remotely, a temporary copy of that database is saved on the user's remote workstation. All changes made by the user are made to the copy on the user's remote workstation. The original database used by the *Doors* program on the file server or shared folder does not receive these changes until the user clicks on the SAVE button, physically overwriting the original database in the flashover or shared folder with the newly edited information from the user's workstation. This is done to protect the original database from being affected if a user decides to cancel any changes being made.

For this reason, Keri Systems strongly recommends that only one user/workstation be allowed to view or modify a database at a time.

2.2 Operating *Doors* Badging Functions

Doors Badging operations can be run over a LAN, but as *Doors* has limitations, so does Badging. Badging operations and limitations over a LAN are described in this section.

2.2.1 Badging Software

When *Doors* is installed on the host workstation, the Badging option (which includes the GuardDraw template creation software) must be selected. For proper Badging operation, a license code must be purchased through Customer Support and entered into the *Doors* program.

NOTE: The license code is a unique number based on a computer's hardware ID number. It is ***not*** *transferable to other computers; each computer that will be printing badges will need to have its own Badging license code. Badging is a fee-based option and while Badging can be run in Demo mode without a license code, all printed badges will have "SAMPLE" watermarked across the face of the badge.*

Before printing badges, the driver for the badge printer must be installed on all workstations from which badges will be printed. Next, a badging template must be created. The template defines the content and layout of the information to be printed on the badge. GuardDraw is a standalone program used to create templates. A template can be created on any system with both the GuardDraw program and the badge printer driver installed. Basic information on creating templates is provided in the BADGING APP NOTE. Once created, the template must be saved in a specific folder on the host workstation. This ensures the *Doors* program is able to locate the template when preparing to print badges.

2.2.2 Badge Printing

The badge printer can be either directly connected to the workstation via a parallel printer port or it can be configured as either a network printer or a shared printer on another remote workstation. The badge printer driver and the GuardDraw program must be installed on each remote workstation from which badge print commands are performed.

As mentioned in the previous section, each remote workstation that needs to print a badge must have a license code and that code must be entered into *Doors* before printing the badge. If you are printing **only** from the host workstation, only one license code is required. Information on entering and saving a license number in the *Doors* program is provided in the BADGING APP NOTE.

If an incorrect license code is entered, any badge printing will be performed in demo mode which means badges printed will have a "SAMPLE" watermark across the face of the badge.

Doors does not support the concurrent use of printing licenses, which would allow several remote workstations to print badges on a first-sent, first-printed basis. Badge printing can only be done from one remote workstation at a time.

2.3 Database Sharing Example

A site has installed the *Doors* software in a shared folder in a host workstation at a guard station at the front lobby of a building. The access control network is connected to this host workstation. Three other remote workstations have shared folder access to the *Doors* program via a local area network. The following tasks could be happening concurrently.

1. The Lobby Guard is actively monitoring events on the access control network. The Guard is tracking access events with an eye for Door Forced or Door Held Open alarms. Remember that the host workstation at the guard station is the only workstation that can actively monitor events because it is the only workstation physically connected to the access control network.

2. A Security Official in the Security Office is enrolling new users into the system – block enrolling cards and entering cardholder data into the cardholder spreadsheet.

*NOTE: When sharing the Doors databases, card enrollment from a remote workstation **must** be done through block enrollment. The remote workstation the Security Official is using is not physically connected to the access control system so the Security Official cannot presentation enroll a person by presenting a card to the enrollment reader.*

3. A Clerk in the Human Resources department is editing the holiday schedule for a new year, changing the dates for holidays such as Easter and Thanksgiving (which vary from year to year).

4. A Manager is running a report on Access Granted events over the last week in December to determine who entered the building during the holiday period.

Other users could be performing similar tasks: creating or editing time zones or access groups, configuring operators, or configuring doors or controllers.

Actions such as manually locking or unlocking doors, collecting events from controllers, manually performing I/O functions, or granting anti passback amnesty must be performed by the Lobby Guard through the host workstation at the guard station.

NOTE: When changes are made that affect the operating parameters of the access control network (such as card enrollment or holiday schedule changes) the Operator controlling the host workstation physically connected to the access control network must be notified and instructed to Update the Network so that these changes are implemented by the access control network.

3.0 Controlling *Doors* from Remote Workstations on a Network

A more complete method of using *Doors* in a network is to use third-party, remote control software, such as Symantec's pcANYWHERE, to remotely control the host workstation to which the *Doors* software has been installed. Remote control software allows any user on a network to connect to a remote workstation on that network and control that remote workstation just as if they were sitting in front of that workstation. Connection can be made by modem or via network. Figure 10 provides a diagram of how this remote control accessed *Doors* application works.

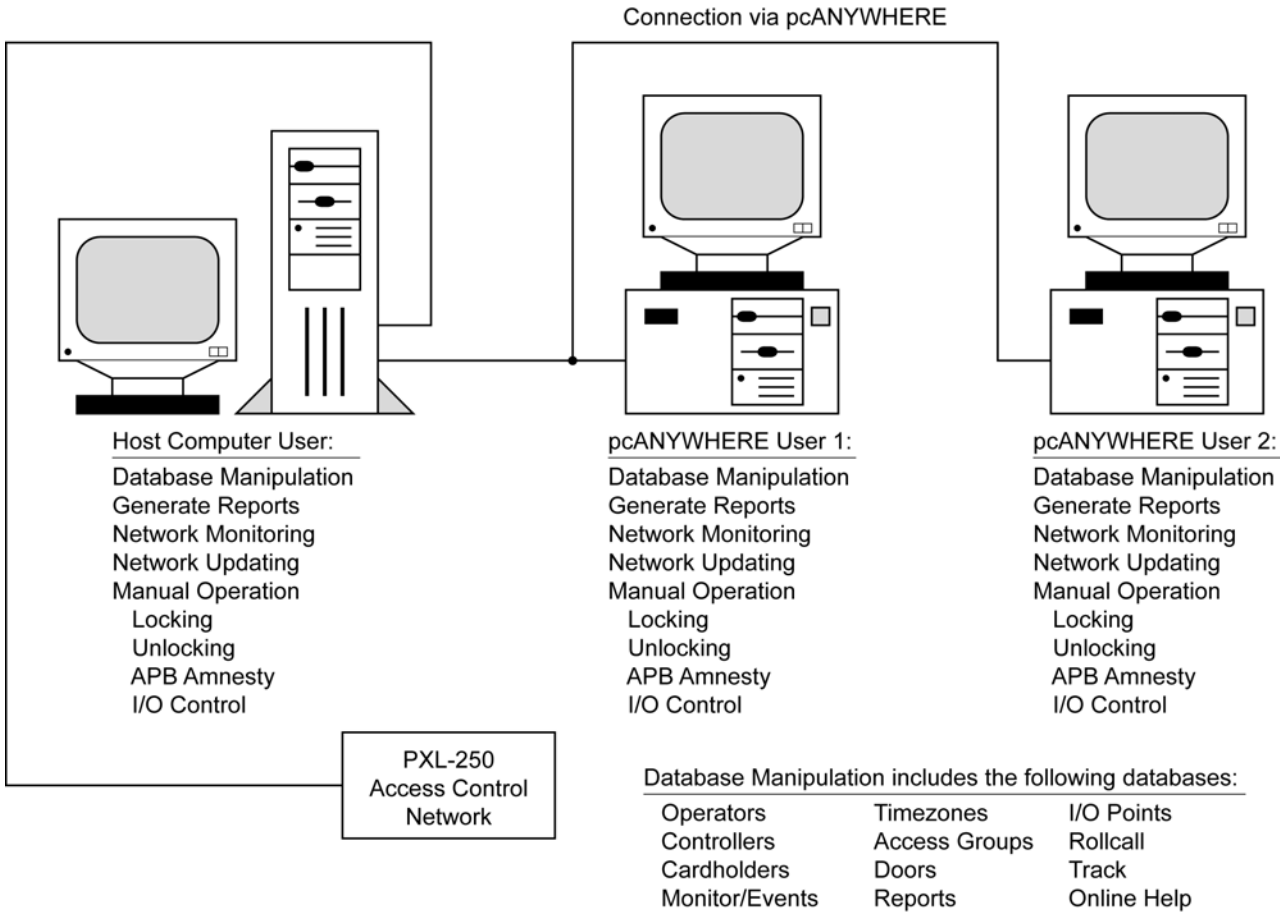

Figure 10: Controlling *Doors* from Remote Workstations

Doors™ in a Network Environment

With remote control software the user will actually run and control the *Doors* software on the host workstation from the remote workstation; **the host workstation will be unavailable for any other purpose**. Because the requirements and operation of remote control software varies by program, a detailed description of how to use this software cannot be provided. However, certain basic rules apply regardless of the remote control software package. Perform the following steps to use remote control software to run the *Doors* program from a remote workstation.

1. Install the *Doors* software on the designated host workstation.
2. Install the Host Mode software for the remote access program on the host workstation with the *Doors* software (refer to the remote control software manual for installation/configuration information – Host Mode software allows remote workstations to access the host workstation).
3. Install the Client Mode software on the remote workstations of those who wish to remotely control the *Doors* software (refer to the remote control software manual for installation/ configuration information – Client Mode software allows remote workstations to access the *Doors* host workstation with Host Mode software installed).
4. Run the remote control client software and connect to the remote control server.
5. Run the *Doors* program from within the remotely controlled host workstation by using the *Doors* shortcut on the host workstation's desktop or the Run command in the Start menu.

*NOTE: The limitation of accessing Doors via remote control software is that only **one** remote workstation can access Doors at a time. However, the advantage is that any changes or modifications made by that user can be sent immediately to the access control network without concern of interference by another user. Database conflicts that can occur when sharing the Doors databases (see Section 2.0 on page 2) cannot happen because of the one remote workstation at a time limitation.*