Full Control Internet

Management, Administration, Security And Control For Windows 95 / 98 / ME / NT / 2000 / XP

Installing, Using and Mastering Full Control Internet

Bardon Data Systems

Full Control Internet

Management, Administration, Security And Control
For Windows 95 / 98 / ME / NT / 2000 / XP

Installing, Using and Mastering
Full Control Internet

Contents

3. Security And Administration

4. The Remote Administration Manager

Appendix A: Miscellaneous

Chapter 1
Getting Started

Introduction

Full Control Internet: systems management, security, access control, event logging, web-browser tracking, remote administration, and helpdesk tools.

Full Control Internet is a remote Internet-based systems management solution for the administration of Windows (95/98/ME/NT/2000/XP) computers. It provides system administrators with comprehensive resource management, whether the resource is on the local computer, the enterprise LAN, or on the Internet anywhere in the world. Administrators can specify allowed programs, files, websites, and other resources. Full Control Internet logs the use of all resources. It also makes this information available to the administrator in real time. In addition to remote Internet-based administration, Full Control Internet includes security access control, time limits, logging, and Internet usage tracking. The combination provides effective, reliable access management and remote administration while still allowing use of the regular Windows desktop. The result is that with Full Control, computers remain stable and administrators always know what is going on.

Remote administration: Full Control Internet's system administration capabilities can maintain any size setup, from enterprise networked installations to a single standalone computer. All computers, anywhere in the world, can be managed from one central location. This includes the ability to remotely monitor, update, logoff, shut down, reboot or reconfigure Full Control Internet stations. Administrators can remotely manipulate the Registry, see and change the status of remote computers, and more, all from one central location. Administrators can also run commands remotely -- installers, uninstallers, maintenance programs, batch files, or any other software. These commands can even be broadcast to all stations at once, a handy way to automate software or file distribution or do any other mass-manipulation chores.

System stabilization: After you set up your systems the way you want them, what will keep them that way? What prevents the installation and use of unauthorized software, as soon as you turn your back? Full Control Internet features One Click System Stabilization to prevent unauthorized software download, installation, and use.

Internet and application oversight: Full Control Internet allows software or Internet usage based on the administrator's specifications. It logs all computer activity, all attempts to access unauthorized files, folders, or websites, attempted password hacking, and more. Its built-in reports and graphs can analyze this information, or the data can be exported to any database or spreadsheet.

Access control: Full Control Internet provides reliable security coverage, even in Safe Mode. It lets the system administrator specify exactly what programs can be run, by whom, and for how long. It allows full access to authorized software and Internet resources, yet prevents accidental or malicious system modifications. The user is validated at logon, can't run other programs, can't change the computer's setup, can't get to restricted files, folders, or websites. Full Control Internet can also control keyboard and mouse activity, boot-time behavior, shutdown options, file-save directories, and more.

Configuration tracking and helpdesk support: When a computer acts oddly or crashes for no reason, wouldn't it be handy if support staff could call up a minute-by-minute list of all running programs? That's what Diagnostic Snapshot Logging is all about. It even lists hidden programs that won't show up on the Close Programs (Ctrl+Alt+Del) screen. And after the problem is identified, the Rollback feature allows you to undo unintended or malicious configuration changes when misguided users, flawed applications or incomplete uninstallers make a mess of your computer.

Logon validation: Full Control Internet can validate users at logon, even on laptops and other stand-alone Windows computers -- no network or server is required. Unlike the standard-issue Windows logon screen, Full Control Internet ensures that only valid users can log on. Full Control Internet coordinates with your network server to ensure that invalid users cannot log on, even just onto the local computer.

HIPAA and Part 11 Compliance: Full Control Internet provides the enhanced oversight mandated by HIPAA, 21 CFR Part 11, and similar government regulations, with specific features needed to address these regulations.

What it looks like: By default, Full Control Internet puts a small  tray icon next to the clock on the taskbar. (It can be hidden if desired.) Click this tray icon to list the current program and user time limits, and a menu with password-protected setup and session options.

Setup and configuration: You can set up the configuration from the Administration Manager console, or from each client computer. From the Administration Manager, click the Clones menu, make your changes, then publish the new clone-settings to the managed computers. From a managed client. click the tray icon to access the setup options. If the tray icon is hidden, type the hotkey or run Full Control Internet's companion Reset program to access the setup options.

Each user is assigned to a Group, that is, a set of configuration settings. The Group Setup screen controls per-group options. Each group can have different time limits, locked or hidden directories, allowed applications, desktop look-and-feel options, and more. The user logs on at the regular Windows logon screen. If the logged-on user is listed in a group those settings are put in place for that user. For users not explicitly listed in a group, Full Control Internet can choose a group based on the user's network domain rights (if that box is checked on the Security tab). Otherwise, users get Default Group settings. Or you can set up Full Control Internet so unknown users are not allowed to log on at all.

The System Setup screen controls global options, web-browser monitoring, event logging, remote oversight management, and automated backups of critical system configuration files. These settings are active for all users whenever Full Control Internet is running.

Press F1 or click Help on each tab for its context-sensitive help, or use the Quick Start documentation for fast step-by-step setup instructions.

Installing And Uninstalling

Installing Full Control Internet: To install Full Control Internet or its Remote Administration Manager, run the program **install.exe** that comes with Full Control Internet. The installer will not put anything into any folder other than the one you specify (other than NT/2000/XP drivers which are installed into NT/2000/XP's "drivers" folder) or change any system files (other than the Registry per Microsoft standards). In NT/2000/XP, the logged-on user must have Administrator rights for the install to be successful.

Installing Administration Tools: In a regular interactive install you will be asked if you want to install the helpfile and Remote Administration Manager. In an unattended automated install, they will be installed only if you use the /admin parameter (see below for more on automated installation). The Remote Administration Manager needs to be installed on just one computer. This can be any computer with an IP address that is directly visible to the client computers it will manage. Are your client computers on networks that use NAT (network address translation, or "masquerading")? If all your client computers are on the same masqueraded subnet, the Administration Manager can be on a masqueraded computer on that same subnet. It will be invisible to the Internet, yet visible to the computers it oversees. If your managed computers aren't all on the same subnet, the Administration Manager must be on a computer with a static IP address so it will be visible to all your client computers, on all your LANs. The section on the Remote Administration Manager has more on this.

Cloning While Installing: If you have created a clone file with the passwords and settings you want, you can transfer this information to another client computer while installing. To do this, copy that clone file into the same directory as the installer, and rename it to *clonefci.bds*. When the installer runs, it will find that clone file. The updated settings are put into effect as soon as Full Control Internet starts. The clone also includes your Remote Management connection information so this is a good way to immediately set up your new computer to be overseen by the Remote Administration Manager. For more information, read about How To Clone A Computer.

Registry Backup: The first time you run Full Control Internet under Windows 95/98/ME, it creates the files *userfci.1st* and *sysfci.1st* in your Windows directory. In Windows ME it also creates a *classfci.1st* file. These are backup copies of *user.dat, system.dat*, and (in ME) *classes.dat*, the files which contain the Windows Registry entries. In addition, at the start of each Windows 95/98/ME session, Full Control Internet backs up the current Registry files to *userfci.bds, sysfci.bds*, and (in ME) *classfci.bds* in your Windows directory (c:\windows on most 95/98/ME computers) unless you check the box to skip Registry backups. To reset your system as it was prior to the current session, or prior to installing Full Control Internet, restart in DOS and copy one of these backup sets over top of *user.dat* and *system.dat* and (in ME) *classes.dat* in your Windows directory.

Uninstalling: Full Control Internet's uninstaller is listed with Full Control Internet's icons on the Start menu. It can also be run from the Start menu's Add/Remove Programs list. To cleanly uninstall, the uninstaller must be used. It is not sufficient to simply delete the Full Control Internet files.

If you are uninstalling remotely, you may want to run the uninstaller with the /auto command-line parameter, so no prompts or messages appear on the remote computer. The usage syntax for the uninstaller's /auto parameter is exactly the same as for an Automated Unattended Remote Install (see below).

Full Control Internet can't be uninstalled while it is running. In NT/2000/XP , the logged-on user must have Administrator rights for the uninstall to be successful. The uninstaller closes all active Explorer windows, a necessary step to deactivate some of the oversight components.

Automated Unattended Remote Install: The Full Control Internet installer can be run in an unattended automated mode which requires no user input. The following command-line parameters are used when doing this:

/auto	installer runs in automated mode
/addstart	icons will be added to the Start menu
/admin	also install the helpfile, Administration Manager, etc.
/targetdir=	full path to the local folder into which files should be installed
/pausecmd=secs,cmd	seconds to wait, then command to run after install

Example: \\server\c\masterdir\install.exe /auto /targetdir=c:\dir\otherdir\finaldir

The /auto item tells the installer to run in its automated mode. Without the /auto item, the installer runs in the usual interactive mode.

The /addstart item is optional. If you give this parameter, the same items are added to the target computer's Start menu as when an interactive install is performed, and a window appears showing these items. Note that Full Control Internet runs perfectly well without being listed on the Start menu.

The /admin parameter tells the installer to also include the helpfile and Remote Administration Manager. These tools should only be installed to the administration computer, so it can monitor and control the other computers.

The /targetdir item is also optional. If it is not given, Full Control Internet will be installed into the default directory, which is the \Program Files\Full Control Internet folder on the same drive as the computer's Windows directory.

The optional /pausecmd= parameter waits a designated number of seconds after a successful install, then runs a command.

Tools such as SMS can run parameterized commands remotely, or command-line parameters can be given by running the installer from a batch file, Shortcut, etc. This is easier than creating an SMS distribution. Simply place the Full Control Internet files in a network folder visible from your target computers (a

read-only folder is fine) and distribute a command that points at the installer in that server's visible folder. You can even set up the batch file to delete itself after the install is complete. See below for more on this technique.

Even without a tool like SMS, there are a number of ways to install Full Control Internet on each user's computer. First, copy the files on the Full Control Internet disk (or download) to a network directory, then you could do any of the following:

- Run the server-based install command automatically from your network's login script, by adding a command such as the following, which will install the software if it has not yet been installed on that computer:

```
IF NOT EXIST c:\your path\fcinet.exe \\server\c\somedir\install.exe /auto
```

- Or email all your users a message with a "click here" item which runs the installer from your server, perhaps from a batch file with a similar IF NOT EXIST test as shown above.

- Or place in each remote computer's Startup folder a batch file that runs the install. As above, you can use a similar IF NOT EXIST test for the install. Or even better, you can have the batch file delete itself after it has done its work by putting "del %0" on the last line. This ensures that you only install once, and it cleans up the batch file after it is no longer needed. Here's an example:

```
@echo off
\\server\c\temp\fcisetup\install.exe /auto /addstart /targetdir=c:\FC Internet
del %0
```

This will cause the batch file to run the installer in its unattended mode. The batch file will then delete itself. Because the batch file starts with *@echo off*, there is no screen output so the window closes immediately, and because it ends with del %0 the batch file deletes itself after it has run one time.

Automatic Launch: When performing an automated install, the Full Control Internet program is immediately launched by the installer. To take full advantage of this, you will probably want to clone your master setup and put the resulting clone file in the same directory as the installer program itself. If you do so, the installer will see the clone file and copy its settings and licensing information to the target computer. Then, as soon as Full Control Internet launches it will set up any options, including user management settings, "logon validation" and "run at startup" options and anything else you want to specify in the clone settings.

Upgrading From Full Control 2: Full Control Internet can read Full Control 2 clone files. To do this, go to the Remote Management tab of the System Setup screen and click the *Import Clone File* button. The old-style clone's settings will be converted automatically as they are read. Study the results to ensure that the automatic conversion meets your needs. After confirming the settings, you can export them as a new Full Control Internet clone file.

Quick Start

Full Control Internet In A Nutshell: Full Control Internet's Remote Administration Manager lets the administrator oversee and manage computers in real-time over the LAN or the Internet. Its autonomous client-side oversight enforces the administrator's designated policies on program and Internet usage by monitoring every user logon, every running program, every accessed website, and by logging all activity. If you have set up a particular application as a managed program, Full Control Internet will enforce the time limits, password protection, and other control you have specified for it. if desired, so they won't run. Full Control Internet can also restrict access to interface elements such as desktop icons, Start Menu entries, Control Panel, Explorer, and web browsers. Most restrictions can be "per-user" with different settings for each user.

In addition to controlling managed programs, the user can be validated at logon. Each user is in a group, and each group can have different oversight controls. Full Control Internet looks at the name of the current user (that is, the user name given at the regular Windows logon screen). If the logged-on user is listed in a group that group's settings are put in place for that user. For users not explicitly listed in a group, Full Control Internet can choose a group based on the user's network domain rights (if that box is checked on the Security tab). Otherwise, users get Default Group settings. Or you can set up Full Control Internet so unknown users are not allowed to log on at all.

Full Control Internet can be launched at any time, like any other program, or it can be set to launch automatically at startup in a secure way that cannot be bypassed, not even in Safe Mode. When it is launched, by default it will put a small icon  in the taskbar tray, next to the clock. Clicking this icon displays a popup menu with status and time limit information, and password-protected administration options. If the tray icon is hidden, press the hotkey or run Full Control Internet's companion Reset program to access the setup options.

The *system administrator* sets up and maintains the system. Unlike a regular user, this person has access to many system administration features that allow the administrator to set up and change the system, monitor it through usage reports and logs, and remotely control and reconfigure Full Control Internet computers over a network or across the Internet.

Quick Start: Full Control Internet comes preconfigured with default settings so that you can just install it and go. However, you will likely want to modify these default settings. Here's how:

- List the port and IP address of the Remote Administration Manager that will oversee this computer. This ensures that this computer will connect to the Remote Administration Manager each time it starts. One easy way to include these connection settings is to use a configuration clone file that is read when you install Full Control Internet; further clone updates can be sent later, on the fly

by the administrator.

- Decide if users can connect to the Remote Administration Manager from any IP address, or only from certain specific IP addresses. If the latter, list allowed addresses in the Remote Administration Manager.

- Decide if unknown users can log on, or if users must be "known" in order to use the computer. Then use the Security tab of the System Setup dialog to indicate if users must be validated at startup and what validation criteria will be applied.

- In 95/98/ME, if you want to provide each user with different Full Control Internet restrictions, set up Windows to display its "log on by user name" screen when Windows starts. (See Using The Windows Logon Screen for more on this.) However, even if you don't use the logon screen, Full Control Internet will work perfectly well by providing users the permissions and restrictions you have listed as the default.

- Configure systemwide settings with the System Setup screen. Modify the settings in the first three tabs (Setup, Security and Event Log) as needed. Use the fourth tab (Remote Management) to set up network-based Full Control Internet configuration updates, remote management and monitoring, and other communication and control options. The fifth tab (Rollback) lets you back up and restore important Windows configuration files, very handy when a misguided user or flawed application makes a mess of the computer.

- Configure your groups. Each user is assigned to a group. When that user logs on, that group's settings are put into effect. Full Control Internet comes preconfigured with a number of groups. Or, create new groups using the Configuration screen, then specify the group's settings with the Group Setup screen. You can update this group's settings at any time. You may want to copy a group and use the copy as the basis for setting up another group.

- List your users by clicking the Administration screen's Users button. Add the new users, then assign them to groups. Users can be added singly by hand, or automatically imported by reading a file. If the logged-on user is listed in a group that group's settings are put in place for that user. For users not explicitly listed in a group, Full Control Internet can choose a group based on the user's network domain rights or on an environment variable (both of these options are available on the Security tab). Otherwise, users get Default Group settings.

You're Done: Now that the computer is configured as needed, you may want to create a clone file which specifies this computer's configuration. You can then use this clone data file to dynamically update your computers. A clone file is also a good way to back-up your work.

The Setup Password

The first time you start Full Control Internet, it asks you for a setup password. This password is saved permanently so you never need to enter one again if you don't want to. However, you can change the password at any time with the Setup tab of the System Setup dialog. Security experts recommend changing your passwords regularly.

Should passwords be case-sensitive? The *case sensitive* setting of the Setup tab controls this.

The setup password can be used whenever any other Full Control Internet password is required. For example, if a managed program is password-protected, the setup password can be given instead of the program's password.

To meet the needs of certain regulatory and compliance situations, Full Control Internet can be configured to require two separate setup passwords to perform administration tasks. This is set on the Setup tab of the System Setup screen.

The pre-purchase evaluation version of Full Control Internet does not save the password from session to session. This is for your protection, to ensure that you are never locked out of the computer during your "test-drive."

Setup Mode

Setup Mode: In Setup Mode, security checks are temporarily suspended. The current user is by definition the system administrator, someone who already has access to the entire system. For such a user, further security testing serves no useful purpose. Therefore, in Setup Mode, passwords are not required or requested, and Full Control Internet won't interfere with any program. This makes it easy for the system administrator to modify Full Control Internet settings or use software tools that a normal user would not have access to.

Click the  tray icon to enter Setup Mode. If the tray icon is hidden, type the hotkey or run Full Control Internet's companion Reset program.

To exit from Setup Mode, choose *Resume Control* from Full Control Internet's main Configuration screen.

Emergency Passwords

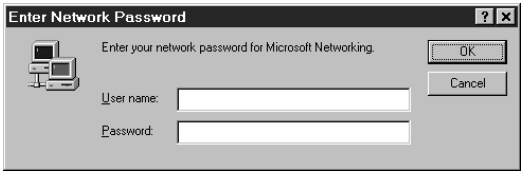
Forgot your setup password? Don't worry, you're not locked out. Each Full Control Internet system has built-in "emergency password" capability. Emergency passwords are secured so that they cannot be used in an unauthorized manner. If you are in a situation where you need one, contact Bardon Data Systems and, after providing appropriate identification, one will be generated for your specific need.

If you tried what you thought was the right password, and it didn't work, you still may not need an emergency password. Passwords are case-sensitive by default, so if your Caps Lock is on, the password might not match. Try hitting the Caps Lock key, then give the password again.

To meet the needs of certain regulatory and compliance situations, Full Control Internet may be configured so two separate setup passwords are required. The same emergency password cannot be used for both of these separate setup passwords.

The "test-drive" version of Full Control Internet has yet another built-in option. While evaluating, the setup password is not saved from session to session. This means that if you forget your password you can simply restart your computer. You will be prompted for a new setup password when Full Control Internet restarts. After purchase, this "back door" security hole is no longer active.

Using the Windows Logon Screen



Full Control Internet can use the logon name in either Windows 95/98/ME or NT/2000/XP to provide per-user validation and customization. To do this, the computer needs to be set up so it requests a logon name from the user. Here is how to set up your Windows 95/98/ME computers so users must give a logon name at startup. (Most installations of Windows NT/2000/XP already requires that users log on with a name and password, so there is nothing extra to set up.)

When you boot your 95/98/ME computer, do you see a logon screen similar to the one in the picture, which asks for your user name and password? If so, you are all set. The name given by the user in that screen will be seen by Full Control Internet when Full Control Internet starts. If that name matches a username listed in Full Control Internet, that user's set of restrictions and controls will be put into place for this logon.

If you don't mind that all users have the same restrictions, you don't need to set up Windows to display the logon screen. In that case, just set the Default User settings, and they will be put into place for every logon.

But if you want different users to get different Full Control Internet settings, the user must have a place to log in, so they can say who they are. Full Control Internet will pick up this name and configure itself for that user. If the logged-on user is listed in a group that group's settings are put in place for that user. For users not explicitly listed in a group, Full Control Internet can choose a group based on the user's network domain rights (if that box is checked on the Security tab). Otherwise, users get Default Group settings.

You can even set Full Control Internet to validate the logon. If you set this up, and the name is not listed as valid, Full Control Internet will not allow the logon to proceed.

There are a number of ways to tell Windows to display its "log on by user name" screen when Windows starts.

Of course, one way is to open the Windows Control Panel's *Passwords* applet and enable the saving of individual user profiles. If you do this, Windows will save each user's individual configuration separately, and will ask for a logon name at the start of each session so it can tell which configuration to use.

However, saving separate profiles for each user can use quite a bit of disk space. For this reason, Full Control Internet does not require that Windows save each user's individual configuration separately. All that is needed is to have Windows

display the logon-name screen itself.

To set this up, open the Network applet of the Windows Control Panel. As your Primary Network Logon, choose anything other than Windows Logon. For standalone computers or those using Windows networking, *Client for Microsoft Networks* is a good choice. If it's not already on the list, click the Add button and add this client. When you click OK to leave the Network applet, Windows will ask you to provide its installation disk, then it will want to reboot.

When Windows comes up again, you will see the logon screen. Give a logon name and (optionally) a password for that name. You can now provide Full Control Internet with settings under that logon name.

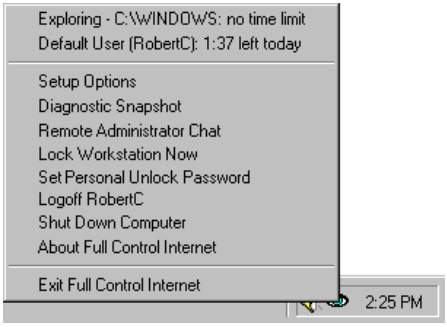
A "back door" way to enable the logon screen is to delete the *.PWL (Windows password list) file saved under a user's name. Use Explorer to search for PWL files, and delete the ones named for the necessary users. The next time that username is given at logon, Windows will show its logon screen. At that point you can tell Windows to keep showing that screen at logon. Note, though, that other kinds of passwords are stored in PWL files, for example those for Dial-Up Networking. These other passwords will have to be entered again.

When you are all set up, you'll find that it's fast and easy to log on as another user. Click the Start button, then choose *Log Off*. (In some versions of Windows, choose *Shut Down*, then select "Close all programs and log on as a different user.") If this Start option has been disabled by Full Control Internet, you can use the password-protected Logoff option on the  Full Control Internet tray icon next to the clock on the taskbar. Click the tray icon to display its popup menu. If the Start button's *Shut Down* option hasn't been disabled, for convenience no password is required to use the tray icon Logoff option.

Chapter 2

A Tour Of Full Control Internet

Taskbar Tray Icon



While Full Control Internet is running, the Taskbar can show a Full Control Internet icon in the "tray" area next to the clock. This icon can be hidden if desired.

Full Control Internet can also hide the entire Taskbar or lock all the tray icons. If you do this, Full Control Internet's tray icon is not available, so to enter Setup Mode you'll need to use the hotkey or the Reset Mode option.

Clicking on the tray icon pops up a menu. The top lines in the menu show the current program and user time limits. Below that are configurable menu options. Management options can be password-protected. Each line in this menu is described below.

Current program name and time limit: This is the name and time limit control for the program which was active at the moment the tray icon was clicked. Only managed programs can have time limits. Choosing this item closes the menu, but has no other effect.

Current user name and time limit: This is the name and time limit control (if any) for the current logged-on user. Choosing this item closes the menu, but has no other effect.

Setup Options: Choosing this option displays the Configuration Screen. This is how you get into Setup Mode. The setup password is required.

Diagnostic Snapshot: This is added to the popup menu if you have checked the Access tab box "Show Diagnostic Snapshot option on tray icon menu." The user can click on this line to generate and display a Diagnostic Snapshot. This can be a very useful tool for remote troubleshooting.

Remote Administrator Chat: If the administrator has allowed this item to be

displayed, the user can click on it to initiate a two-way Realtime Chat conversation with the Remote Administration Manager, in which text typed by one party is immediately displayed to the other party.

Lock Workstation Now: Use this to lock the workstation, for example if the user needs to walk away from the computer temporarily. When locked, currently running applications are minimized, and new applications are closed. Full Control Internet will display a screen in which the user can give the workstation-unlock password, as well as other end-of-session options set on the Security tab. If a *Personal Unlock Password* (see below) has been set for this user on this computer, that is the tested password. Otherwise the group default workstation-unlock password is tested. This is set up on the Time Control tab.

To use this feature, there must be a workstation-unlock password on the Time Control tab, and the administrator must check the box on the Security tab to *Allow workstation unlock with password*.

Full Control Internet supports Identix biometric fingerprint validation. If the Biometric Validation box is checked on the Setup tab, an enrolled fingerprint must also be provided to unlock the session. If Identix fingerprint validation is not installed, checking this box has no effect.

Set Personal Unlock Password: Initially, the workstation unlock password is the group default workstation unlock password as set up on the Time Control tab. However, this user, on this computer, can set a different password. It is valid only on the one computer where it is entered, and only when that user is logged in. To set a new personal password, give the previous password. If there is no previous password, give the group's default password. As usual, the setup password can be used here too, if necessary.

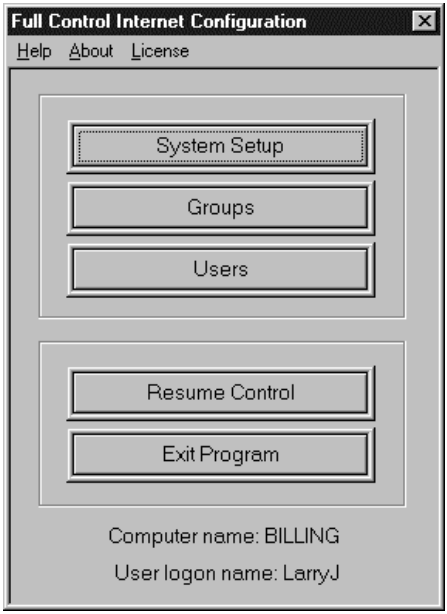
Logoff Current User: If this item is chosen, the logoff password is required, or the setup password if no logoff password has been specified. For convenience, no password is required if the Start button's *Shut Down* command has not been disabled.

Shut Down Computer: If this item is chosen, the shutdown password is required, or the setup password if no shutdown password has been specified. For convenience, no password is required if the Start button's *Shut Down* command has not been disabled.

About Full Control Internet: This displays the About box with version and contact information. This entry is not password-protected.

Exit Full Control Internet: Choosing this option will exit from Full Control Internet. The setup password is required.

The Configuration Screen



This configuration screen is displayed when you click on the Full Control Internet tray icon (next to the clock on the taskbar) and choose *Setup Options* from the popup menu. If the tray icon is hidden, type the designated hotkey or run Full Control Internet's companion Reset program to access the setup options. The setup password is required. Full Control Internet then goes into its Setup Mode in which security checks are suspended. This makes it easier for the administrator to configure the system. To return the system to its previous security mode, choose Resume Control.

A similar screen is displayed when you choose the *Full Control Internet Clone* option from the *Clones* menu of the Remote Administration Manager. This option invokes Administration Manager Setup Mode which allows you to set up a clone file from the Administration Manager, then distribute its settings to all your computers. If started in this way, this configuration screen includes buttons to import or export a clone file.

Help: The information in the Help system is designed for administrators, not casual users.

About: Full Control Internet version and other information.

License: This displays the actual running file's name, and a license code used for validation purposes. There is also an option to "un-license" this computer, which is useful if you need to re-enter the license number or enter a new number. In the pre-purchase evaluation version, there is no license so this displays "How To Order" information. If this computer connects to the Remote Administration Manager, its licensing information can be obtained from there. That is, if you enter in the Remote Administration Manager your license number(s), the Remote Administration Manager will distribute licensing information to the connected computers that it oversees.

System Setup: This displays the System Setup screen. This dialog has five tabs: *Setup, Security*, *Event Log*, *Remote Management* and *Rollback.*

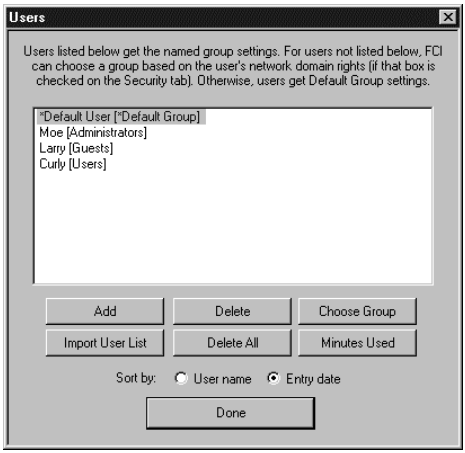
Groups: This displays the Groups screen. After choosing an existing group or creating a new one, the Group Setup screen is displayed, allowing that group's settings to be modified. This screen has seven tabs: *Access, Managed Programs, Interface, Input Control, Time Control, Window Control,* and *File Control.*

Users: This displays the Users screen. This screen lists all users that Full Control Internet knows about, and the Group settings to be applied when that user logs on. For users not listed, Full Control Internet can choose a group based on the user's network domain rights (if that box is checked on the Security tab). Otherwise, users get Default Group settings.

Resume Control: This exits from Setup Mode and puts into place the settings defined in the current user's Group.

Exit Program: This closes Full Control Internet and clears all its access controls.

User Setup Screen



This screen lets you add or delete users, move them into groups, or change the amount of time they have available.

The names shown in this list are the same names which the users type in at the regular Windows logon screen. If the name given at the Windows logon screen matches a name on the Users list, Full Control Internet uses the settings you have given for that user's group. For users not explicitly listed, Full Control Internet can select the highest-numbered group in which that user has network domain rights, or it can pick a group based on an environment variable (both of these options are available on the Security tab). If no group is specified in any of these ways, the user gets Default Group settings.

Full Control Internet can perform logon validation in a number of ways. One way denies access to any user not named on the Users list. If that validation option isn't being used, and no name matches or the user cancels out of the Windows logon screen, Full Control Internet uses its Default Group settings. The Default User settings can be modified, but they cannot be deleted.

This screen also shows what group this user is a member of.

Add: Add one new user at a time.

Delete: Deletes one or more selected users.

Choose Group: Moves one or more selected users to another group.

Import User List: Add multiple users from a plain-text file. The delimiter between user names can be a comma, a tab, a double-quote, a newline, or any combination of these. Multiple delimiters together are treated as a single delimiter, for example the quote-comma-quote between items in a CSV (comma separated values) list. New users are placed initially in the Default Group.

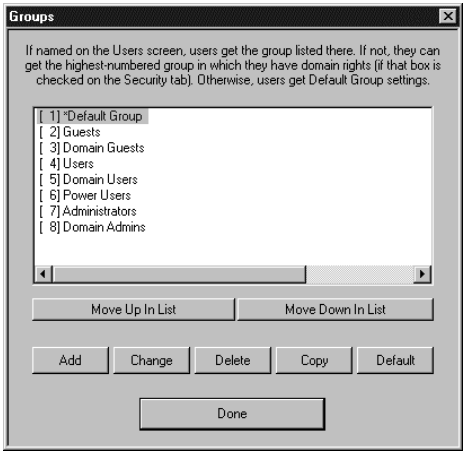
Delete All: Delete every user on the list. A consistency check is performed to ensure that everything stays accessible through this process. It slows down the deletion process, but the safety is worth the speed penalty.

Minutes Used: Update the current minutes used for this user.

Sort by: The list can be displayed alphabetically by user name, or in entry-date

order. Sorting by entry date can be handy. Let's say you import a list of users from a file, and you want them all to be added to the Power Users group. Click the radio button to sort by entry date. All the new users will sorted to the bottom of the list, making it easy to select them all. Click the Choose Group button to select the desired group and you're done.

Groups Setup Screen



The Groups screen is displayed by clicking the Groups button on the menu. A group is a set of settings. You set up a group's settings as you prefer, then (optionally) on the Users screen you assign users to a group. When that user logs on, the group's settings are put into effect. For users not explicitly listed on the Users screen, Full Control Internet can select the highest-numbered group in which that user has domain rights (if that box is checked on the Security tab). Or it can pick a group based on an environment variable. If no group is specified in any of these ways, the user gets Default Group settings.

With the Groups screen, administrators can add or modify a group. Select the desired group, then click Add, Change, Delete, Copy, or Default. Each of these buttons is described below. When you are finished using this screen, click Done.

The functions available on the Groups screen are as follows:

Group Numbers / Move Up / Move Down: For users not explicitly listed on the Users screen, Full Control Internet can select a group based on the user's network domain rights (if that box is checked on the Security tab). It selects the highest-numbered group in which that user has domain rights. Or it can pick a group based on an environment variable (if that box is checked on the Security tab). If no group is specified in any of these ways, the user gets Default Group settings.

Use the *Move Up* and *Move Down* buttons to change a group's number. The group number is used when someone logs on whose name is not explicitly listed on the Users screen, and the *network domain rights* box is checked on the Security tab. Full Control Internet will query the NT/2000/XP Domain Controller for a list of network groups in which this user has rights. These domain-group names are compared to the names of the Full Control Internet groups. The user is given the settings of the Full Control Internet group with the highest-numbered matching name.

For example, if a user is not listed on the Users screen but has been given domain rights on the NT-based network, Full Control Internet first gets the user's logon name. The network domain rights box has been checked, so Full Control Internet queries the NT-based network and discovers that this user is in the Domain Users and the Domain Admins groups. On the Groups screen, the

Domain Users group is number 5 and the Domain Admins group is number 8, so this user is given the Full Control Internet settings associated with the Domain Admins group. Note that if the network domain rights box is not checked, Full Control Internet will not query the Domain Controller for this information. In that case, a user who is not listed on the Users screen gets Default Group settings.

Add: Add a new group. It will be created with default settings. The new group's setup screen will be displayed.

Change: Change the settings for an existing group. That group's setup screen will be displayed. You can also double-click the name on the list.

Delete: Delete a group from the list.

Copy: Make a copy of one group's settings. The name of the new group will be "Copy of <the original name>". The new group's setup screen will be displayed, allowing you to change this name or any other settings.

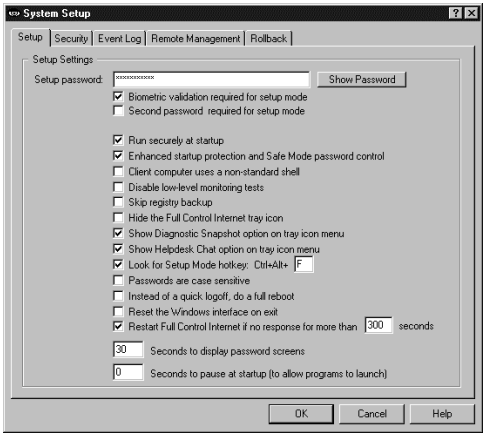
Default: Copy a group's settings into the Default Group's slot. Unlike the Copy button, a new group is not created. Clicking the Default button simply copies the selected group's setting to the Default Group.

System Setup Dialog

To set up systemwide options, use the System Setup tabbed dialog. This screen has five tabs:

Setup: systemwide preference options
Security: global security options
Event Log: audit trail usage and tracking options
Remote Management: network-based remote configuration control
Rollback: save and restore important system configuration files

Setup Tab



This tab of the System Setup screen is where you give the setup password, boot-time options, and other systemwide preferences.

Setup Password: This is the administrator password. Like all Full Control Internet passwords, it is initially displayed with asterisks. Use the Show Password button to see the password. If a licensed copy of Full Control Internet is installed on the computer running the Remote Administration Manager, the Setup password is required to make changes through the Remote Administration Manager.

Biometric validation required: Full Control Internet supports Identix biometric fingerprint validation. If this box is checked, an enrolled fingerprint must be provided to use Setup Mode. If Identix fingerprint validation is not installed, checking this box has no effect.

Second password required: Check this box to require that two separate passwords be given to enter Setup Mode, change settings, or perform certain other administrator overrides. The "Setup password" control at the top of this screen is replaced with two password protected buttons, each of which changes one administrator password. There is no "show password" option for these two passwords. Instead, asterisks are always displayed for their characters. If a licensed copy is installed on the computer running the Administration Manager, both Setup passwords are required to make changes through the Administration Manager.

Run securely at startup: This will set up the computer so Full Control Internet is

run whenever Windows starts. Unlike a shortcut in the Startup folder, this method cannot be bypassed by pressing the Shift key when Windows comes up.

Enhanced startup protection and Safe Mode password control: Checking this box will set Full Control Internet to validate the user's logon name immediately when they type it in, rather than after the Windows desktop appears. It will also password-protect Safe Mode, a special mode built in to Windows to allow for error recovery. In Safe Mode, many protections are disabled by Windows. If you check this box, Full Control Internet will treat Safe Mode as an extension of its own administrators-only Setup Mode by requesting its setup password before allowing access to Safe Mode.

Non-standard shell: Windows computers almost always use the standard system shell, which displays the familiar Start button, taskbar, desktop icons, etc. Full Control Internet can also be used with non-standard shells. Some logon-related options are grayed out and unavailable when using a non-standard shell, since their handling of the startup and logon process varies widely. You can still check the Full Control Internet option to "run securely at startup." The shell (standard or non-standard) then looks for this information at startup so it knows what to launch.

Disable low-level monitoring: Full Control Internet monitors system activity at all levels. If its low-level monitoring conflicts with any other installed software, it can be disabled here. Affected features include File Control, locking the CD drive door, and disabling Ctrl+Alt+Del. Also, control of the Windows keys is not as strong.

Skip registry backup: At startup Full Control Internet backs up the current Registry files to *userfci.bds* and *sysfci.bds* (and *classfci.bds* in Windows ME) in your Windows directory. This safety measure provides a useful fallback, allowing you to reset your system as it was prior to the current session. (To do this, restart in DOS and copy these backup files over top of *user.dat* and *system.dat* (and *classes.dat* in Windows ME) in your Windows directory.) However, saving the backup files takes a few seconds at launch. Check this box if you prefer a faster launch sequence at the expense of a bit of safety.

Hide the Full Control Internet tray icon: With the tray icon hidden, there is no on-screen indication that Full Control Internet is running. However, there is also no access to the tray icon's popup menu, so to configure Full Control Internet when the tray icon is hidden press the hotkey (see below) or run the Full Control Internet Reset program (reset.exe), or start Full Control Internet from a command prompt with the /reset parameter.

Show Diagnostic Snapshot Option: If you check this box, a "Diagnostic Snapshot" item is added to the popup tray icon menu. The user can click on this line to generate and display a Diagnostic Snapshot. This can be a very useful tool for remote troubleshooting.

Show Remote Administrator Chat option: If you check this box, a "Remote

Administrator Chat" item is added to the popup tray icon menu. The user can click on this line to begin a conversation with the administrator sitting at the Remote Administration Manager.

Look for Setup Mode hotkey: If this box is checked, Full Control Internet will ask for the Setup Mode password when the designated hotkey is pressed. If the password is given, Full Control Internet will go into Setup Mode. You can set the hotkey as any letter from A to Z. Invoke the hotkey by simultaneously pressing the Control key, the Alt key, and your letter. The hotkey is a good way to go into Setup Mode when you have set up Full Control Internet to hide the tray icon or the entire taskbar.

Passwords are case sensitive: Should passwords be case sensitive? This setting will affect all managed program passwords and the Setup password.

Instead of a quick logoff, do a full reboot: To log on as a new user, some computers or networks require a full reboot instead of the quick "log on as a different user" procedure usually used by Windows. Check this box to do so.

Reset the Windows interface: Microsoft has documented a bug in Windows 98 (and NT using the IE shell) which prevents it from re-reading certain settings from the registry when they are changed. Instead, Windows 98 uses cached settings held in memory. These settings are only updated at the next logoff or restart. Checking this box forces Windows to re-read the new settings instead of using the old (cached) settings. This is not needed under Windows 95, Windows 2000, or Windows XP, which correctly reads these settings from their original location.

Here is how to see if your computers can benefit from this "reset" setting. Log on as a user name which invokes a Group in which some of the Start menu items should be missing, for example Run, Find, and Logoff. While not in Setup Mode, click on the Start button and look for these items. If they are still there, try to click on them -- even if these menu entries are visible they should be disabled.

Now go into Setup Mode and then click on the Start button again. Did the missing (or disabled) items come back (or become usable) when you entered Setup Mode? If they did not come back when you entered Setup Mode, check this box, click OK to save the settings, exit normally from Full Control Internet, restart your computer, and try the test again. If the Start menu items are now available when you enter Setup Mode, leave the box checked. Note: on some computers the tray icons may vanish when doing a reset. If this is an issue for you, don't use this feature.

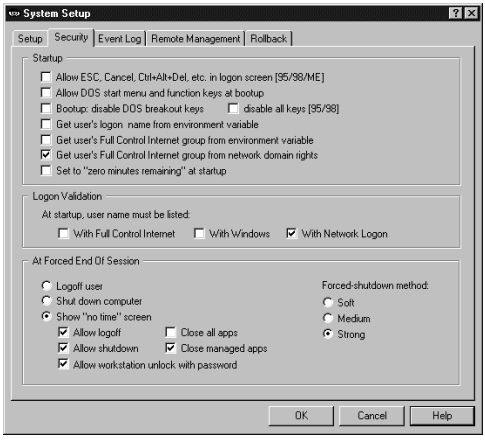
Restart Full Control Internet if no response: Full Control Internet includes components that make sure in various ways that the program continues to run normally. One of these components can provide "program is hung" protection. If you check this box, this component listens for messages from Full Control Internet to ensure that everything is still running normally. If you want to use this component, indicate here how many seconds it should wait before concluding that Full Control Internet is not responding. We recommend setting this to at

least 180 seconds to allow for certain kinds of applications which occasionally monopolize the computer briefly. While the computer is monopolized in this way, Full Control Internet can't send these "I'm OK" messages, so be sure the time is long enough to bridge any such periods.

Seconds to display password screens: Indicate how long you want a password screen to stay visible before it times out.

Seconds to pause at startup: This pause applies only if Full Control Internet is run automatically at startup. It's here to accommodate other programs which are run at startup, which require complete access to the computer as they launch. If you give a pause here, Full Control Internet will wait that many seconds before activating its security oversight.

Security Tab



Use this tab of the System Setup screen to choose boot-time options, validation preferences, and other systemwide security settings.

Allow ESC, Cancel, Ctrl+Alt+Del, etc. in logon screen [95/98/ME]: Unless this box is checked, Full Control Internet disables the Escape key and Cancel button in logon data-entry screens. It also prevents any other bypass of the logon process, such as pressing Ctrl+Alt+Del to bring up the Close Programs box or Ctrl+Esc to bring up the Task Manager. If you are doing your logon validation through a Novell or NT/2000/XP network, you should check the "With Network Logon" box, and you should probably check this box to allow the ESC key, Cancel button, etc. On stand-alone computers, or on peer-to-peer networks, you'll generally want to un-check this box, thus providing protection. Generally, you will want to un-check this box (to deny use of ESC, Cancel, etc.) if you are doing logon validation "With Full Control Internet" or "With Windows", or if you haven't checked any of the three logon validation boxes. This option is ignored under NT/2000/XP, which does not allow invalid logons.

Allow DOS start menu and function keys at bootup: This option is primarily for Windows 95/98, but also has a useful effect under NT/2000/XP. Under Windows 95/98, it lets you control whether the keyboard and startup menu can be used when the computer starts. At boot time, pressing F4 starts the previous version of DOS, F8 brings up the startup menu providing methods to run bare DOS, "safe mode," etc. To enhance security, uncheck this option so Full Control

Internet will disable access to these and the other boot-time keys. However, even when these keys are disabled, if Windows detects an abnormal bootup it will display the startup menu anyway. This could allow the user access to the "backdoor" methods described above. Therefore, using this option also sets a system flag which makes the startup menu more difficult to use: if the menu does indeed appear, its default choice is instantly chosen, then the menu immediately vanishes. Under NT/2000/XP, this option immediately closes the Boot Loader menu by automatically selecting the default choice Therefore, when using this option on dual-boot systems where you always want NT/2000/XP to load, make sure you have set NT/2000/XP as your default operating system in your boot.ini file. This setting is ignored under Windows ME because that operating system cannot boot to DOS.

Bootup: disable DOS breakout keys / disable all keys: In Windows 95/98, DOS programs that run from the autoexec.bat file can create a problem, because users can type Ctrl+C or Ctrl+Break to terminate those programs and gain access to the DOS prompt. While such programs are active, users can also type Ctrl+Alt+Del to restart the computer. To prevent the use of these keys, check the box labeled *disable DOS breakout keys.* Or, if you want to completely disable the keyboard until Windows loads, check the box labeled *disable all keys.* These options will add commands to your autoexec.bat to monitor the keyboard; if the computer has no autoexec.bat, no oversight is necessary so no commands are added.

Usually, Full Control Internet can find your autoexec.bat file just fine, but if your autoexec.bat file is not in the obvious location, you may need to create a BDSAUTOEXEC environment variable, and set it to the full path and filename of your autoexec.bat (for example BDSAUTOEXEC=e:\buried\autoexec.bat). This will tell Full Control Internet where to find your autoexec.bat file.

These options are grayed-out if you have allowed the DOS start menu and function keys at bootup (the checkbox directly above this one). They are ignored in NT/2000/XP where DOS does not load before Windows.

Get user's logon name from environment variable: At startup, Full Control Internet looks for the logon name of the current user in the Windows-standard way. However, some older Novell networks are not fully Windows-aware and do not place the user's logon name in the standard place. To address this, Full Control Internet can get the user name from the FULLCTL environment variable instead. Of course, you will need to modify your logon script to place the current user name into this environment variable at logon.

Get user's FCI group from environment variable: If a user's logon name is not explicitly listed on the Users screen, and this box is checked, Full Control Internet will look for the BDSGRPENVAR environment variable to see which group's settings should be used for this session. For example, at logon you might use your login script to set the BDSGRPENVAR to the name of this user's Novell network group. If Full Control Internet has a group of the same name it will use that group's settings during this session.

Get user's FCI group from network domain rights: If a user's logon name is not explicitly listed on the Users screen, and this box is checked, Full Control Internet will query the NT/2000/XP Domain Controller for a list of network groups in which this user has rights. These domain-group names are compared to the names of the Full Control Internet groups as listed on the Groups screen. Full Control Internet's groups are numbered; the user is given the settings of the group with the highest-numbered matching name.

If the *network domain rights* box is not checked, a user who is not listed on the Users screen gets Default Group settings.

Check this box if your computers are on a domain-based network. That way, you need only enter your users in the usual Microsoft way -- you don't need to also list them with Full Control Internet. When you change or delete a user in your domain, that change is immediately reflected in Full Control Internet.

What if this box is checked for a non-networked (or peer-to-peer networked) computer? The computer tries to find a Domain Controller, it can't find one, no domain groups match, so the user gets the Default Group settings. It takes a few seconds for a 95/98/ME computer to figure out it's not on a domain, and during this period the computer locks up. This is harmless; it unlocks as soon as the network query is complete, and it is only an issue on a 95/98/ME computer. An NT/2000/XP computer can figure this out instantly, so there is no lockup.

If you must have this box checked on non-networked computers (for example, so you can use just one clone file for all your computers), one way to avoid the network query (and the lockup) is to configure the individual computer to skip this step. NT/2000/XP computers never lock up but it could be handy on your non-networked 95/98/ME computers. To do this, set the environment variable:

BDSGRPDOMAIN=FALSE

Doing this on your non-networked 95/98/ME computers allows you the simplicity of using the same clone file for all your computers regardless of their network/domain situation.

Set to "zero minutes remaining" at startup: Check this box to have "zero time remaining" at startup. This is useful if the time on a computer is sent in as needed using the Remote Administration Manager or another system which can send time to Full Control Internet from the outside, for example a bill acceptor or smart-card reader. You can turn the computer on at the start of the day, yet no one can use it until time is sent to the computer externally.

Logon Validation: When Full Control Internet starts, it can examine the Windows logon name as given by the user at the regular Windows logon screen when Windows started. If an invalid name is detected, Full Control Internet will logoff Windows. This is a useful feature if you don't have centralized network-based logon validation (through Netware, NT/2000/XP, etc) or if you prefer

validation that will continue to work if your server or network goes down.

If you have checked *Enhanced startup protection and Safe Mode password control o*n the Setup tab, the validation is tested as soon as the user tries to log on, that is, before the Windows desktop appears. If you haven't checked this box, the logon validation is tested after the desktop appears, when Full Control Internet starts.

There are three ways that Full Control Internet can validate the logon name. You can use one or more of these tests.

With Full Control Internet: To log on, the user must give a logon name which is listed on the Users screen. If this is checked and the user gives an unlisted name, Full Control Internet logs off Windows. If the user hits Escape or otherwise cancels the Windows logon process, no name is given so (again) Full Control Internet logs off Windows.

With Windows: To log on, the user must give a name which is known to Windows as a valid logon name, that is, a name that has previously been set up through the Windows logon mechanism. If this is checked and the user name was set up less than 30 minutes ago, or if the user hits Escape or otherwise cancels the Windows logon process, Full Control Internet logs off Windows. All valid names are listed in the *system.ini* file under the [Password Lists] section. This section shows the password-list file associated with each valid logon name, so to make a name invalid remove the name's line from this section and delete its password file. This option is ignored under NT/2000/XP , which does not allow invalid logons.

With Network Logon: If you have a network with a Netware or NT/2000/XP server, check this box to ensure that users cannot ever get past the Windows logon unless they are validated by your server. This is especially useful on a Windows 95/98/ME computer, because on such machines even if the logon fails Windows may still allow access to the local computer. This option will work with NT/2000/XP server validation, and many recent versions of Netware.

If either of the first two boxes is checked, it's probably a good idea to set Full Control Internet so it does not let the user press Escape at logon. If the third box is checked, it is a good idea to allow Escape at logon, as many network logon programs make use of the Escape key. Full Control Internet ensures that this is done in a safe way.

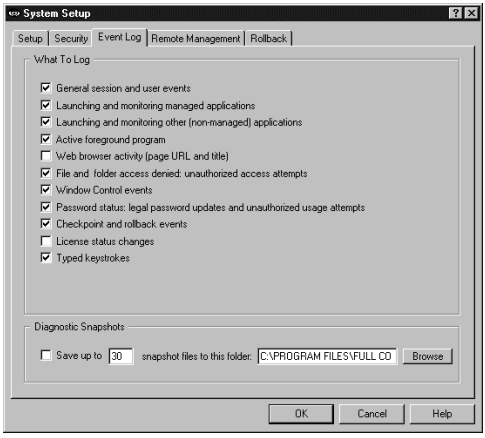
At Forced End Of Session: Full Control Internet can force a session to end for a number of reasons: inactivity timeout, user time limits, blockout periods, or a remote command sent by the Administration Manager. What should happen when this occurs? Choose whether to logoff that user, shut down the computer, or display a "no time left" screen. If the "no time left" screen option is chosen, and the computer continues to run (useful to allow the user to add time to this session, or to send more time with the Administration Manager), should Full Control Internet close all managed applications? Or close all applications,

managed or not? Should the "no time left" screen include buttons which allow the user to log off, shut down, or unlock the workstation? Set these options here.

What if you choose the shutdown or logoff option, and you set Full Control Internet to always "run securely at startup" (see above), and your system runs out of time? That is, if Full Control Internet shuts down or logs off as soon as you start the computer, how do you change the time settings? Not to worry. If at launch there is zero time available, and Full Control Internet is set to logoff or shut down, it will pause an additional 20 seconds specifically to provide an opportunity to get into setup mode. Click on the tray icon to display Full Control Internet's popup menu, then choose the menu's Setup Mode option. If the tray icon is hidden, use the hotkey or run Full Control Internet's companion Reset program to access the setup options. The password screen will appear. While the tray icon's popup menu or the password screen is displayed, the logoff or shutdown procedure will be paused. And if you give the setup password and go into setup mode, the logoff or shutdown procedure will be stopped, leaving you free to make your configuration changes.

Forced-shutdown method: There are three ways that Full Control Internet can shut down the computer. The most secure method is labeled here as *Strong*. It forces other programs to exit and guarantees a secure shutdown. However, some computers hang at shutdown with the *Strong* method. If yours is one of them, try the *Medium* or *Soft* methods. In the *Medium* method, Full Control Internet "requests" that other programs shut down at exit; if any other program refuses, the computer does not shut down. The *Soft* method asks Windows to do the shutdown; Full Control Internet then steps back and waits for Windows to handle it all.

Event Log Tab



Use this tab to indicate the events to log. Events are sent to the Remote Administration Manager for logging. If there is no Internet connection to the Remote Administration Manager, or the connection is temporarily unavailable, logging records are temporarily cached locally. Full Control Internet keeps checking for an available connection to its Remote Administration Manager and the cached log records are sent as soon as this is again available.

What To Log: Check the events you want logged. You can log these events:

General session and user events: Each time Full Control Internet started or shut down, entered or exited Setup Mode, or encountered certain error conditions.

Launching and monitoring managed applications: Each time a managed program is started or terminated. Termination could be forced or voluntary.

Launching and monitoring other (non-managed) applications: Each time a non-managed program is started or terminated. Termination could be forced or voluntary.

Active foreground program: Checking this box will log the program name, window title and amount of time of every window the user actually worked in, so you can see where they actually spent their time. Foreground times of Web browser windows will be logged if the *Web browser activity* box (below) is also checked.

Web browser activity: Each time a browser accesses a webpage. Logged information includes the title, URL and amount of time on that page. The amount of time during which the browser window was the active foreground window will be logged if the *Active foreground program* box is also checked.

File and folder access denied: Check this box if you use Full Control Internet's File Control feature, or the Allowed Folders option of the Window Control feature. When using either of these features to limit file access, some programs (and users!) may still try to manipulate read-only files, write to invisible directories, etc. Full Control Internet can log these invalid access attempts. A list of these events can be very useful. For example, if a program doesn't run correctly, perhaps it needs access to a protected file. The access-denied reports will show this readily.

Window Control events: When the Window Control discovers a window it needs to manage, should that be logged? Also, check this box to send Window Control Alerts to the Remote Administration Manager. Alerts can pop up a message, play a sound, or send an email to tell the administrator about the condition.

Password status: Check this box to have Full Control Internet log each time a password was changed, and each attempt to use an invalid password.

Checkpoint and rollback events: Log when a Full Control Internet saves a checkpoint or rolls back to a previously saved checkpoint.

License status changes: Check this box to have Full Control Internet log each time the computer is licensed or unlicensed, whether this is done locally or by the Remote Administration Manager.

Typed keystrokes: Check this box to have Full Control Internet log all keys typed by the user into any Windows program.

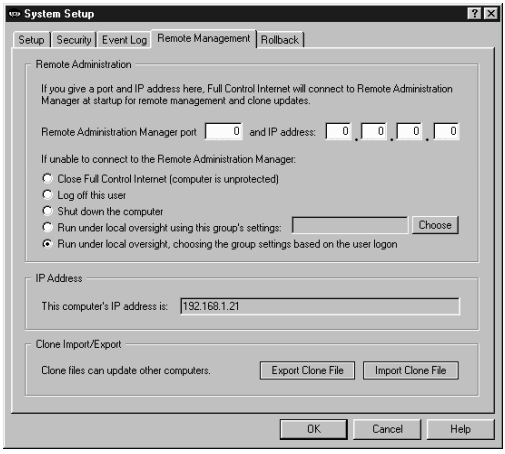
Diagnostic Snapshots: Full Control Internet can take "snapshots" listing all running applications in great detail. For each running process, they show the windows opened, the primary file's date and size, the product name, version, company, copyright information, and description, the threads created, any other modules (files) loaded, and the amount of memory used. It lists every running program and system component, even hidden programs that won't show up on the Close Programs (Ctrl+Alt+Del) screen.

If checked, Full Control Internet will create a snapshot file about once a minute. It will save as many snapshot files as you want, up to 99 files. If the maximum number of files have already been created, it will delete the oldest file to make room for a new one.

This is a useful tool for diagnosing a computer that is behaving oddly, or crashing for no apparent reason. When the odd symptoms appear or when the computer crashes you'll have a minute-by-minute record of every application's state leading up to the problem. Snapshots are saved as plain-text files so they can be accessed even if Windows won't run.

Diagnostic snapshots can also be requested and viewed from the Remote Administration Manager.

Remote Management Tab



This tab lets you set up features which provide network-based remote configuration and application control.

Remote Administration: List the port and IP address of the Remote Administration Manager overseeing this computer. The easiest way to get this port and IP address is from the Remote Administration Manager's Communications Ports And IP Address dialog.

Here you also can indicate how you want Full Control Internet to behave if it is unable to connect to the Remote Administration Manager. It can simply close Full Control Internet (leaving the computer unprotected), logoff, shut down, or use its previous settings to run under local oversight. Under local oversight, it can (as usual) choose the group based on the user who has logged on, or for added security it can use the settings of a specific group, perhaps a group with very restrictive settings. If it runs under local oversight it will periodically attempt to reconnect with the Remote Administration Manager. When it does, it will upload its log records and otherwise catch itself up with the central server.

IP Address: For convenience, this computer's IP address is listed here. If you use network address translation, this is the local masqueraded address, not an address visible to the Internet at large.

Export Clone File: Clicking this button sets up to create a clone data file. The file will be created when you click OK to exit from the System Setup screen. By default it is named *clonefci.bds* and is in the Full Control Internet directory. This file contains all the data that defines this computer's configuration, and any display restrictions, per-group settings, or other features you have set up to control which managed programs or groups are controlled on what computers. Cloning is further described in How To Clone A Computer.

Import Clone File: Clicking this button sets up to read a clone data file and update the current computer's configuration. The file will be read when you click OK to exit from the System Setup screen. It's sometimes useful to be able to instantly update the current computer.

Full Control Internet can read Full Control 2 clone files manually via the *Import Clone File* button. The old-style clone's settings will be converted automatically as they are read. We strongly suggest that you study the results to ensure that the automatic conversion meets your needs. After confirming the settings, you can export them as a new Full Control Internet clone file which can be automatically distributed in any of the usual ways.

Per-user workstation unlock passwords (set from the Tray Icon) are valid only on the one computer where they are entered. They are not cloned, and do not carry over when a new clone is read.

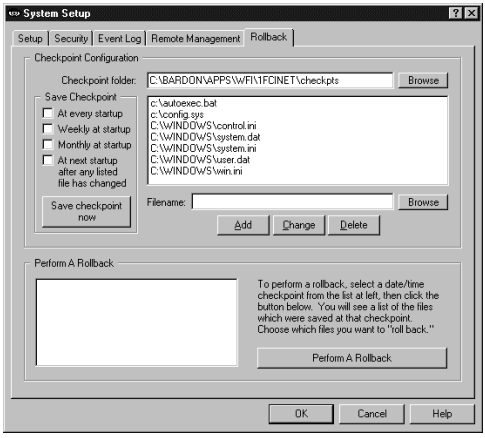
Administration Manager note: Clone configuration files can be created and managed from the Remote Administration Manager. When using the Remote Management tab from the Administration Manager, the Import and Export buttons are disabled, since importing and exporting are done from the main Configuration screen.

Licensing note: If this computer connects to the Remote Administration Manager, its licensing information can be obtained from there. That is, if you list the port and IP address of the Remote Administration Manager that will be overseeing this computer, and if you enter into the Remote Administration Manager your license number(s), the Remote Administration Manager will distribute licensing information to the connected computers that it oversees.

Checkpoint / Rollback Tab

Ever had your system trashed by a misguided user, or a piece of software that changed your Registry or other system files, and left the computer a mess? Ever

think, "if only I could roll back the files to the way they were before?" That's what the Rollback tab is for. Full Control Internet can save system-file checkpoints on your schedule. These checkpoints are available if you need to do a rollback.



Use the top half of the Rollback tab to list the files you want backed up when Full Control Internet saves a checkpoint. Give the checkpoint folder to which they should be saved. When you install Full Control Internet, a starter list is provided, containing typical system files which are often useful to protect. The checkpoint/rollback feature is primarily intended to back up system files, but you can add any file you like to the list. For example, you might want to search your system for *.PWL files (Windows password lists) and add any appropriate ones that turn up. Or consider adding various drivers and other support files.

A checkpoint can be saved automatically at every Full Control Internet startup, or once a week at startup, or every 30 days ("monthly") at startup, or at the first startup after any listed file has been modified, or when you click the Rollback tab's "save checkpoint now" button.

When Full Control Internet "saves a checkpoint" it creates a new subdirectory under the designated checkpoint folder and copies all listed files to it. The files are not compressed or modified. This means that if necessary, you can get to them from DOS and restore them to their original location with DOS commands ... very handy if your computer won't boot Windows! Since the files are saved with their original attribute settings, you may have to use the DOS command ATTRIB so commands like DIR and COPY can see them. For example, the Registry (*.dat) files have the attributes of hidden, system, and read-only, so you'd use the commands ATTRIB -H -S -R USER.DAT and ATTRIB -H -S -R SYSTEM.DAT to make them visible.

To perform a rollback, select a date/time checkpoint from the list in the bottom of this screen, then click the rollback button. You will see a list of the files which were saved at that checkpoint. Choose the files you want to roll back.

Full Control Internet has two ways it can "roll back" a file. It can simply copy the file back to its original location, or it can use a more elaborate file-restore method involving batch files, your autoexec.bat, and a reboot. The second method is useful for system files that cannot be restored while Windows is running. System-type filenames invariably conform to the old DOS 8.3 naming convention, so if a chosen file's filename is bigger than the old DOS 8.3 format, it isn't a system file and Full Control Internet always "rolls it back" by just copying it to its

original location. Files that fit into the old 8.3 format might be system files, so they are examined more closely. Full Control Internet knows about many types of files. For example, it knows that it can simply copy your autoexec.bat and config.sys files, but it needs to use the more elaborate method to restore your Registry files. If it can't tell what to do about a particular file, it asks. Full Control Internet can use either method to restore files under Windows 95/98. Under ME or NT/2000/XP, it uses only the first method, due to the lack of any automated method to temporarily go to DOS. Note that Windows ME and XP have their own built-in rollback mechanisms which may be useful under certain circumstances.

The Remote Administration Manager can tell a networked workstation to save a new checkpoint, or restore a saved checkpoint, by sending a message to that computer.

Perform A Rollback: Select an existing checkpoint, then click the "perform a rollback" button on the Rollback tab of the System Setup screen. On the screen that appears, choose one or more files that you want to "roll back" to the previous version. Click a filename in the list to select it. To de-select a selected file, click its name again.

Group Setup Dialog

Full Control Internet looks at the name of the user currently logged in to Windows or can get the user name from an environment variable. This user can be validated at logon to ensure authorized access. If the logged-on user is listed in a group the group's settings are put in place for that user. For users not listed in a group, Full Control Internet can choose a group based on the user's network domain rights or on an environment variable (both set on the Security tab). Otherwise, users get Default Group settings. Or you can set up Full Control Internet so unknown users are not allowed to log on at all.

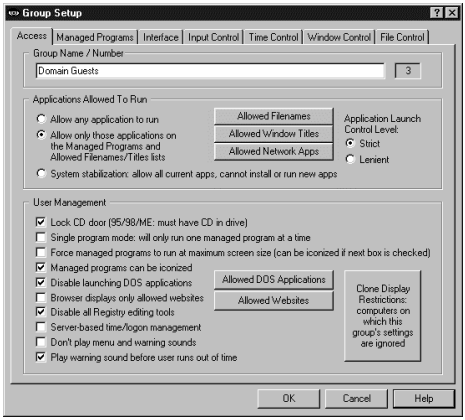
Note that you don't have to tell Windows to save a different configuration for each user. All that is needed is to have Windows display the logon-name screen itself. Full Control Internet will then apply its own settings for that user.

To set up these options, launch the Group Setup screen from the Configuration screen.

The Group Setup screen has seven tabs:

Access: program management, time limits, and user options
Managed Programs: applications with time limits and other controls
Interface: hide desktop icons, drive/network access, wallpaper
Input Control: Start button, keyboard, mouse, and inactivity restrictions
Time Control: timeouts and blockouts
Window Control: close or manipulate any window when it appears
File Control: make files and directories invisible or read-only

Access Tab



This tab lets you set the group name, management options, and ways that programs will and won't run when launched by users who are members of this group.

Group Name / Number: This is the name by which the group is identified. You can rename a group at any time. The Group Number is displayed here for reference. Full Control Internet uses the Group Number if the logged-on user is not listed in a group and you have told Full Control Internet to choose a group based on the user's network domain rights (this is set on the Security tab). The Group Number can be changed on the Groups screen.

Applications Allowed To Run: Full Control Internet can restrict the programs which can be run by members of this group. Applications listed as Managed Programs are always allowed to run, subject to their individual time and password restrictions. But what about non-managed programs? Indicate here how you want them treated.

• If you *Allow any application to run* there are no restrictions on non-managed programs (other than the box just below here, labeled *Disable launching DOS applications*). If allowed, non-managed programs are logged, but no time limits are enforced against them.

• If you *Allow only those applications on the Managed Programs and Allowed Filenames/Titles lists* you can control exactly which non-managed programs can be run. Use the *Allowed Filenames* button to list the full name with the path, or just the file name itself (for example *c:\windows\sol.exe* vs. *sol.exe)*. Listing the full path is more secure; listing just the filename is easier. If you select the Lenient option (see below) you can also list allowed programs by window title on the *Allowed Window Titles* button. Remember to list all applications run automatically at startup, in addition to applications your users can run. If you clone this computer the resulting clone file will include all the allowed filenames and window titles you entered here; the list is transferred with the clonefile to new computers (compare this to the System Stabilization option). Strict/lenient applies when you use this option.

• if you use the *System Stabilization* option, Full Control Internet automatically generates an *Allowed Filenames* list of every program on a visible "letter" drive, including programs on mapped drives. These programs are allowed; new

programs cannot be installed or run. If you clone this computer the resulting clonefile will NOT include all the allowed filenames and window titles you entered here; the list is rebuilt separately on each computer as needed (when first installed, when exiting from Setup Mode, or after the Administration Manager remotely "Runs A Program" and temporarily "Disables security control" while doing so). So, even if your computers are not identical, you can stabilize all your computers with one clonefile (compare this to the previous option). Strict/lenient applies when you use this option. For programs run from a network share, if using Lenient, all such programs are allowed, if using Strict, the only network programs allowed are those you listed on the *Allowed Network Apps* screen.

Launch Control Level: If you control the applications allowed to run, when the user tries to launch any other program, Full Control Internet will not let them run. In doing so, should Full Control Internet be strict or lenient about such programs?

Strict: This is the tightest possible control. The only programs that can be run by this user are Full Control Internet managed programs and those listed under *Allowed Filenames* or *Allowed Network Apps*. Full Control Internet sets certain low-level Windows options when this user logs on, and clears them when Full Control Internet exits at this user's logoff. But if for any reason Full Control Internet exits abnormally, the Strict low-level "don't run" settings will still be in place, and almost nothing on your computer will run. If this happens, Full Control Internet provides a number of recovery options.

Lenient: This option isn't as strong as Strict method, but it does not create any low-level restrictions. Instead, Full Control Internet itself looks at all new top-level windows. A window owned by another window is ignored (for example a Save As dialog). If the window's title doesn't match any entry on the *Allowed Window Titles* list, or any filenames on the *Allowed Filenames* list, the window is terminated. Use the *Allowed Window Titles* button to list the titles of windows that are allowed to run. To add a titlebar name, give the exact (case sensitive) title bar text of allowed windows. You can use * and ? wildcards freely when giving the window title. Full Control Internet will also allow any window from a program on the *Allowed Filenames* list. If you use the *System Stabilization* option all programs run from UNC network shared folders are allowed.

How To Get Full Control Internet To Totally Ignore A Program: There's another use for the *Allowed Filenames* and *Allowed Window Titles* lists. When you add an item, if you check the "treat as a system component" box the program will be completely ignored by Full Control Internet, as if it were a system component such as the Taskbar or desktop. Sometimes it’s useful to treat certain programs this way, for example a fax monitor, proxy software, antivirus application, or other system-level program. To leave such a program completely undisturbed by Full Control Internet, list it as an Allowed Application, and check the “system component” box on the add-entry screen. You’ll generally list it by filename, but you can also list it by window title.

User Management: These settings let you customize the way in which Full Control Internet runs programs.

Lock CD drive door: Check this box to help prevent valuable CDs from walking away from the computer. In Windows 95/98/ME, the drive locks when the CD is inserted. In Windows NT/2000/XP the door is locked whether or not a CD is present.

Single program mode: If checked, when the user launches a managed program, any other currently-running managed program will be forcibly terminated.

Maximum screen size: Check this box to ask managed programs to run in a maximized window that covers the entire screen. Most programs comply with this request. This can help discourage the temptation to launch other programs before exiting from this one.

Can be iconized: Check this box to allow managed programs to be minimized to the taskbar.

> *The difference between the "maximized" and "iconized" options is this: the "force maximize" option forces managed programs to run fullscreen at all times. The "can iconize" option allows programs to be minimized (become iconic). A fullscreen program can be minimized, if the "can iconize" box is checked.*

Disable launching DOS applications: Check this box if you do not want to allow members of this group to run any DOS programs. However, to let members of this group run particular DOS applications when DOS programs are disabled, click the *Allowed DOS Applications* button and add the full-path filename of each "exception" to the list, then set up those DOS applications to run through the companion fcRunApp program.

Browser displays only allowed websites: If you check this box and a browser displays a webpage that isn't on the allowed-websites list, the browser will be closed. Click the *Allowed Websites* button to add to this list. You can add URLs or website titles. Full Control Internet tries to match your text against the URL displayed in the browser's URL line, and also against the titlebar text at the top of the browser's window. If either one matches, that website is allowed. Wildcard characters can be used freely when you give your allowed websites. In particular, asterisks are very useful. For example, *bardon* will allow titles like "Bardon Data Systems Website" as well as URLs like "http://www.bardon.com/fullctl.htm/". Another example is *microsoft.com/technet* which will match the URL of a particular section of Microsoft's website. Notice how the asterisks are used at each end of these examples. Asterisks match any number of characters, so they will allow any text before "your" text, and any text after it. You can freely include any number of wildcards (asterisks and question-marks) anywhere in your exception, even in the middle. Also, it's not case-sensitive. Notice how exceptions with dots and slashes ("*www.bardon.com/fullctl.htm*") will generally match only URLs, and exceptions with embedded spaces ("*Bardon Data*") will generally match only titles. This option works with Netscape or Internet Explorer version 3 or later.

Disable all Registry editing tools: With this box checked, the user cannot run regedit.exe, regedt32.exe, and similar registry editing tools.

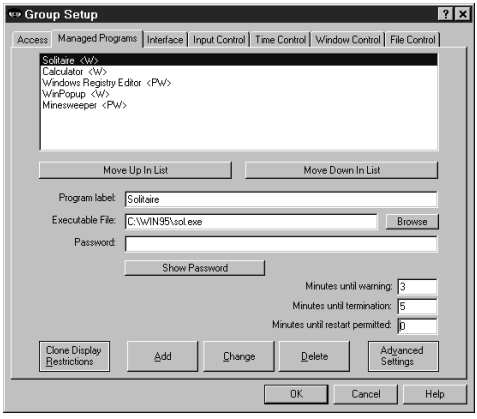
Server-based time/logon management: If this box is checked, the Administration Manager will save that user's time and restore it to the remote computer when that user logs on next time. For example, let's say a group gives its users 60 minutes per day, and a member of that group is active for 20 minutes at Computer 1, then logs off. When that user logs on to Computer 2 under the same name, the Administration Manager will reset Computer 2 so it has only 40 minutes remaining. The Administration Manager will also make sure that this user can only log on to one computer at a time. The Administration Manager must be running to coordinate these features.

Don't play menu and warning sounds: Check this box to disable the "click" menu and button sound, and all other sounds generated by Full Control Internet.

Play warning sound: Do you want Full Control Internet to play a warning sound before this user runs out of time? The sound is played at the same time the user-time warning screen pops up. If no managed program is running at the warning time, no warning sound is played.

Clone Display Restrictions: Will you be cloning this computer's Full Control Internet setup? If so, you may want to click this button and use the Display Restrictions screen to list by name the computers on which this group's settings should be considered at logon. Or if it's easier, list the computers on which it should not be considered. Or give a file name; if the file is present (and optionally, if the file's contents match), the managed program will be monitored. See the Display Restrictions page for more information on this.

Managed Programs Tab



"Managed programs" are applications set up on this group's Managed Programs tab. They can have a time limit, password, and other access configuration options. You can list any Windows application. However, a DOS application cannot be listed as a managed program. The companion fcRunApp utility provides a managed way to run DOS programs.

Full Control Internet monitors all system activity. As the user runs programs (from the Start button, Explorer, or in any other way) Full Control Internet looks at them. If any

application is on the managed programs list, Full Control Internet applies its associated settings: password, time limits, and so on.

To set up a managed program, give the Executable File and a Program Label text for this application, then click *Add*. If desired, you can also give a password and other settings for this application.

To delete an application, select it from the list and click the *Delete* button. To change an application's settings, select it from the list, change its information, and click the *Change* button.

A program not listed here can be launched only if the "Applications Allowed To Run" section of the Group Access tab has been set up to permit this.

Other ways to customize the behavior of managed programs are described under Display Restrictions and Advanced Program Settings.

Applications List: The list at the top of the screen shows all managed programs for this group. Following each application's name is a set of letters, enclosed in angle brackets. These letters indicate the Restrictions and Advanced settings for that program. Of course they aren't as detailed as the Restrictions and Advanced screens themselves, but they are handy to quickly see which flags are set. The one-letter codes are as follows:

P: This program has a password
R: Clone display restrictions are set
W: Show warning screen for timeout warning
S: Play warning sound for timeout warning
A: AutoRun this program at user logon
O: Allow only one copy of this program to run at a time
K: AutoRun, then keep it running until user logoff
T: Don't terminate program at user timeout
N: No file control while this program is the active window
F: Custom file control while this program is the active window
X: Identix biometric validation required to use this program

Move Up / Move Down: Use these buttons to change the order of the applications in the list.

Program Label: The text used when referencing this program on the tray icon menu, and for logging and other internal recordkeeping and tracking purposes.

Executable File: The full path and filename of the program. Whenever the user launches a new program, Full Control Internet will compare its filename to the names on this list. If a match is found, Full Control Internet will apply that listing's program-management settings to the new window.

The filename given here must be the actual executable file, not a Shortcut to the program. One way to get the executable file from the Shortcut is to click the

Browse button, then navigate to the Shortcut and select it -- the actual executable program filename will appear as the Executable File. Another way is to right-click on the Shortcut, select Properties from the pop-up menu, and get the target filename from the Properties screen.

Password: Will a password be required to run this program? If so, list it here. The case sensitive setting of the Security Settings tab controls whether this password is case sensitive.

Minutes Until Warning: The number of minutes from the start of the managed program until the warning message is displayed. Set this to zero if you don't want any warning message for this program. You can also turn off the warning message for this program by un-checking the *Show timeout warning screen* box in the Advanced Settings dialog. Un-checking that box will also stop any User Timeout warning screen from popping up while this program is active, useful for fussy games that take over the screen and don't like external dialogs popping up while they are active. Setting this Minutes Until Warning to zero has no effect on the User Timeout warning screen.

Minutes Until Termination: The number of minutes from the start of the managed program until the program is terminated. It must be a larger number than the Minutes Until Warning. For example, you might set 10 Minutes Until Warning, and 14 Minutes Until Termination. Set this to zero if you don't want any time limits for this program.

Minutes Until Restart Permitted: It's sometimes useful to be able to set a "waiting period" before an application can be restarted after termination. For example, if a parent sets up Junior's game with 30 Minutes Until Termination, what's to prevent Junior from simply restarting the game right away? To take care of this, set 60 Minutes Until Restart Permitted and Junior will have to do something else for an hour. Maybe even homework....

Advanced: The Advanced Settings button lets you provide further customizations. You can provide a customized warning message, choose a timeout-warning sound, and change a number of options which modify the way this application launches and terminates. You can also copy this managed program setup to other Full Control Internet group configurations. (The Advanced settings are described in detail elsewhere in this documentation.)

Advanced settings can only be changed for an existing managed program. To set these options for a new managed program you must first *Add* the program using only the basic settings, then re-select the new program in the list at the top of the page, then click the Advanced button to change those settings.

Clone Display Restrictions: Will you be cloning this computer's Full Control Internet setup? If so, you may want to click this button and use the Display Restrictions screen to list by name the computers on which this managed program should monitored. Or if it's easier, list the computers on which it should *not* be monitored. Or give a file name; if the file is present (and optionally, if the

file's contents match), the managed program will be monitored. See the Display Restrictions page for more on this.

Interface Tab

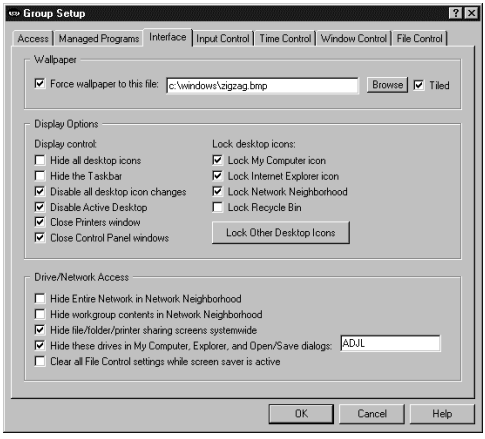
This screen lets you specify how Windows will look and act whenever a member of this group is logged on. (Related settings can be specified on the Input Control tab.)

Wallpaper: Check the box if you want to force the background wallpaper to remain at your chosen setting while this user is logged on. Give the bitmap file name, and check the "tiled" box if you want to tile the wallpaper. If you want to set to "no wallpaper" check the "force wallpaper" box and leave the bitmap file name blank.

Display Control: These checkboxes control the Windows desktop options which are available to the user.

Hide all desktop icons: If this is checked, all desktop icons are made invisible. They reappear when entering Setup Mode or at Full Control Internet's exit.

Hide the Taskbar: If this is checked, the Taskbar and Start button are made invisible. The Start menu and Tray are unavailable.



Disable all desktop icon changes: If this is checked, the user cannot move or rename any desktop icons. Desktop drag/drop changes are also disabled, which means that new items cannot be added by dropping them onto the desktop. Disabled icons can still be used to launch programs, they just can't be moved or renamed; to do that, use the "Lock desktop icons" option (below) to set important desktop icons so they can't launch programs.

Note that this option does not disable the icon right-click menu; to do that, and completely lock down the Desktop, you'll also want to check the option on the Input Control tab labeled "Lock down Windows Explorer, the Desktop, and open/save screens."

Disable Active Desktop: If the computer has Windows 98 or Internet Explorer, the user can turn the entire desktop into a web browser. Check this box if you don't want to allow Active Desktop to be used. When checked, Full Control Internet monitors for Active Desktop activity, so if a user turns on Active Desktop, it is forced off again.

Close Printer windows: This controls the ability to add, delete, or modify a printer.

Close Control Panel windows: This box disables access to Control Panel and Control Panel applets.

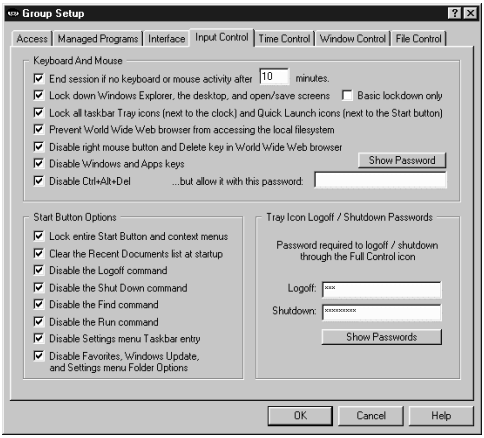
Lock Desktop Icons: A "locked" icon is visible, but completely dead. Unlike the "Disable all desktop icon changes" option (above), clicking on a locked icon will not run its program. It cannot be opened, selected, activated, deleted, moved, or changed. Full Control Internet provides the ability to lock these particular desktop icons because these are the ones that cannot be simply removed from the desktop, as a normal Shortcut can. For convenience, there are checkboxes for locking typical common icons, however you can use the "Lock Other Icons" button to lock any desktop icon by giving its name. (The "name" is the text displayed under the desktop icon.)

Drive/Network Access: These options control access to files, folders, and printers. Check the first box to hide the Entire Network icon in Explorer and Network Neighborhood; check the second box to hide workgroup members in Explorer and Network Neighborhood. (That is, check both boxes to hide everything.) If you don't want to allow users to modify the existing file or printer sharing settings, check the third box.

Check the fourth box to hide the drives whose drive-letters you specify. The listed drives and their folders will not be shown in Explorer, My Computer, or Windows-standard Open/Save dialogs unless explicitly specified. The drives and files are not themselves made invisible; only their listings in Explorer, My Computer, and Windows-standard Open/Save dialogs are hidden. It's like an unlisted phone -- the number isn't in the book, but it will still ring if you call it. This is a fairly good way to remove obvious sources of temptation, and sometimes that's all you need. However, even if (for example) the C drive is controlled through this option, a user can still save a file to c:\somedir\myfile.txt by simply typing the full path into the Save dialog. And if Explorer is explicitly told to open on to a hidden drive, that drive will be displayed. For a much stronger "invisible files" mechanism, consider the File Control feature of Full Control Internet, which makes files and folders so totally invisible that not even Windows itself can see them. You can give systemwide restrictions on the File Control tab, or per-program file control restrictions from the Advanced screen of the Managed Programs tab.

The fifth box is labeled "Clear all File Control settings while screen saver is active." Some screen savers do actual work while they are active, such as defrag the hard drive or test for viruses. Check this box if you use such a screen saver and want to give it access to all files. File Control settings will be temporarily suspended whether they are global settings from the File Control tab or per-program settings from the Advanced screen of the Managed Programs tab.

Input Control Tab



Use these options to indicate how Full Control Internet should treat certain kinds of user input. (Related settings can be specified on the Interface tab.)

Keyboard And Mouse: Full Control Internet can monitor keyboard and mouse activity in Explorer and file-management screens. This can prevent the use of the Delete key, the special Windows keys, the mouse's right-button context menus, and Explorer features such as Find File, Find Folder, Find Computer, and Map Network Drive. In addition, Full Control Internet can disable the right mouse button and Delete key in Netscape or Internet Explorer (version 3 or later). All these features can provide "back door" access methods to your computer.

End session if no keyboard or mouse activity**:** Like a screensaver, Full Control Internet can test for inactivity. It can log off the user, shut down the computer, or display a "no time left" screen with the options specified on the Security tab.

Lock down Windows Explorer, the desktop, and open/save screens: If checked, Full Control Internet will disable Delete and Cut from Explorer's menu or toolbar, or from the keyboard. It will also look for certain Explorer-related window titles and cancel them when found, so as to disable their function (Confirm File Delete, Confirm Folder Delete, Folder Options, Internet Options, Customize, Confirm Multiple File Delete, Find, Map Network Drive, and Create Shortcut, however if there is a Window Control for any of these, the Window Control takes precedence). It will also disable right-mouse-button context menus which, if uncontrolled, can allow the user to run applications, delete and rename files, etc. In NT/2000/XP, checking this box will also close the Task Manager. Disabling these makes Explorer safer. This also prevents using the Delete key and right mouse button on the Desktop, in standard Windows Open/Save dialogs, and most Microsoft Office applications. Note that if your goal is to completely lock down the Desktop, you'll also want to check the Disable all desktop icon changes option on the Interface tab.

Basic lockdown only: If checking the desktop/Explorer box causes any software conflicts (unlikely, but this is Windows after all), use this fallback method which monitors in a different way. The fallback method won't lock desktop icons, and in Explorer it won't catch the use of Cut, and it takes a fraction of a second to catch Delete. During the first few seconds after it is launched, Full Control Internet always uses this "fallback" method.

Lock tray and QuickLaunch icons: Some programs put small icons in the taskbar's "tray" area (next to the clock) or "Quick Launch" area (next to the Start button). Check this box to disable all these icons. (Full Control Internet's tray icon is not available either, so to enter Setup Mode you'll need to use the hotkey or the Reset Mode option.) Note that the clock's Date/Time Properties screen can be disabled elsewhere in Full Control. You can also prevent the clock from being displayed on the taskbar at all.

Prevent World Wide Web browser from accessing the local filesystem: Web browsers can be used to get into the computer's file system. Check this box to prevent browsers from showing files or directories on the local hard disk or network. It will be forced back to a valid website, or closed if no valid site is available. This applies to Netscape and Internet Explorer version 3 or later.

Disable right mouse button and Delete key in World Wide Web browsers: As with Windows Explorer, right-mouse context menus can allow a Web browser to save files and otherwise access areas perhaps best left alone. Full Control Internet can monitor Netscape or Internet Explorer (version 3 or later).

Disable Windows and Apps keys: These keys, found on most keyboards, can launch Explorer windows, the Run dialog, the System Properties hardware setup dialog, and more.

Disable Ctrl+Alt+Del: With this checked, Ctrl+Alt+Del is protected. If you have listed a Ctrl+Alt+Del password, that password is required to use the Close Programs box. If no password is listed, pressing Ctrl+Alt+Del has no effect at all. Additionally, Full Control Internet supports Identix biometric fingerprint validation. If a Ctrl+Alt+Del password is listed here and the Biometric Validation box is checked on the Setup tab, an enrolled fingerprint must be provided to unlock the session. If Identix validation is not installed, checking this box has no effect.

Start Button Options: Use these options to selectively disable elements found on the Start button's popup menu. Note that in general these options disable Start Button *access* to these Windows elements, not the elements themselves. Full Control Internet provides other options to disable the elements themselves, including options on the Interface tab, the *Keyboard And Mouse* options described above, Window Control, and File Control. Some people prefer to use these other options instead, and leave the Start button alone.

These Start Button Options change settings within Windows itself. Start button restrictions are set into place immediately, but on some computers these settings won't be cleared until the next logon. In particular, due to a bug in the Win98/IE4 taskbar, its Start button settings will only update at the next logon. With such systems, you'll need to check the *Enhanced Startup Protection* box on the Security Settings tab. This sets your chosen Start button options in place before Windows builds the Start menu, so its entries will reflect your chosen settings.

Using any of these options will also disable the user's ability to move and delete

entries on the Win98/IE4 Start menu itself.

Lock entire Start Button and context menus: When checked, the Start Menu can't be opened. Clicking on the button does nothing, as do Ctrl+Esc or the Windows keys. If you have hidden all desktop icons and the user double-clicks on the desktop, the menu will appear briefly but will be immediately closed.

Clear the Recent Documents list at startup: When checked, the Start button's list of recently used documents is emptied when Full Control Internet starts, or when the administrator exits from Setup Mode.

Disable Logoff: When checked, the user cannot use the Start button's *Logoff* command. Also see Tray Icon Logoff / Shutdown Passwords, below.

Disable Shut Down: When checked, the user cannot use the Start button's *Shut Down* command, or the *Shut Down* button on the Ctrl+Alt+Del "Close Programs" screen. Also see Tray Icon Logoff / Shutdown Passwords, below.

Disable Find: When checked, the user cannot use the Start button's *Find* command. However, on many computers the *Find* command can still be used through Explorer. To disable that route, check the *Lock down Windows Explorer* box at the top of this tab.

Disable Run: When checked, the user cannot use the Start button's *Run* command line.

Disable Settings menu Taskbar entry: When checked, the user cannot use the Start button's *Settings* | *Taskbar* command to change Taskbar options or Start Menu programs, nor can the user access this screen by right-clicking on the taskbar to access its Properties menu item.

Disable Favorites, Windows Update, and Settings menu Folder Options: Windows 98 and Internet Explorer add these entries to the Start menu. *Favorites* provides access to entertainment and software-update options. *Windows Update* allows users to arbitrarily download new system components and modify the computer's configuration. *Folder Options* allows modification of a number of system settings. If you'd prefer to focus user attention and update your systems in a more organized fashion, check this box to disable these entries. Note: due to Windows bugs, Windows 98 and IE4/5 rebuild the Start menu only at user logon, so to disable these entries on Win98/IE computers you'll need to check the *Enhanced Startup Protection* box on the Security Settings tab. This puts these options in place before Windows builds the Start menu, so its entries will reflect your chosen settings.

Tray Icon Logoff / Shutdown Passwords: If you have disabled the Start button's *Logoff* or *Shut Down* commands, there is no Windows-standard way to shut down the computer or log on as a different user. However, even when you have disabled these you may sometimes want to provide this to certain users. You can do this through the Full Control Internet tray icon's popup menu.

When disabled, a password is required to use the logoff or shutdown items on the Full Control Internet tray icon's popup menu. This could be the password listed here, or the Full Control Internet setup password. If a command is not disabled, the icon menu's logoff or shutdown do not require a password.

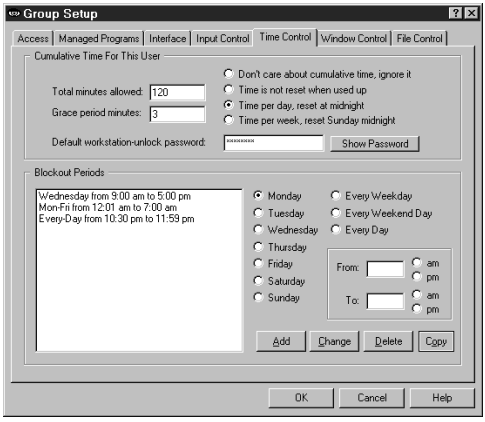
Time Control Tab

Cumulative Time: In addition to each program's individual time limit, the group itself can have a time limit, which controls the maximum time allowed for users in this group. If desired, specify the maximum number of minutes allowed before forced termination. You can change the number of minutes currently used by a particular user from the Users screen.

When the user's time runs out, any active programs are terminated. By default, a three minute "grace period" warning is provided to the user. However the grace period can be changed to whatever you want. Setting it to zero will tell Full Control Internet to give no warning before user timeout.

The time-limit option is very flexible. You can set this as cumulative time per day or per week, in which case the maximum time is again available whenever the time period restarts. Time per day restarts at midnight; time per week restarts on Sunday at midnight. You can use the Managed Program tab's Advanced screen to set any managed program so it continues to work for a timed-out user where the computer is still running.

You can also set this as time per logon, in which case the maximum time is available whenever this user logs on.



Default workstation-unlock password: If a password is listed here, then when there is an inactivity timeout, or when the user locks the workstation, the user will be allowed to unlock the session. If the user has used the Tray Icon option to set a per-user workstation unlock password, that per-user password is required to unlock this session. If the user hasn't set a per-user password, the default workstation-unlock password is required. To use this feature, a default password must be given here, otherwise the user is not given the option to unlock the session.

Blockout Periods: These are days and times during which no programs can be run by this user (except those managed programs which were set so as to

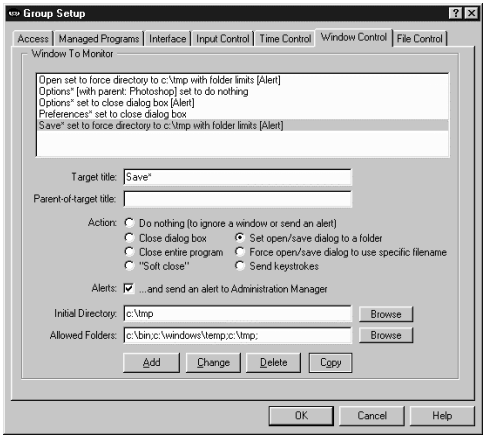
continue to work for a timed-out user), for example "Tuesdays from 7:00 pm to 9:00 pm" or "Weekdays from 9:00 am to 5:00 pm." You can set up as many blockout periods as you like. Blockout periods must start and end on the same day. You can't set up a blockout that goes past midnight (for example "Weekdays from 8:00 pm to 8:00 am") but you can achieve the same effect by entering this as two separate blockout periods, one from 8 pm to 11:59 pm, and the other from midnight to 8 am.

Copy: To copy a blockout to another group, select that item and click the Copy button. You can copy a blockout to one specific group, or to "Every Group."

Window Control Tab

Window Control lets you control virtually any window or dialog when it appears. You can close a window (in one of three ways); you can set *Open* or *Save As* dialogs to a particular folder, from which the user provides the actual filename; you can generate "on the fly" a unique folder-and-filename yourself, forcing the dialog to open or save using only that one specific filename; and most powerful of all, you can send any keystrokes to any window the moment it appears.

You might wonder how these "close window" options differ from Full Control Internet's "allowed applications" feature, which can also look at window titles to decide whether they should be closed. There are two differences. First, the "allowed applications" feature only considers the main window of a program, but the Window Control options will work on any window, including dialogs and other "little" windows that are associated with a main program, which lets you allow a program yet disallow certain specific dialogs. Second, the Window Control feature offers three different ways to close different kinds of windows. These are the first three radio buttons on this screen. See below for details.



The latter three options allow entry into an edit line, labeled above as *Keystrokes* (this label changes depending on which option is selected). In addition to anything else, you can use the words %CURRTIME% (which will be replaced in use with a unique 8-digit number based on the current time), %USERNAME% (user name given through current network or Windows logon), %GROUPNAME% (that user's Full Control Internet group) and %COMPUTERNAME% (the designated name of this current Full Control Internet computer). These are often handy when constructing forced file or directory names. They can also be used when sending keystrokes. (These

special names must be in upper case.)

Let's look at each option in turn.

Target title: Full Control Internet looks at the title bar text of the current active window or dialog, and if the text matches a target title on the Window Control list, the corresponding action is taken. The * and ? wildcards can be used freely in the target title specification.

Parent-of-target title: Sometimes you want to differently manipulate dialogs in different programs, even though the dialogs have the same title. For example, maybe you want to force the Open screen in Word to go to c:\documents, and the Open screen in Excel to go to c:\spreadsheets. Or maybe you want to close the Options screen in Explorer but not the Options screen in any other program. To do this, give the title of the dialog's "parent" window. This is usually the main window of the program. The * and ? wildcards can be used freely, so for example listing *Word* will cover any parent-window with "Word" in its title bar. The title is not case sensitive. If the parent-title is blank, the target title applies to all programs.

Allowed Folders: Some options allow you to specify an *Allowed Folders* list. This is a list of directories which are "available" while the target-title window is visible. All other folders are off-limits. For example, the target title might be *Save As* with an Allowed Folders list of *c:\users\Brenda;d:\general\tmp;A:\;* (Note that each directory name ends with a semicolon, even the final one on the list.) In this example, whenever a *Save As* screen appears in an application, the user can save only to the three named locations *when saving from that application*. This is an important distinction, because unlike the settings on the File Control tab (where it is not advisable to for example make your Windows directory invisible), the Allowed Folders restrictions are not imposed systemwide. Only the program displaying the matching (target title) window is restricted to the locations on the Allowed Folders list. Because of this, the Allowed Folders restrictions can control file-open and file-save locations with a great deal of precision.

List directories in the usual way, with a drive letter followed by a colon and the full path. Multiple directories are separated by a semicolon. Type in the folder names, or use the Browse button to select them. If you Browse for more folders, your newly-selected folder will be added to the current text already listed. For convenience, if you list the root directory of a floppy drive (like A:\ in the example above) that entire floppy drive is available, not just its root directory. Also note that if the Allowed Folders list is blank, all folders are allowed.

In case you need to, you can list files as well as folders. This is useful if certain files need to remain visible while the Allowed Folders list is controlling file access. Allowed Folders works by applying File Control to your system - the only folders that remain available are the ones on the Allowed Folders list. Sometimes, though, you need to not "lock out" a certain file at this time. Allowing this is easy, just add the file to the Allowed Folders list.

A report is available on the Reports Tab listing any attempted accesses of the files which were hidden due to this setting. This report is especially useful when your file-access restrictions cause a program to behave oddly. You know it needs access to a file you've restricted, but which file is it? This report will list all the files it tried to access, but couldn't. Look at the list, identify the problem file, then add it to the Allowed Folders list.

Alerts: When this Window Control's event is detected, a message is sent to the Remote Administration Manager which triggers an Alert. This can pop up a message, play a sound, or send an email to tell the administrator about this condition. To send an Alert, you must check the box to log *Window Control Events* on the Event Log tab of the System Setup screen.

There are many ways in which a Window Control can work:

Do nothing: This option has two useful purposes. First, you can use it to set up an "exception" to another Window Control, for example if you have another Window Control which closes all Options dialogs, you could add a do-nothing Window Control so the Options dialog from Excel is allowed to remain open. Second, you can use it to set up a Window Control that doesn't actually do anything, but does send an Alert when a particular program is launched. To send an Alert you must check the box on the Event Log tab to log Window Control events.

Close dialog box: Many programs provide menu items which pop up dialog boxes. Perhaps you don't want a particular dialog box available to the user. If so, give that dialog's titlebar text as the target title. When a window of that title appears, it will be closed. Use this for dialogs that close when you hit the Escape key.

Close entire program: If you want to be sure a particular program never runs, list its titlebar text here. It will be terminated in the usual Full Control Internet fashion as soon as it comes up. Of course, another way to disallow such programs is by making sure inappropriate programs are not allowed to this user. But then you have to list every non-managed program which is allowed to run. That can get tedious. Use the "close entire program" when you are willing to allow most programs, but want to deny access to one specific program.

"Soft close": You won't need this often, but when you do it's very handy. Like the "close entire program" option, this is intended to close an entire application, not a dialog box. Use this to close those rare applications that *must* be given the opportunity to close in their own manner. Some programs leave themselves or the computer in a sub-optimal state when forced to terminate in the usual Full Control Internet fashion. However, such programs might tolerate this "soft close" method, which attempts to use the program's own termination procedure to get it to exit gracefully. This method won't always work; in particular, it might trigger an "are you sure you want to exit" message from the program you are trying to terminate, which could allow the user to continue. But if the program does not have this sort of "are you sure" message (or if you can disable that message),

the "soft close" can provide a useful alternative method of terminating fussy programs. "Soft close" is especially handy when trying to persuade a recalcitrant game to restore the normal Windows screen colors at exit.

Set open/save dialog to a folder: Use this when you want users to open files from, or save files to, a particular folder. Give the proper directory in the edit line (which will relabel itself to "Initial Directory:" when using this option). You can drag-and-drop a folder from Explorer onto that line too, if you prefer. Your target title will generally be "Open" or "Save As" because this works best with the standard Windows file-open and file-save dialogs. However, it can often be used with other non-standard dialogs as well.

When used by itself, this option does not force the dialog to stay in the directory to which it has been set, so you'll generally want to also provide an Allowed Folders list, to not only set your users to a specific directory, but also keep them there.

Note that other Full Control Internet options let you hide drives, or make files or folders read-only or invisible, but these other options *keep the user away from* a location. Setting open/save screens to a folder actively *moves the user to* a location, and makes sure they stay there when used in conjunction with the Allowed Folders option.

Force open/save dialog to use a specific filename: This is similar to setting a file-open or file-save dialog to a folder, but this option generates a filename, sets the screen to the generated filename, then presses Enter to submit the name and immediately close the dialog. As with the folder option, this works best with the standard Windows file-open and file-save dialogs. You may wonder how this option can be used more than once without the latter use overwriting the former. The answer is to generate the filename "on the fly" by including the word %CURRTIME% as part of the forced filename, which will be replaced in use with a unique 8-digit number based on the current time. You can also use the words %USERNAME% (user name given through current network or Windows logon), %GROUPNAME% (that user's Full Control Internet group) and %COMPUTERNAME% (the designated name of this current Full Control Internet computer). All these are case sensitive. And here's a hint: when constructing the filename, don't give a file extension. Instead, let the Save As dialog add its default extension to your generated name. This allows Windows to do certain automated processing based on the file's extension.

Send keystrokes: This option lets you send any keystrokes to any window the moment that window's target title appears. For example, you could use this to manipulate a nonstandard file-open or file-save window, one that won't respond to the "set to a folder" option. Do this by sending the exact keystrokes the nonstandard screen needs in order to have it do what you want. You can also use the Allowed Folders settings to force such nonstandard "Open" or "Save As" screens to only use specific directories.

What keystrokes can you send to a window? You can give regular characters, of

course, so to send "abc" simply type that into the edit line (which will relabel itself to "Keystrokes:" when using this option). You can also give special characters. To press the Shift key, use the plus sign +. To press the Control key, use the caret ^. To press the Alt key, use the percent sign %. One way to press Enter is use the tilde ~.

If you need to use a special character in its usual sense, enclose it in brackets. For example to send an actual plus character you'd type {+}. To send an open or close bracket, type {{} or {}} as required.

You can also use certain nonprinting characters by giving their name in brackets. Here is a list: {Bksp} {Break} {CapsLock} {Clear} {Del} [End} {Enter} {Esc} {Help} {Home} {Insert} {NumLock} {PgDn} {PgUp} {PrtSc} {ScrollLock} {Tab} {F1} to {F12} {Up} {Down} {Left} {Right}

To give a regular key combined with Shift, Control, or Alt, precede the key with one or more of the +^% special characters. To indicate that more than one of these are held down while pressing a key, enclose the entire set in brackets, for example {^%J}. Parentheses can be used to group keystrokes. For example, to hold down the Shift while pressing BDS, use +(BDS). To hold down Shift for only the first of these, use +BDS.

Keys can be repeated. To repeat a keystroke, use the form {key number}. There must always be a space between the key and the number. For example {Up 5} presses the up-arrow five times, and {J 12} presses the J key 12 times.

Log typed keystrokes: This option lets you log all keystrokes typed by the user while the designated window is the active forground program. Keystrokes are logged through the Remote Administration Manager to the Event Log database. It works just like the systemwide keystroke event logging, but only keys typed into this one window are logged.

Copy: To copy an item to another group, select that item and click the Copy button. You can copy an item to one specific group, or to "Every Group."

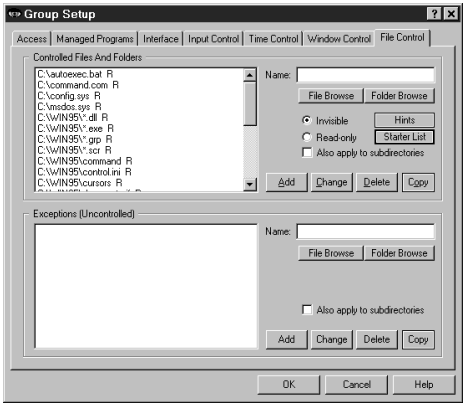
File Control Tab

With this screen, you can make any local file or directory read-only or invisible. Full Control Internet's file control mechanism is very powerful. Unlike the hide-drives list on the Interface tab, files and folders hidden by File Control are totally invisible, even to Windows itself. They simply do not exist. Because controlled files and folders are locked to both the user and the operating system, certain files and folders should be controlled only with caution. See below for some cautions, hints, and suggestions.

In addition to these systemwide restrictions, you can also give per-program file control restrictions that are in effect only when a particular managed program is

active. This is done from the Advanced screen of the Managed Programs tab. If per-program restrictions are given, and that program happens to be the active window, the per-program restrictions will override these systemwide settings on the File Control tab.

If your screen saver does actual work while it is active, such as defrag the hard drive or test for viruses, you may want to give it access to all files. To do this, go to the Interface tab and check the box labeled "Clear all File Control settings while screen saver is active."



Restrictions: Use the *Controlled Files And Folders* section to indicate the protection you want. For convenience, you can use a single entry to protect an entire branch of your directory tree by checking the "also apply to subdirectories" box. The flags I, R, and S (invisible, read-only, and subdirectories) at the end of each line indicate the protection applied to that entry. Each group can have individual File Control listings. You can use the words %COMPUTERNAME% (the current computer's name), %USERNAME% (user name given through current network or Windows logon), %GROUPNAME% (that user's Full Control Internet group) and %CURRTIME% (a unique number based on the current time) as part of the file or folder names you enter. (All these are case sensitive.)

Exceptions: Use the *Exceptions* section when you want to protect the named *Controlled Files And Folders* in general within this Group, but want one file or folder to be available. It's useful if you've made a folder invisible but you need access to one particular file in that folder. For example, suppose an application isn't running properly and you suspect that a necessary component has been made invisible or read-only. Use the access-denied report to list by program name the files which that application is unable to access, then add the required files to the Exceptions section for this group. *Exceptions* are displayed only if there are *Controlled Files And Folders* listed.

Copy: To copy a list to another group, click the appropriate Copy button. You can copy a list to one specific group, or to "Every Group."

Starter List: Click the Starter List button to generate a list of files and folders which are often advisable to lock. However, no list can apply to every computer, so test to make sure that these entries are appropriate in your particular situation.

Hints: Full Control Internet can make any local (non-network) file or folder read-only or totally invisible. Controlled files and folders are completely locked to users, applications, and even Windows itself. Be careful when controlling them!

Here are some examples:

Windows Directory: Don't make everything in the Windows directory invisible. Windows will be unable to function. Instead, protect Windows by making important components read-only. Click the Starter List button for sample settings that work well on most computers.

Full Control Internet Directory: It's not necessary to protect Full Control Internet's own folder. Sometimes it needs to write its own files to its own directory. Don't worry, this is taken into account in Full Control Internet's own built-in protection.

Entire Drive: On most computers if you make your entire C:\ drive invisible (including all subdirectories), your programs can't be seen. This will also include the Windows directory, and Windows will be unable to function. Instead, separately add your application and data folders, then protect individual Windows components. Click the Starter List button for sample settings that work well on most computers.

Directories Listed In Environment Variables: Folders listed under TEMP or TMP environment variables need to remain available for creating temporary files. Some programs also list their own necessary directories in environment variables. Certain folders under the Windows directory must remain available too, such as the Recent Documents and Spool folders.

Download, Cache and Cookies Directories: Web browsers and other programs assume that they can update such directories at any time.

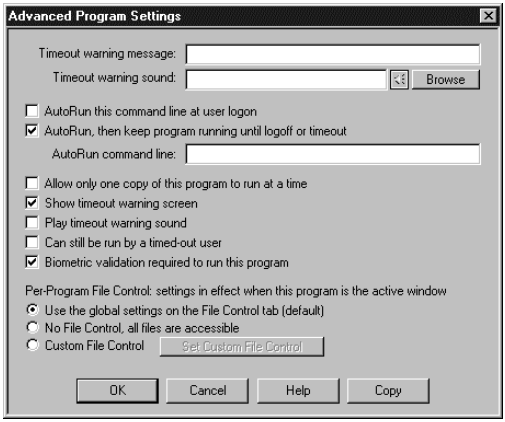
Recycle Bin And Similar Folders: The Recycle Bin and similar folders used by Windows, Norton Utilities, and other programs must be available so files can be moved into them when deleted.

How To Set Up Per-User Folders: The *Exceptions* section also provides a neat way to quickly set up private work areas for each user. Let's say you have a subdirectory named User Folders, under which each user has a personal directory which has the same name the user will give when logging on. To ensure privacy for each user, make all subdirectories of the User Folders directory invisible by giving a filespec something like C:\...\User Folders*.* and checking the Invisible and Subdirectories boxes. Then set up an Exception that looks something like C:\...\User Folders\%USERNAME% and check that line's Subdirectories box, too. When a user logs on, Full Control Internet will make all the User Folders invisible, *except* the one with the same name as the logged-on user. If you want to organize things even more, you could give the Exception as C:\...\User Folders\%GROUPNAME%\%USERNAME% or some such.

Access-Denied Reports: If any of your programs don't work correctly under Full Control Internet's file protection, use Full Control Internet's access-denied reports to see which required files were unavailable, and what programs requested them. Then list those files or folders as Exceptions.

Use Window Control Instead? A listing on the File Control tab restricts all running programs, at all times that a user from this group is logged on. Another option might be to consider using the Allowed Folders option on the Window Control tab to limit access only when an Open or Save As screen is displayed, and only for the one program which is displaying the Open or Save As screen.

Advanced Program Settings



The Advanced Program Settings screen is reached by clicking the Advanced button on the Managed Programs tab of the Group Setup dialog. The options on this screen let you further customize the way a program runs. You can also copy a program's settings to another Full Control Internet group.

Timeout warning message: This is your customized warning message to be displayed for this program when it is almost out of time. If you don't provide a message, a generic warning message is used. It's helpful to indicate in your warning message just how much time remains before termination. Your message can be up to 300 characters long.

Timeout warning sound: Choose any WAV file to be played to warn the user that this program will soon run out of time. If no file is specified, and the *Play Warning Sound* box (below) is checked, Full Control Internet plays its built-in warning sound. No sound is played if the Quiet Mode option has been selected.

AutoRun this command at user logon: Check this box to run the *AutoRun command line* automatically when the user logs on.

AutoRun, then keep program running until logoff or timeout: If this box is checked, the *AutoRun command line* will run automatically when the user logs on, and in addition it will be re-run as necessary to ensure that its program (the executable listed on the Managed Programs tab) is always running. If you check this box it is unnecessary to also check "AutoRun at logon".

AutoRun command line: This is the full command line to run if either of the AutoRun boxes is checked. It including any command-line parameters.

Allow only one copy of this program to run at a time: By default, Full Control Internet acts like regular Windows and allows multiple instances of a program to run. Check this box if you want to restrict this program so only one copy can be active at a time. Note that this does not limit multiple windows from *one* copy of a program (for example, multiple Web browser windows). Rather, it prevents launching more than one simultaneous copy of a program.

Show timeout warning screen: Un-check this box if you don't want any warning message for this program. You can also turn off the warning message for this program by setting the Minutes Until Warning to zero on the Managed Programs

tab of the Group Setup dialog. What's the difference? Un-checking this box will stop any user timeout warning screen from popping up while this program is active; setting the Minutes Until Warning to zero has no effect on the user timeout warning screen.

Play timeout warning sound: Should a sound be played to warn the user that this program will soon run out of time? If this box is checked and no Timeout Warning Sound file is specified, Full Control Internet plays its built-in warning sound.

Can still be run by a timed-out user: This applies if, when a user runs out of time, you have set Full Control Internet to display its "no time left" screen instead of logging off or shutting down the computer. In that case, Full Control Internet ensures that no new programs can run ... unless it's a managed program with this box checked.

Biometric validation required: Full Control Internet supports Identix biometric fingerprint validation. If this box is checked, an enrolled fingerprint must be provided to use this program. If Identix fingerprint validation is not installed, checking this box has no effect.

Per-Program File Control: You can set the files and folders which are available when this program is the active foreground window. It works much like the systemwide options on the File Control Tab, but it allows you to control access to a much finer degree of precision. The radio buttons provide three options. If you choose the first radio button, this program uses the systemwide File Control Tab restrictions, and will have no special settings of its own. If you choose the second radio button, all restrictions will be removed while this program is the active window, providing full access to everything. The third radio button allows you to specify custom settings to be put into place while this program is active. Click the button to "Set Custom File Control" and give these settings on the Custom Per-Program File Control screen.

Copy: To copy this managed program's settings to another group, click the Copy button. You can copy the settings to one specific group, or to "Every Group" on this computer.

Abnormal Exit in Strict Mode

On the Access tab if using the Strict option under "Applications Allowed To Run" control, if for any reason Full Control Internet exits abnormally, the Strict low-level "don't run" settings will still be in place, and almost nothing on your computer will run. If this happens, Full Control Internet provides a number of recovery options, which are listed here in the recommended order.

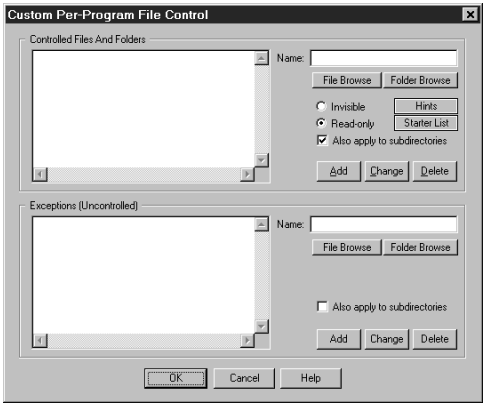
• First, try to run Full Control Internet again; you can exit immediately if you like, because when Full Control Internet exits normally it clears any leftover control settings.

• If you can't launch Full Control Internet normally, try starting in Reset Mode. You can run the Full Control Internet *Reset* program (reset.exe) from the Start menu, from Explorer, or in any other convenient way. Like Full Control Internet itself, reset.exe should always run. As above, simply start Full Control Internet and exit normally to clear the settings.

• Restart the computer in Safe Mode. Strict security settings are ignored in Safe Mode, so Full Control Internet will *always* run. Launch Full Control Internet and then exit normally; the security settings will be cleared. Then reboot in regular Windows and you'll be back to normal.

• Another way to reset to usable settings is by restoring the *user.dat*, *system.dat*, and (in ME) *classes.dat* Registry files. Each time Full Control Internet starts, it saves backups of these files as *userfci.bds*, *sysfci.bds*, and (in ME) *classfci.bds* in your Windows directory. Using them to restore your previous files will clear any restrictions. However, you will lose any system configuration changes you made since they were backed up. In Windows 95/98/ME, you must boot to plain DOS ("command prompt only", or use a DOS boot disk) to copy these files. Copy *userfci.bds* to *user.dat*, and copy *sysfci.bds* to *system.dat*. In Windows ME, copy *classfci.bds* to *classes.dat*. These are hidden, system, read-only files in your Windows directory so you will need to use the DOS commands ATTRIB -H -S -R USER.DAT and ATTRIB -H -S -R SYSTEM.DAT to make them visible. Similarly, use ATTRIB to make *userfci.bds*, *sysfci.bds*, and *classfci.bds* visible so you can copy them. In Windows NT/2000/XP, you can restore the Registry through your Emergency Recovery Disk which you previously created using the NT/2000/XP facilities. Or if the computer is set up to allow booting into Windows 95/98/ME or from a floppy, you can restore the Registry files in that way. Windows ME and XP also provide their own rollback facility that may be useful for this purpose.

Per-Program File Control



This screen is accessed from the Advanced dialog of the Managed Programs tab. On this screen, you can list files and folders to be protected while a particular program is the active foreground window. This works very much like the File Control tab except that it sets restrictions and exceptions which will be put into place only when its program is active. Per-program settings override any systemwide File Control settings given on the File Control tab.

A easy "special case" of this feature is available for screen savers. If your screen saver does actual work while it is active, such as defragmenting the hard drive or testing for viruses, you may want to give it access to all files. To do this, go to the Interface tab and check the box labeled "Clear all File Control settings while screen saver is active."

Restrictions: Use the *Controlled Files And Folders* section to indicate the protection you want. For convenience, you can use a single entry to protect an entire branch of your directory tree by checking the "also apply to subdirectories" box. The flags I, R, and S (invisible, read-only, and subdirectories) at the end of each line indicate the protection applied to that entry. Each group can have individual File Control listings. You can use the words %COMPUTERNAME% (the current computer's name), %USERNAME% (user name given through current network or Windows logon), %GROUPNAME% (that user's Full Control Internet group) and %CURRTIME% (a unique number based on the current time) as part of the file or folder names you enter. All these are case sensitive.

Exceptions: Use the *Exceptions* section when you want to protect the named *Controlled Files And Folders* in general while this program is the active window, but want one file or folder to be available. It's useful if you've made a folder invisible but you need access to one particular file in that folder. For example, suppose an application isn't running properly and you suspect that a necessary component has been made invisible or read-only. Use the access-denied report to list by program name the files which that application is unable to access, then add the required files to the Exceptions section for this group. *Exceptions* are displayed only if there are *Controlled Files And Folders* listed.

Starter List: Click the Starter List button to generate a list of files and folders which are often advisable to lock. However, no list can apply to every computer, so test to make sure that these entries are appropriate in your particular situation.

Hints: Full Control Internet can make any local (non-network) file or folder read-only or totally invisible. Controlled files and folders are completely locked to users, applications, and even Windows itself. Be careful when controlling them! See the File Control Tab section for some examples.

Chapter 3
Security And Administration

System Administration With Full Control Internet

The concept of Full Control Internet is that there is a system administrator who sets up and maintains the system. This person has access to many features that a normal user cannot use. These features allow the administrator to set up and change the system, and monitor it through usage reports and logs. Some features are especially intended to be handy when managing more than one Full Control Internet-enabled computer, on a LAN or over the Internet.

Full Control Internet provides many ways for you to manage computers remotely. You can set up your master clone configuration with per-computer options which let you specify which managed programs and users will be monitored on what computers. In this way, you can create and distribute just one master clone setup, yet the options available on each client computer will be a function of the configuration of that computer, and the name of the user currently logged on to that computer.

While a client computer is active you can use the Remote Administration Manager to reconfigure that computer and modify its settings on the fly. You can query the status of the remote computer and then manage it based on that status. The Remote Administration Manager is designed specifically to allow administrators to dynamically modify settings and control access and activity on remote computers. See *Administration Manager Strategies* for hints and ideas on using this tool.

Security Considerations

Full Control Internet provides very thorough security control for your computer. Here are some things you can do to help Full Control Internet, and provide further protection.

Protect important drives, files, and folders: You may not want users freely accessing the computer's directory structure, changing or deleting files, etc. To prevent this, use Full Control Internet's File Control to make your important files and folders read-only or invisible. Another option is to use the Interface Tab to hide drives when this user is logged on. However, the "hide drives" method is not as strong. Though the drives are not listed in Explorer, My Computer, and elsewhere, their files and folders are available by simply typing in the full path to them (for example in the Run screen or Open/Save dialogs). File Control is a much more reliable way to control sensitive areas.

Consider what is run at startup: The programs listed in your Startup folder are launched whenever Windows starts. Programs listed on the load= and run= lines of your WIN.INI file are also run at startup, as are programs listed in certain Registry keys. It's a good idea to think about these programs, and ensure that none allow access to areas you'd rather keep hidden.

Disable booting from floppy disk: If your computer is booted to DOS from a floppy, Full Control Internet won't run so it can't protect your system. Fortunately, it's easy to guard against this. On most computers, you can use the boot-time CMOS setup screen to disable booting from floppy, or perhaps to reverse the testing order of the drives (so it will first try to boot from C:, then try A: only if C: doesn't work). On most machines you run the CMOS setup by pressing DEL at startup, but if yours is different, don't worry. It generally says right on the boot-time screen which key to press to run your CMOS setup.

Use a CMOS password: On most computers you can password-protect your CMOS setup screen so nobody else can undo your protection. Be careful! The CMOS setup configures some very important settings. Doing the wrong thing can have serious consequences.

Change passwords regularly: An easy way to enhance security is to change the setup and application passwords on a regular basis. Change them to something that isn't obvious, so as to make them difficult to guess.

Make the Default Group settings rather restrictive: If you are not using Full Control Internet's logon validation, a user can log on to Windows under an unknown name. If that happens, the Default Group settings are used. Encourage users to log on under their own names by setting up the Default Group to allow very little activity.

Administration Manager Strategies

The Remote Administration Manager gives you a realtime view of what is running, for how long, on which computers, by which users. Its centralized logging provides a user activity audit trail, and its remote administration capabilities let you update and modify the client computers from your central location.

The Remote Administration Manager is installed on only one computer. This is the central computer from which you (the administrator) will do your remote administration. This computer should have good physical security. It should not be out in the open where 'just anybody' can get at it. It is a server.

In general the Remote Administration Manager is always running so it can stay in contact with the desktop clients, keep the central event log up to date, and send your commands to the managed computers. However, it's okay if it exits. The desktop clients will try periodically to reconnect, and cache their log records locally until they do.

The event log collects many different kinds of information. The built-in reports cover the most common inquiries, but other inquiries are quite possible. The event log format is documented, allowing you to construct any query that is of interest. Most production environments should log to a standard format like Access, Excel, or a SQL database, not the Bardon Default logging format.

When certain events occur you might want the system to generate an Event Alert which can display a message, play a sound, or remotely notify you by pager or email (including an SMS email to your cell phone).

If your managed computers are on different LANs, the Remote Administration Manager must be run on a computer with a static IP address (one that is directly visible to the Internet) so it is visible to all your various desktop client computers. As with all static IP computers (for example, webservers), you should run appropriate security software on this computer such as firewall, antivirus, etc. The desktop clients can be on either static IP computers or masqueraded computers. If the desktop clients are run in static IP computers, appropriate security software should be run there as well.

For added security you may want to list with the Remote Administration Manager the IP addresses of all desktop clients allowed to contact it. Connection requests from other IP addresses will be refused. Refused connections are logged. Look at these items in the event log to list computers that were not allowed access. Perhaps someone is trying to break into your system. Or perhaps some are legitimate desktop clients that should be added to the list.

If a licensed copy of WinU Internet or Full Control Internet is also installed on your administration computer, its setup password is required in order to use any

Administration Manager feature which modifies the remote computers. To those without this password, the Administration manager is only a 'read-only' screen that cannot send commands to the connected computers. After the password is given, the Administration Manager won't ask again for 15 minutes. If you want to re-lock the password security before the 15 minute period expires (perhaps so you can walk away from the computer) use the *Password Lock Now* item on the *Setup* menu. If a licensed copy is installed, both Setup passwords are required.

To see what a desktop client is doing, use the Commands | Program Management screen to list running programs. Need to close one of them? Copy/paste from this report the filename of the program to close, also on the Commands | Program Management screen. Something isn't running that should be active? Launch it from the Commands | Program Management screen. If your launched program requires a more open security situation (for example, an installer or uninstaller) check the box to temporarily disable security control.

Need to move a new program to one or more desktop clients (as opposed to running a program that is already there)? Use the Commands | File Transfer screen. After it is transferred, you can run it using the Commands | Program Management screen.

Need to remotely mass-install a new-version update of WinU Internet or Full Control Internet on all your managed computers? You can't simply remotely run the installer, because WinU Internet or Full Control Internet is already running, and it might not allow an installer to run on that computer, not to mention that Windows won't let you overwrite a running program. The solution is to use the Commands | Version Update screen.

If you need to have a conversation with a user, connect to that user with Realtime Chat. The administrator can initiate a Chat session from the Commands | Other Settings screen at any time. The user can initiate a Chat session if the administrator has allowed the Chat item to be displayed on the  tray icon menu.

To distribute licenses to your connected computers, enter them on the Managed License Numbers screen. The license will be sent to the client computers as they connect to the Remote Administration Manager. Multiple license numbers can be entered.

How To Clone A Computer

Full Control Internet's cloning feature saves this computer's Full Control Internet settings so they can be copied to another computer or kept as a backup.

To clone a computer, first set up your chosen groups, users, managed programs, passwords, sounds, display restrictions, licensing information, etc. You can set this up from the Remote Administration Manager or from one of your client computers. After it is set up, click the *Export Clone File* button to save it. On the client computers, this button is on the Remote Management tab. If you are doing your setup from the Remote Administration Manager it is on the Configuration screen.

There are three ways to use a clone file to transfer the exported clone configuration data to a remote computer:

Update when installing: To include the clone data as part of the initial installation process, copy the clone data file to the same directory as the Full Control Internet installer (typically, a floppy disk or a network install directory), with the other Full Control Internet files. It must be named *clonefci.bds.* Run the Full Control Internet installer in the usual way. When the installer sees the *clonefci.bds* data file, it will offer to copy the clone data onto the new machine. When performing an automated "quiet" install, if a *clonefci.bds* data file is found, its settings are always read, and Full Control Internet is then immediately launched by the installer and sets up any options specified in the clone file.

Updating manually: To update manually, enter Full Control Internet's setup mode on the client computer you want to update, go to the Remote Management tab, and click its *Import Clone File* button. The clone file does not need to be named *clonefci.bds* because you are explicitly pointing Full Control Internet to the clone file you want it to use.

Update from the Remote Administration Manager: Any clone file that is visible to the Remote Administration Manager can be sent to one or more client computers to update their settings. From the Remote Administration Manager main menu, choose Clones, then Send A Clone File. While updating from the Remote Administration Manager, Full Control Internet displays an "Updating..." screen. If you prefer that this screen not be displayed, create an environment variable named BDSUPD and set it to FALSE. That is, put a line saying SET BDSUPD=FALSE in your autoexec.bat (95/98/ME). Under NT/2000/XP set this under the systemwide or per-user environment variables.

A useful tool for cloning is Full Control Internet's Display Restrictions feature. This lets you control the computers on which a user or managed program is monitored. When setting up your master computer, you can give information for

each individual user and managed program. At runtime Full Control Internet can test the name of the current computer, the presence/absence of a file, and/or that file's contents. Using this feature, you can set up just one clone file to distribute to all Full Control Internet computers, yet have each computer use an individual configuration. For example, if you want a program to be available on some computers but not on others, list that application as a managed program, set its display restrictions so the program-management listing is not visible on certain computers, and set global restrictions on allowed applications so non-managed programs won't run. In this way you can distribute the same clone file to different computers and achieve individual results on each workstation.

This technique also works with all the other per-user settings. Full Control Internet's Interface Control, File Control, Input Control, Time Control, and Window Control are set up per-group; the above mechanisms let you control what each user can do, on which computers. As above, you need only distribute one master clone configuration to tightly control all file and program access per-computer and per-user throughout the enterprise.

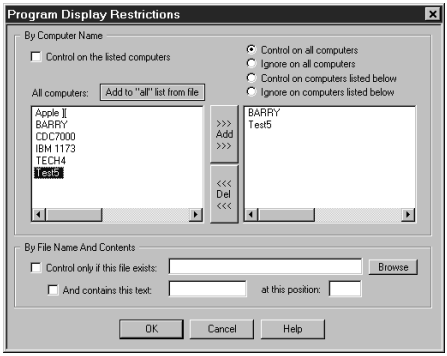
Full Control Internet can read Full Control 2 clone files. To do this, go to the Remote Management tab of the System Setup screen and click the *Import Clone File* button. The old-style clone's settings will be converted automatically as they are read. Study the results to ensure that the automatic conversion meets your needs. After confirming the settings, you can export them as a new Full Control Internet clone file which can be automatically distributed in any of the usual ways.

Per-user workstation unlock passwords (set from the Tray Icon) are valid only on the one computer where they are entered. They are not cloned, and do not carry over when a new clone is read.

Administration Manager note: Clone configuration files can be created and managed from the Remote Administration Manager. When using the Remote Management tab from the Administration Manager, the Import and Export buttons are disabled, since importing and exporting are done from the main Configuration screen.

Licensing note: If this computer connects to the Remote Administration Manager, its licensing information can be obtained from there. That is, if you list the port and IP address of the Remote Administration Manager that will be overseeing this computer, and if you enter into the Remote Administration Manager your license number(s), the Remote Administration Manager will distribute licensing information to the connected computers that it oversees.

Per-Computer Display Restrictions



Let's say you are setting up Full Control Internet on one master computer, and you intend to clone this setup and distribute it to other computers. In this situation, you sometimes need to specify which managed programs and groups will be monitored on what computers.

That's what the Display Restrictions screen is for. You can get here from two places on the Group Setup tabbed dialog. If you reach this screen from the Managed Programs tab, you can specify the computers on which that application will be treated as a managed program. If you get here from the Access tab, you can specify the computers on which a group's settings are considered at logon. For example, if a group's Restrictions settings are such that the group is to be ignored on this computer, Full Control Internet's logon validation can be set up to not accept a user who is a member of that group. If the user is allowed to log on under that "unknown" name the Default Group settings will be used. Similarly, if a managed program's Restrictions don't allow its listing to be seen on the current computer, then when that program is run it will be treated as a non-managed program.

Selection Criteria: Full Control Internet can look at the target computer's name to decide whether to monitor this managed program or group. Or it can decide based on the presence/absence of a file, or by that file's contents. You can use one or more of these tests. If you use multiple tests, all tests must be met.

Control on the listed computers: Check this box to use the Full Control Internet computer name to decide whether to monitor this managed program or group. Then choose one of the radio buttons to decide which name-based test Full Control Internet will perform. Should the program or group be controlled on all listed computers? Or ignored on all listed computers, and controlled on the rest? For convenience, there are also selections for "all computers."

To put a computer on the list, add its name to the right-side box. Double-click on its name in the left-box list, or select it in that list and press the *Add* button. To remove a computer from the list, double-click on its name in the right-box list, or select it in that list and press the *Del* button.

Control only if this file exists: Check this box to have Full Control Internet look for the named file to decide whether to monitor this managed program or user. If the file exists, the program or user will be monitored. You can also test the file's contents (see below).

And contains this text: Check this box if you want Full Control Internet to test the text characters contained in the file. In this test, Full Control Internet will open the file and read it. Do the characters in the file match the characters you have typed here? If so, the program or user will be monitored.

At this position: The test characters do not have to be at the beginning of the file. If you want Full Control Internet to look at characters elsewhere in the file, give the offset here. The first character in the file is number 1, the second is 2, etc. By default, Full Control Internet will test at the beginning of the file (character number 1).

Adding Computers To The List: How do names get on to the "all computers" list? These come from two sources: the Administration Manager data and your own list of computers.

First, if the Administration Manager has been run on this computer, it has saved its data here. Full Control Internet will find and read its saved-data list, and include any computers that Administration Manager knows about. Running the Administration Manager and modifying the Display Restrictions are both done only by the system administrator, so it's not unlikely that the same computer is used for both tasks.

Second, you can use the "add from file" button to import your own list of computers. Click the button and give the name of your plain-text file. The delimiter between computer names can be a comma, a tab, a double-quote, a newline, or any combination of these. Multiple delimiters together are treated as a single delimiter, for example the quote-comma-quote between items in a CSV (comma separated values) list.

Realtime Interactive Chat

The administrator or the user can initiate a Realtime Chat conversation, in which text typed by one party is immediately displayed to the other party. The administrator initiates a chat session by checking the Chat box on the Other Settings screen. If allowed to do so, the user initiates a chat session by selecting the Remote Administrator Chat item on the tray icon menu.

A separate chat window is displayed for each conversation. Because there is only one Remote Administration Manager, the user can only have one chat conversation at a time. However, the administrator can have many chat sessions active simultaneously.

The administrator can initiate a chat session with the user at any time. However, the user can initiate a chat session only if the administrator has allowed the Chat item to be displayed on the tray icon menu.

The ports used by the Remote Administration Manager for chat communications are set on the Communication port and IP address dialog. Two ports are used per chat session, so there must be at least two ports available.

Reset Mode

Reset Mode is a fail-safe mechanism built into Full Control Internet. It lets you start Full Control Internet and use its setup screens while not actually launching the security protections which those screens define. This is useful if you accidentally create some security control which locks you out of the computer. It can also be used to get into Setup Mode while Full Control Internet is running.

Before Full Control Internet Starts: To start Full Control Internet in Reset Mode, run the Full Control Internet Reset program (reset.exe) from Explorer, or in any other convenient way. When used before Full Control Internet starts, reset.exe must be in the same directory as the Full Control Internet program itself. Another way is to start Full Control Internet in reset mode from a command prompt with the /reset parameter (c:\somedir\otherdir\fc.exe /reset).

While Full Control Internet Is Running: Reset Mode is also used to access Full Control Internet's configuration options while Full Control Internet is running, for example when you have set (on the Security Settings tab) that its tray icon should be hidden. If Full Control Internet is already running when you start in Reset Mode, Full Control Internet will ask for its setup password, then go into setup mode and displays its Configuration screen allowing you to make any necessary changes. When using Reset Mode in this way, after leaving setup mode the disabled security settings listed below will be re-enabled and Full Control Internet will function normally.

You will be prompted for your setup password so as to be allowed to use Reset Mode. After giving it, you can change your configuration screens and eliminate the setting that caused the problem. Then exit Full Control Internet normally.

Automatically At Startup: There may be a situation where you need to get into Reset mode, but something is happening right at startup that prevents this. One way around this is to run Reset Mode from a shortcut or batch file in your Startup folder with the /wait parameter. This will launch reset.exe, wait the specified number of seconds, and only then ask the running copy of Full Control Internet to go into Reset Mode. The batch file only needs one line, something like this:

c:\..<your path here>...\reset.exe /wait=180

In this example, fcreset.exe will wait 180 seconds before asking Full Control Internet to go into Reset Mode. If you just give the parameter as /wait with no equals sign or number of seconds, it defaults to waiting 120 seconds.

How To Use: When in Reset Mode, you should simply make the necessary setup changes and then exit, because most of Full Control Internet's strongest security settings are not in effect. In this mode, Full Control Internet does not perform the following security checks: exit if this is an expired beta copy; test its components for tampering; validate user names at logon; enforce the inactivity timer; run AutoRun programs for this user; exit if a user's time has run out;

process remote clone files or administration messages; monitor for Window Control; do logging; prevent running DOS applications; prevent running programs not on the Managed Programs or Allowed Applications lists; hide drives; prevent saving settings on exit; restrict Control Panel or Start Menu access; monitor keyboard or mouse activity (for example, for the Windows keys, Delete key, or right-mouse context menus); keep the CD door locked; disable Ctrl+Alt+Del; and make files or directories invisible or read-only.

Password Screen Timeouts: In Reset Mode password screen timeouts are set extra-long to ensure that you are able to give a password regardless of how fast you have set the password-screen timeout.

Using The fcRunApp Utility

The fcRunApp program can run a DOS application when DOS apps are otherwise disabled by Full Control Internet. The allowed DOS application must be listed as an "exception" on the Access tab of the Group Setup screen, and the allowed DOS application must be launched through fcRunApp. To do this, you need to run fcRunApp from a shortcut (.lnk file) so you can give it a command line. This command line tells fcRunApp which DOS program to run. So, you might set up MyDOScmd.lnk which might have a Target command line of the form:

```
    c:\somedir\otherdir\fcRunApp.exe
/cmd=d:\anydir\doscmd.com param1 param2 etc
```

The /cmd= is where you list the actual DOS command, including any parameters the DOS command requires.

In this case, you'd add d:\anydir\doscmd.com to the *Allowed DOS Applications* list -- just the full-path program name itself, not its command-line parameters. Entries on this list are not case sensitive.

When You Need It: If Full Control Internet is running and has disabled launching DOS applications the DOS command won't run if you launch it in the usual way, even if it is listed on the *Allowed DOS Applications* list -- fcRunApp must actually run the DOS command. This is because fcRunApp tells Full Control Internet that a DOS command is about to be run, and the name of that command. Only if the command is on the *Allowed DOS Applications* list will Full Control Internet allow it to run. You can have as many fcRunApp shortcuts as you like, each running a different DOS command. If Full Control Internet isn't active when you run such a shortcut fcRunApp simply launches the DOS program.

Setting It Up: Here's an example. Let's say you want to allow users to run the DOS program c:\somedir\otherdir\list.com.

First create a shortcut to fcRunApp. Right-click on the shortcut and select Properties to display the Properties dialog. In this dialog, click on the Shortcut tab. In the middle of the screen is the Target line, which runs fcRunApp. It probably looks something like this:

```
    "C:\Program Files\Full Control\fcRunApp.exe"
```

Put your cursor at the end of that line and add

```
    /cmd=c:\somedir\otherdir\list.com
```

to the end of the line. Now the line looks like something like this:

```
    "C:\Program Files\Full Control\fcRunApp.exe"
```

```
/cmd=c:\somedir\otherdir\list.com
```

Depending on the program you're running, you may also want to set the shortcut's "start in" field to that DOS program's home directory. When it's set as you need it to be, click OK to save the shortcut.

Now you need to tell Full Control Internet that it's all right for fcRunApp to run list.com. Start Full Control Internet, go to the first tab of the Group Setup screen for the user who is allowed to run list.com and click the Allowed DOS Applications button. Up comes a list. Add the full path of the DOS program (c:\somedir\otherdir\list.com in this example) to the list.

What if you wanted to run a DOS app with parameters? For example, list.com is a file viewer -- what if you wanted to always view particular files? OK, in the shortcut's target line you might have:

```
    "C:\Program Files\Full Control\fcRunApp.exe"
/cmd=c:\somedir\otherdir\list.com myfile.txt otherfile.txt
another.txt
```

The parameters follow the command, just as you'd expect on a DOS command line.

When you list this as an Allowed DOS Application on the Access tab in Full Control Internet you only need to give the actual executable file name to the Allowed list (c:\somedir\otherdir\list.com in our example). That is, you don't list parameters there.

Applications Allowed To Run: On the Access tab, you can "Allow only those applications on the Managed Programs and Allowed Applications lists" to run. If you use this restriction, you must do one further step in order to launch an Allowed DOS Application through fcRunApp. To do this, click on the Allowed Window Titles button (on the Access tab) and give the titlebar text of the DOS program. The titlebar text appears at the very top of the window. For example, the titlebar text of the Full Control Internet helpfile is " Full Control Internet Help." (If your DOS application runs fullscreen, you can press Alt+Enter to toggle the program into windowed mode to see its title bar.)

Logoff And Shutdown Applets

Microsoft has documented a bug in Windows 98, and in NT using the same IE shell, which prevents it from re-reading certain settings from the registry when they are changed. Instead, Windows 98 uses its old cached settings still incorrectly held in memory.

On such computers, the Start button or desktop options don't clear when Full Control Internet exits, and you need to log off to get everything back in sync. If you are using the option on the Setup Settings tab to "reset the Windows interface on exit" you will not have this problem.

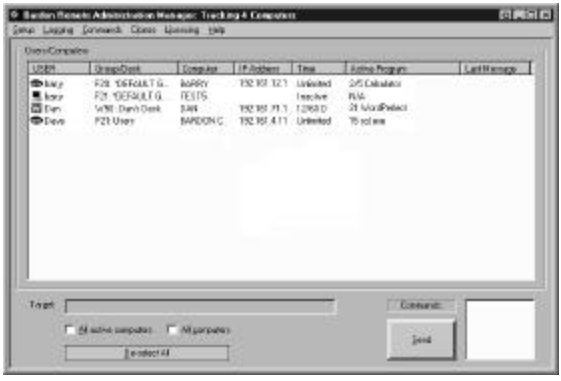
But what if your computer can't use this option, and the Start button's logoff item is itself hidden? In that case you can use the logoff.exe applet. Similarly, if you need to shut down the computer in this situation you can use the shutdown.exe applet.

These are installed into Full Control Internet's section of the Start menu so you will always have Logoff and Shutdown menu items. Don't worry, if Full Control Internet is running and you have restricted logoff/shutdown they first require a password.

Chapter 4

The Remote Administration Manager

Administration Manager Overview



With the Administration Manager you can manage all your WinU Internet and Full Control Internet computers from across your LAN or from anywhere on the Internet. See the Administration Manager Strategies section for ideas and pointers on this.

Briefly, you can reset time limits, list running programs, close programs, start new programs, modify the Registry, distribute software and files, set up and distribute clone-update settings, logoff any user, shut down any computer, save or restore a checkpoint, send a brief popup message, or generate various activity reports on the target remote computers.

The commands are set up on the Time Control screen, the Programs screen, the Registry screen, the Other Settings screen, and the Reports screen. Use the Commands menu to bring up these screens.

The Administration Manager can also enforce centralized time and access limits, and have Full Control Internet update itself using the Version Update menu item.

The remote stations can be running Full Control Internet or WinU Internet. The Administration Manager can be resized and its columns adjusted as needed. It remembers its columns, size and position from session to session.

Password Protection: If a licensed copy of WinU Internet or Full Control Internet is also installed on your administration computer, its setup password is required in order to use any Administration Manager feature which modifies the remote computers. To those without this password, the Administration manager is only a 'read-only' screen that cannot send commands to the connected computers. After the password is given, the Administration Manager won't ask

again for 15 minutes. If you want to re-lock the password security before the 15 minute period expires (perhaps so you can walk away from the computer) use the *Password Lock Now* item on the *Setup* menu. If a licensed copy is installed, both setup passwords are required.

Network Considerations: The Administration Manager can be run on any computer with an IP address that is visible to the client computers it will manage. Are your client computers on networks that use NAT (network address translation, or "masquerading")? NAT is a common networking technique whereby the IP addresses within the masqueraded network are not directly accessible to any "outside" computers. Because masqueraded computers are not visible to the Internet, they are more secure. Compare this to a computer with a static IP address, such as a web server or email gateway, which is directly visible over the Internet. There are many excellent and reliable tools to protect such computers (firewalls, scanners, etc.) but an *invisible* computer is inherently more secure than a *visible* computer.

The desktop clients can be on either static IP computers or masqueraded computers. The question here is whether the Administration Manager itself can also be run from a masqueraded computer, or whether it must be on a computer with a static IP address. The answer depends on whether your client computers are on one LAN segment, or spread across multiple LANs.

One LAN: If all your client computers are on the same masqueraded subnet, the Administration Manager can be on a masqueraded computer on that same subnet, making the Administration Manager's computer invisible to the Internet, yet completely visible to the computers it oversees.

Multiple LANs: What if your managed computers aren't all on the same masqueraded subnet? Perhaps you have multiple facilities, each with its own LAN, and you want to manage all your computers from one Administration Manager in a central location. In this case, the Administration Manager must be on a computer with a static IP address so it will be visible to all your client computers, on all your LANs.

Setting Up The Client Computers: In most cases, nothing special must be done to set up the remote computers to be managed by the Administration Manager. Simply install the client software onto these computers in a way that gets the port and IP address of the Administration Manager computer into the client's Remote Management tab, so the client knows where to look for its Administration Manager. One easy way to do this is to install with a clone file containing the management information, along with (might as well) any other clone settings you'd like the client computer to have. If a client loses contact with the Administration Manager, it continues to protect the computer with the last clone settings it was given.

The Main Screen List: The *Users/Computers* list on the main screen shows information about who is and isn't logged on, and the current state of those users and computers. The columns list the current logged-on user's name, the

currently active WinU Internet desktop or Full Control Internet group, the name of the computer, time settings, whether this computer is currently active, and whether a password is available for this computer. Click any column header to sort the list by that column; click it again to reverse-sort. The columns are:

User: This is the current logged-on user's name, as given at the Windows logon screen. The displayed icon shows whether the user is inactive, active in WinU Internet, or active in Full Control Internet.

Group/Desk: This is the active Full Control Internet group or WinU Internet desktop. If this is a Full Control Internet computer, the line starts with "F" and the Full Control Internet version number, then lists the currently active group. If this is a WinU Internet computer, the line starts with "W" and the WinU Internet version number, then lists the currently active WinU Internet desktop.

Computer: The name of this computer, for example as set on the Identification tab of the Network control panel applet.

IP Address: The IP address of this computer.

Time: The cumulative time limits currently in effect. It indicates "unlimited" if there are no cumulative time limits for this Group/Desk. Otherwise it is listed as the number of minutes used, the number of minutes total, and a flag for the time mode: T (total, never reset), D (minutes per day), W (minutes per week), or L (minutes per logon). If this user/computer is not logged on, it is listed as "Inactive" here, and the left-edge computer icon is dark.

Active Program: If this user/computer is currently logged on, this column shows the current active application (foreground window) and the current number of minutes since that application was started. Time-limited managed programs also show the total time allowed, separated by a slash. If it is a Full Control Internet managed program or a program launched from a WinU Internet button, the name shown here is the name you gave when you set up that program or button, otherwise it is the actual executable filename. If you have allowed your users to launch multiple instances of Full Control Internet managed applications, remember that these are all considered together for time-control purposes, so the current minutes shown are the number of minutes since the first instance was launched.

Last Message: As messages are exchanged between the Administration Manager and the client computers, this field is updated.

Commands: You can send commands to any listed computer. To do this, first choose target computers from the Administration Manager's main screen list. To target multiple computers, use your mouse or the Control and Shift keys just as in Explorer to select multiple list entries, or check the "all computers" or "all active computers" box. Next, use the Commands menu. As you add each command, a brief reminder is added to the Commands list. You can clear a command by selecting it on the reminder list, then using the Command menu option to *Delete*

Selected Commands. (Of course, you can also go back into that option's *Command* screen and change it there.) Click the *Send Now* button to queue the command for sending. Commands are actually sent when the client computer next contacts the Administration Manager, which it does every minute or so.

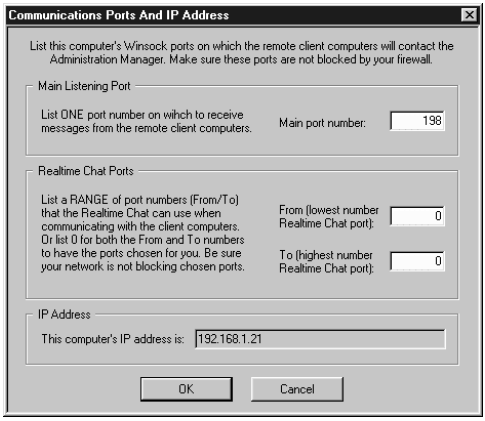
Centralized time and access limits: To enforce centralized time and access limits, check the "server-based time/logon management" box on the Access tab of the Group Setup screen. The Administration Manager will save the time of that group's users and restore it to the remote computer when those users log on later. For example, let's say a group gives its users 60 minutes per day, and a member is active for 20 minutes at Computer 1, then logs off. When that user logs on to Computer 2, the Administration Manager will reset Computer 2 so it has only 40 minutes remaining. The Administration Manager will also make sure that members of this group can only log on to one computer at a time.

Menu Items: The Administration Manager's menu can specify various settings.

Setup Menu Overview

This menu is used to specify basic configuration options.

Setup Menu: *Communications Ports And IP Address*



Use the Communication Ports and IP Address dialog to list this computer's Winsock ports on which the remote client computers will contact the Administration Manager. Make sure these ports are not blocked by your firewall.

Main Listening Port: This is the Winsock listening port on which the client computers will contact the Remote Administration Manager.

Realtime Chat Ports: A realtime chat session is a typed conversation between the administrator at the Remote Administration Manager computer and a user at one of the client computers (see Realtime Chat). Like all other computer-to-computer communication, it sends messages to a port and IP address. If your firewall is set to restrict such communication to a specific range of port numbers, list that range here; there must be at least two ports available. Or, if all ports are open and available for this, leave the *From* and the *To* ports set at 0 to have the port number chosen for you.

IP Address: For your convenience, the IP address of this computer is listed here as well. This is the IP address at which the client computers will contact the Remote Administration Manager.

Setup Menu: *Allowed Connections*

Use the Allowed Connections dialog to provide a security checklist which identifies every client computer which is allowed to contact this Remote Administration Manager. Providing this list makes for greater security because connection attempts from other IP addresses are ignored.

Give the IP address for each allowed computer. In addition, for extra security, you can provide the computer name which must also match.

If a connection is refused, the IP address and computer name of that computer is logged and (if set) an alert is sent. The administrator can look in the event log for refused connections to see if any of them should be listed here as allowed.

If no listings are given here, any client computer can contact the Remote Administration Manager. Their messages are accepted as long as the other security checks are satisfied.

Read List From File: For mass-input of Allowed Connections they can be read in from a file. Allowed connections are listed one per line. The file's lines can have the IP address and computer name, separated by a comma:

111.222.333.444,computername

Or the file's lines can be just the IP address:

111.222.333.444

There should be no spaces in the IP address. Spaces within the computername are allowed, but not leading or trailing spaces. It is acceptable if some lines have a computername and some do not.

Setup Menu: *Delete Selected Users/Computers*

Choosing this menu item will remove any selected users/computers from the

main list. This can be used, for example, to clean off inactive users/computers that won't ever again become active

---

Setup Menu: *Show Inactive Users/Computers*

Choosing this menu item will toggle whether a user/computer listing continue to display after that user logs off.

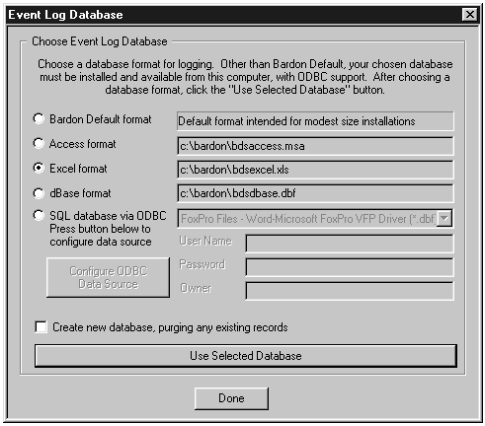
Setup Menu: *Password Lock Now*

If a licensed copy of WinU Internet or Full Control Internet is also installed on your administration computer, its setup password is required in order to use any Administration Manager feature which modifies the remote computers. To those without this password, the Administration Manager is only a 'read-only' screen that cannot send commands to the connected computers. After the password is given, the Administration Manager won't ask again for 15 minutes. If you want to re-lock the password security before the 15 minute period expires (perhaps so you can walk away from the computer) use *Password Lock Now.*

Logging Menu Overview

Options for saving and using event-log data, reports, and Alerts.

Logging Menu: *Event Log Database Format*



On this screen, select the database to which events should be logged. Events are sent from the client computers to the Remote Administration Manager to be logged into the central event log database. Events can be logged in many database formats: Access, Excel, dBase, or any installed format that supports ODBC connectivity. Third party tools can generally handle large volumes of data, and they often include advanced report generation tools that can be very useful. There is also a Bardon Default format suitable for modest size installations.

Bardon Default format: If no third-party database (Access, Excel, etc) is desired or installed, the events can be logged to Bardon's own default format, a basic

database with reasonable, though limited, capabilities. This format is acceptable for modest size installations. Larger facilities should use another format which is designed for large volumes of data.

Access / Excel / dBase format: Most current versions of Windows include the Jet database engine. With this, databases can be created in Access, Excel, and dBase formats even if the actual program is not installed on the computer. However, the actual program is required in order to view the database.

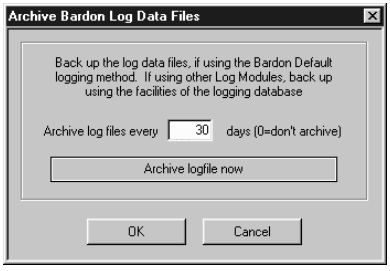
SQL database via ODBC: This option allows you to use virtually any installed SQL database that supports ODBC connectivity. Events will be logged to that database. After choosing this option, you must first use the *Configure ODBC Data Source* button to choose a target database and add a new data source. After doing this you can select that data source in the dropdown list. If your data source requires a User Name, Password, or Owner, fill in those fields on this screen. If this is a new database you must check the box to *Create new database, purging any existing records.* Most SQL databases will require that the logged-in user have permission to create and modify tables in this database.

Create new database, purging any existing records: If checked, clicking the *Use Selected Database* button will clear any existing database records from the selected database. This option must be selected when creating a new database to tell the Remote Administration Manager to create the necessary tables and indexes.

Use Selected Database: After clicking on a radio button to choose a database format, you must then click the *Use Selected Database* button to confirm the change and set up that database for use.

Done: Exit from this screen.

Logging Menu: *Archive The Event Log*

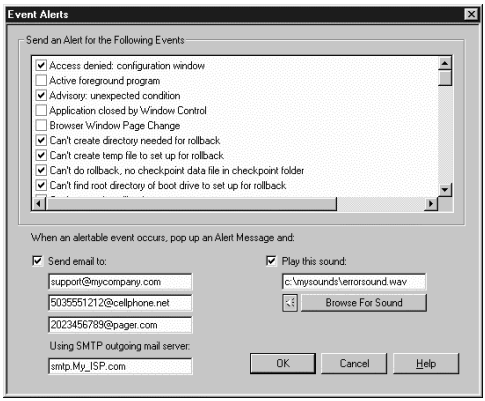


Events can be logged in many database formats, including the Bardon Default format. Use this feature to back up the event log if using the Bardon Default logging method, when it is desired to archive the event log.

The current bdslog.dpb and bdslog.dpi will be renamed to YYYY-MM-DD_hhmm_bdslog.dpb and YYYY-MM-DD_hhmm_bdslog.dpi (where YYYY-MM-DD_hhmm is the current date and time), and new, empty event log files will be created. The archived event log files will be in the same folder as the originals. You can move them from there to another location if you prefer.

Logging Menu: *Set Event Alerts*

Check the events for which you want alerts displayed. When the Administration Manager logs an alertable event, if that event's box is checked it will also be displayed in the Alert Messages dialog.



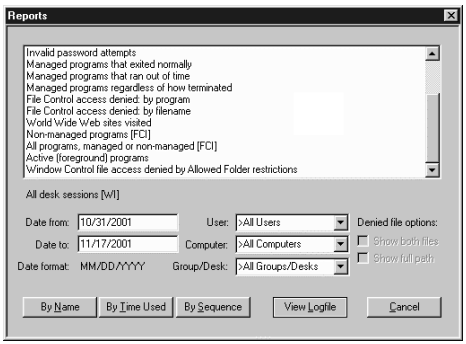
In addition to being listed in the Alert Messages dialog, alerts can also generate a sound on the Administration Manager computer.

Alerts can also trigger an email. You can send the alert email to as many as three separate email addresses. To do this, give the target email address(es) and the SMTP server through which to send the email. You can send to any email address. In addition to traditional desktop computers, many cell phones and pagers can accept a short email message.

Logging Menu: *Show Alerts Window*

Use this menu item to display the Alerts window. The Remote Administration Manager also automatically displays this window when there are alerts which must be presented to the administrator. It displays one alert per line. Lines that are no longer needed can be deleted. The setup password is required to delete such lines.

Logging Menu: *Run Reports*



Full Control Internet can generate a number of built-in reports which show activity on the remote computers. All reports are generated from the Event Log Database that was selected on the Logging menu. For modest-sized installations, the Bardon Default format works well, but for larger installations you will probably want to use one of the other logging options, which can log to Access, Excel, or SQL databases. Whichever logging option is chosen, reports can be run directly from this Administration Manager screen, or the logfile

can be analyzed in its native format. For example, if logging to an Access database you can use Access itself to generate reports, or third party tools that read Access databases. The Log File Format page describes the column layout of the event log.

A report can be targeted by choosing a particular date-from, date-to, user name, computer name, and/or Full Control Internet Group or WinU Internet Desk. A blank search criterion matches all possible entries.

Most of these reports are applicable to a remote computer running either WinU Internet or Full Control Internet. However, a few reports are specific to one or the other. These reports have the target program [WI or FCI] as part of the report description line.

The reports are displayed in a pop-up screen from the Administration Manager. They can be scrolled, selected, copied to the clipboard, or saved to a file.

A selected report's data can be viewed in up to three ways: by *Name*, by *Time Used*, and by *Sequence.* However, not all views are applicable to all reports. If a view is not applicable to a chosen report, its button is disabled. Within each selected view of a report, data can be displayed in a text list, or in a pie-chart graph.

To keep the pie chart readable, only the "top ten" items in the list are shown. In addition, any zero-length items are ignored by the pie chart. However, such items are available in the text list. When the pie-chart graph is visible, the data elements being graphed are shown in text form in the box below the graph.

When viewing by *Name*, the listed items (users, programs, whatever) are sorted in alphabetical order. When viewing by *Time Used*, the listed items are sorted by the amount of time each one took. In either case, if an item has multiple entries, for example, a program that was launched more than once, all its times are added together, and the number shown is the total amount of time the program was run.

When viewing by *Sequence*, items are sorted by the point in time at which they occurred. All items are listed individually; nothing is added together, and the "top ten" items in the pie chart are the ten most recent events.

After a report and a view are selected, the output screen displays that report. This screen can be resized if necessary. Grab an edge and pull to make the screen larger; the report view will grow as well, making more of its data visible.

Reports can be printed or saved to file. Click the output screen's File button to write the report to a file. Click the Print button to print the current report. Click the Font button to select the printed report's font. The Font button does not change the screen font, just the printer font.

Logging DOS Programs: Windows runs DOS programs in a "DOS box" virtual

environment. The actual running program for all DOS applications is the same. Therefore, to log meaningful information when a non-managed DOS program is running, Full Control Internet logs the titlebar text of the DOS box instead of the filename of the running program, which would otherwise be identical in every case.

Available Reports: The available reports are as follows.

All desk sessions [WUI]: This report shows the amount of minutes used by all WinU Internet desks. It tracks events when the user exits a desk voluntarily, or when WinU Internet terminates that desk for timeout reasons.

All user logons [FCI]: This report shows the amount of minutes used by all Full Control Internet users. It tracks events when the user exits a session voluntarily, or when Full Control Internet terminates that user for timeout reasons.

All computer sessions: This report totals the two previous reports to show the amount of minutes used by all users or desks, whether under WinU Internet or Full Control Internet. It tracks events when the user exits a session or desk voluntarily, or when WinU Internet or Full Control Internet terminates that user or desk for timeout reasons.

Sessions that ran out of time: This report shows the ending time and amount of minutes when the user or desk ran out of time. It tracks events when WinU Internet or Full Control Internet terminates that user or desk for timeout reasons. This could be due to the cumulative time limits or the start of a blockout period. In all cases the user is given an advance warning message. This report tracks instances in which this warning was ignored and the user was forcibly terminated.

Password updates and maintenance: This report shows when managed-program passwords or the setup password were changed. It also shows any use of emergency passwords. Since such events take no time, the *Time Used* button is disabled.

Invalid password attempts: This report shows all instances in which an incorrect password was submitted. Since such events take no time, the *Time Used* button is disabled.

Managed programs that exited normally: This report shows all managed programs which were exited normally by the user.

Managed programs that ran out of time: This report shows all managed programs which were forcibly terminated because of time limits.

Managed programs regardless of how terminated: This report totals the two previous reports to show all managed programs that were run by any user or desk, whether they were exited normally or forcibly terminated. It tracks user or desk timeout, application timeout, and voluntary user exit.

File Control access denied: by program: This report lists access-denied events generated for all users, sorted by the program which requested the denied file. The same data is shown in both *File Control access denied* reports. The only difference is how the data is sorted. See below for important details on using the "access denied" reports.

File Control access denied: by filename: This report lists access-denied events generated for all users, sorted by the name of the denied file. The same data is shown in both *File Control access denied* reports. The only difference is how the data is sorted. See below for important details on using the "access denied" reports.

World Wide Web sites visited: This report lists each World Wide Web page by URL and title, and shows the amount of time spent at that website. Note that checking *Session and user events* on the Event Log tab causes browser information to be logged as well, for the *Active (foreground) program* report, though not with quite as much detail as the *World Wide Web sites visited* report.

Non-managed programs [FCI]: This report shows all non-managed programs which were run by any Full Control Internet user. Non-managed programs are those not listed on the Managed Programs tab.

All programs, managed or non-managed [FCI]: This report shows all programs run by any Full Control Internet user, whether managed or non-managed. Managed programs are those listed on the Managed Programs tab. Note that WinU Internet usage can be viewed with the managed programs reports, above.

Active (foreground) programs: This report lists the active foreground program as it changes through the session. It is a good way to see exactly what windows the user accessed, in what order, and for how long. It includes the title bar text of the foreground window, so it will show as a separate entry each webpage visited, Word document edited, etc.

Window Control file access denied by Allowed Folder restrictions: On the Window Control tab you might have listed Allowed Folders for some of the Target Title windows. Doing so prevents users from opening or saving files to unauthorized locations, since access to locations other than the Allowed Folders is not permitted. If the user attempts such unauthorized access, WinU Internet or Full Control Internet denies access and logs the attempt. See below for important details on using the "access denied" reports.

Computer licensed or unlicensed: This report shows all occasions when the computer was licensed or unlicensed by a clonefile, through the Remote Administration Manager distributing licenses, or directly at that computer by the administrator in Setup Mode.

Computer entered Setup Mode: This report shows all occasions when the computer was placed into Setup Mode.

Application or system component access denied: This report shows all occasions when access to an application program or system component was denied to the user. These include (when disallowed) Control Panel, Printers screen, Recycle Bin, Network Neighborhood, Find, Run, disallowed Explorer configuration screens, disallowed options launched by the Windows key, applications not on the Managed Programs, Allowed Files, or Allowed Titles list, timed-out programs, password-protected programs where an invalid password was given, browsers viewing unauthorized websites or local files, or Task Manager.

Checkpoint saved successfully: This report shows all occasions when the computer successfully saved a checkpoint.

Rollback restored successfully: This report shows all occasions when the computer successfully completed a rollback.

Window Control applied: This report shows all occasions when the computer applied a listed Window Control to a window that appeared.

Unable to initialize event log database: This report shows all occasions when the Remote Administration Manager was unable to start the event log database you chose on the Event Log Database tab.

Failed to send alert message to listed email address: When flagging an Event Alert, the Remote Administration Manager can send an email. This report shows all occasions when the Remote Administration Manager was unable to send such an email.

Rejected TCP/IP connection by unauthorized client: If you have set up to allow connections from only specific IP addresses, other IP addresses are not allowed to connect. These rejected connections are logged. These may be overlooked IP addresses that you may want to add, or they could be unauthorized access attempts from outside your system.

Number of simultaneous connected clients exceeds maximum allowed: Each managed client connects regularly to the Remote Administration Manager for updates. After checking for updates, it disconnects until the next time. This report shows all occasions when more than the maximum number try to connect simultaneously. This should be a very rare occurrence.

Keystrokes typed by the user: Keystroke logging can be activated for all windows from the Event Log tab, or for a particular window through Window Control.

Using the "access denied" reports: If you have given file/folder names on the File Control or the Window Control tab, and if you have checked the "file and folder access denied" box on the Event Log tab, you can use the "access denied" reports to list files/folders which were requested but not allowed.

When using the "access denied" reports, two filenames are involved: the name of

the program which requested the file, and the name of the file requested. You can view a report sorted by either the filename of the program which requested the file, or the filename which it requested. In either case, the report's lines can include just the reported file, or both the reported file and the other file. If using just the reported file, the results will be aggregated as tightly as possible, which can be easier to read. If using both files, the additional level of detail may cause useful patterns to emerge.

Additionally, when using the "access denied" reports, you can include the full path of each listed filename, or just list the actual filename without its path. The first way is more detailed. The second is sometimes easier to read.

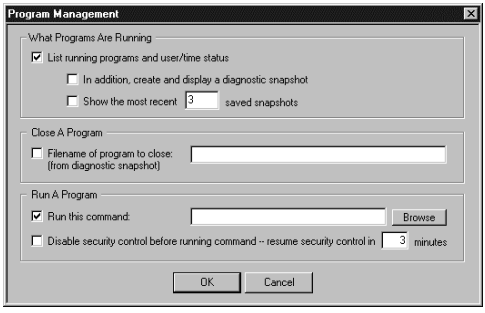
These reports are especially useful when your File Control or Window Control restrictions cause a program to behave oddly. You know that it needs access to a file you've restricted, but which file is it? These reports will list all the files it tried to access, but couldn't. Look at the list, identify the problem file, then modify the File Control or Window Control restrictions as needed. If the problem is with a File Control restriction, you might add an exception. If the problem is with the Window Control allowed-folder list, you might add the problem file to the Allowed Folders list on the Window Control tab. (Despite the name, "Allowed Folders" can list files as well as folders.)

When the Windows operating system itself requests a file, the requesting program is listed as KERNEL32. However, DOS boxes are also part of the operating system, so the program requesting files accessed by DOS programs is also listed as KERNEL32.

Commands Menu Overview

This menu allows you to send commands to the managed client computers. The commands are sent to the computers that are selected (highlighted) on the main Administration Manager screen's list.

Commands Menu: *Program Management*



Options are available from the Programs screen which can list all active programs, close currently running programs, or launch new programs.

What Programs Are Running: Select this to request the status of the target computer(s). In a few seconds a popup will appear which lists all displayed windows, user information, etc.

If you like, it can also list diagnostic snapshot information on all programs, visible or hidden, including those that don't list themselves in the Ctrl+Alt+Del "Close Programs" screen. You can save this information to a file, or select any desired text with your mouse and press Ctrl+C to copy it to the clipboard.

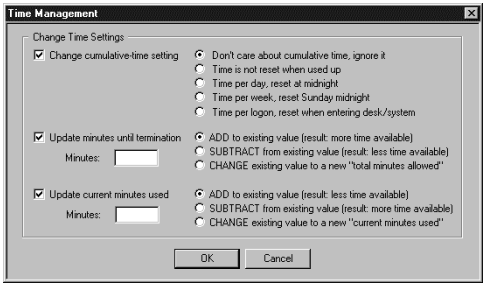
Close A Program: Give the full-path filename of the program you want to close on the target computer. A diagnostic snapshot can show a list of programs currently running on that computer, or you can type in the full-path filename manually.

Run A Program: This is the command-line to run on each selected remote computer. You can run installers, maintenance programs, batch files, or anything else, from your central administration location. They are executed on the target computer. You can even use this to copy files to the target computer by running the DOS command COPY to copy files from a visible shared server folder to a location on your target computer.

Disable security control before running command: You may have to relax the computer's security restrictions to allow the command to run. For example, if your command runs a batch file you'll need to allow DOS programs. Or perhaps you've set up the Allowed Applications so only certain programs will run. Check this box to temporarily allow anything to run on the target computer. If the target computer uses System Stabilization mode, the System Stabilization list will be regenerated on that computer when security control resumes.

Resume security control in N minutes: If you temporarily allow anything to run, how many minutes until the security control is put back into effect? If the target computer uses System Stabilization mode, the System Stabilization list will be regenerated on that computer when security control resumes.

Commands Menu: *Time Management*



The main Administration Manager screen displays the time settings for the currently active WinU Internet desktop or Full Control Internet user and group. Options are available from the Administration Manager's Time Management screen which can adjust these time settings.

Change cumulative-time setting: These are the same choices available on the Time Control tab of the Group Setup dialog.

Update minutes until termination: If you increase the minutes until termination, there will be more time available; if you decrease this, there will be less time available. This change is permanent. It sets the cumulative time Minutes Allowed value, which is saved from session to session. You can *add* minutes to

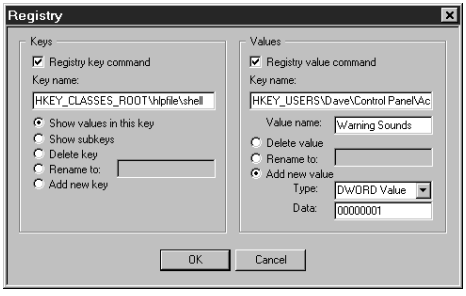
the current value, *subtract* minutes from it, or *change* it to a new value entirely. It can be set from zero (meaning: no time is available) to 9999999 minutes (approximately 19 years).

Update current minutes used: If you increase the current minutes used, there will be less time available; if you decrease the current minutes used, there will be more time available. This change is temporary. It sets the cumulative time Minutes Used value, which is reset whenever required by the current cumulative-time setting (daily, weekly, or at logon). You can *add* minutes to the current value, *subtract* minutes from it, or *change* it to a new value entirely. It can be set from zero (meaning: no time has been used up) to the current "total minutes allowed" value (meaning: all time has been used up). Changing this value will not affect the current-used minutes value used for logging and reports.

If you update the total minutes allowed or the current minutes used, remember that these two values work together. If the total allowed ends up lower than the current used, there will be no time available on the user. Perhaps the best strategy is to either *add* to the total minutes allowed, or *subtract* from the current minutes used. Though the Administration Manager does let you *change* these to specific fixed numbers, be very careful when you *change* one value. Take the other value into consideration or you could end up with a timed-out user!

One way to use the Administration Manager might be to set the public computer to "no time left" when Full Control Internet starts. When a customer comes in, use the Administration Manager to send that machine as many minutes as the customer has paid for (either by adding to *total minutes allowed* or subtracting from the *current minutes used*). Full Control Internet will warn the customer in advance of expiration. You then use the Administration Manager to send the machine more time.

Commands Menu: *Registry Management*



Options are available from the Registry screen which allow you to view and modify registry settings on the remote computer, even if that computer has not been set up for remote registry editing over the LAN. It is intended for occasional use, especially in emergencies.

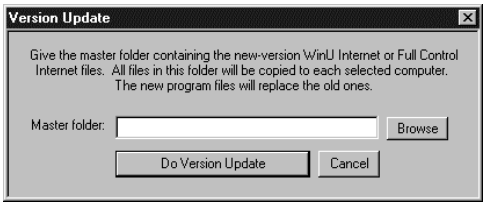
Use the left side to work with registry keys. First, type in the name of the key you want to work with. The name is typed exactly as it might appear in standard tools like Regedit or Regedt32. You can display all values in your chosen key, or all subkeys immediately under your chosen key. You can delete or rename a key, or add a new key.

Use the right side to work with values within keys. First, type in the name of the

key you want to work with, and the desired value under that key. You can delete or rename a value, or add a new value. To add a value, choose its type from the list and give its data. A new DWORD value must contain exactly eight hexadecimal digits; use leading zeros as necessary. A new Binary value consists of pairs of hexadecimal digits separated by commas. A new String value consists of plain text. Because this tool is intended for occasional and emergency use, there is a size limit for String and Binary values of about 175 characters.

Warning: don't modify the registry unless you know what you are doing! The registry holds the computer's basic configuration settings. Windows provides virtually no error checking for registry modifications, making the registry a remarkably easy component to break.

Commands Menu: *Version Update*



How can you remotely mass-install a new-version update of WinU Internet or Full Control Internet on all your managed computers? You can't simply run the installer, because WinU Internet or Full Control Internet is already running, and it might not allow an installer to run on that computer. Also, Windows won't let you overwrite a running program.

To do this, use the Version Update option.

First, copy all the new-version files to a folder visible to the Administration Manager. Make sure these are the only files in the directory.

Next, select the computers you want to update from the Administration Manager's main list of users and computers.

Then click the Version Update item in the Administration Manager's menu. This will display the Version Update dialog. Give the name of the directory holding the new-version files

Finally, click the "Do Version Update" button. This sends all the files in the chosen folder to all selected computers. The computers will update themselves. All the old files will be overwritten with the new files. NT/2000/XP ".sys" files will be copied to the target computer's designated Drivers directory (this user must have permission to do so - see below). After updating, WinU Internet or Full Control Internet will be restarted. This will run the new version from the updated files.

NT/2000/XP Drivers: To update the Bardon NT/2000/XP driver files, the

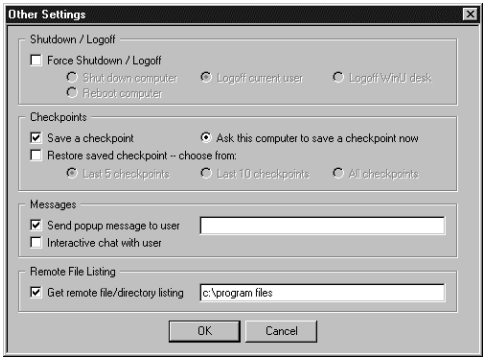
currently logged on user must have permission to copy files to NT/2000/XP's System32\Drivers directory and overwrite files already there. Members of NT/2000/XP's "Administrators" group generally have this privilege; other groups may also, depending on your NT/2000/XP setup. If these files need to be updated remotely, arrange for the user to be logged in to an account with appropriate privileges when you do the Version Update.

Driver files are easily identified by their ".sys" file extension (bardon1.sys, bardon2.sys). There are very few of these in Bardon software, and they rarely change. If the files are unchanged, it makes no difference that the drivers cannot be updated in the current user's security context. Have their dates and/or sizes changed from the previous version?

Another way to update is to simply uninstall Full Control Internet, then reinstall it. This is easily done using any of the remote-management "quiet-mode install" options listed in the Installing And Uninstalling section. If you supply a clone data file with the re-install, no settings will be lost. The uninstall and install must be done while the computer is logged on to an Administrator account.

Commands Menu: *Other Settings*

Options are available from the Other Settings screen which allow you to logoff or shut down a computer, ask it to save or restore a checkpoint, send a popup message or start an interactive chat session with the user, or show a directory listing.



Shutdown / Logoff: *Logoff Current User* will log off from this Windows session. *Logoff WinU Internet Desk* will immediately set the target computer to the default WinU Internet desktop. *Shutdown* and *Reboot* act the same on some computers. For those computers that can handle the distinction, both choices are provided here.

Checkpoints: Select this to ask the computer to save or restore a checkpoint. This assumes that the target computer has been set up to do so, with a checkpoint folder specified and files in the checkpoint files list. A default location for the checkpoint folder is set up when WinU Internet or Full Control Internet is first installed. If restoring a checkpoint, you will see a list of checkpoints from which you can choose the one you want to restore. When restoring, you can restore all files in that checkpoint, or just some of the files.

Send popup message to user: Often, in conjunction with taking some action you'll want to send a popup text message to the affected Full Control Internet computer

users on the network. To do this, type your brief message (150 characters or less) here. The message will pop up on the user's computer before any other specified action is done. So, for example, the user will get to read the attached message before the computer is shut down. Those big-font popup messages time out in two minutes, so if no user is at that particular computer, there will be very little delay.

Interactive chat with user: Launch an interactive real-time chat session with the user on the remote computer. A separate chat session is launched for each selected computer. The administrator can initiate a chat session at any time. The user can initiate a chat session if the administrator has allowed the Chat item to be displayed on the tray icon menu.

Remote File Listing: Use this to list the files and subdirectories contained in a particular folder on the target computer. The results are displayed in alphabetical order.

Commands Menu: *File Transfer*

This feature brings up one of two screens, depending on whether you have chosen to send files from the Remote Administration Manager to one or more clients, or from one or more clients to the Administration Manager.

Using this feature is straightforward. First, select the file that you want to transfer. Wildcards * and ? can be used freely. If wildcards are used, and more than one file matches, then all matching files will be sent. If you give a folder name, all files in that folder will be transferred.

Then select the target directory to which you want to copy the files. When you click OK they will be sent. If the target directory does not exist, it will be created.

To avoid name conflicts, when sending files from one or more client computers to Administration Manager the sending computer's name will be prepended to the copied filename when the file is received by Administration Manager.

Commands Menu: *Send Commands Later*

Commands can be temporarily held, and sent at a future time. Use the *Commands* menu item *Send Command Later* to send a command at a future time. The current pending commands will be held until that time, and then sent.

Commands Menu: *Delete Selected Commands*

You can clear one or more commands from the Commands list by selecting them, then using this option. The Commands list is at the bottom of the main Administration Manager screen. It shows a short reminder of each command you have selected for sending, but which has not yet actually been sent.

Clones Menu Overview

With this menu you can create, modify, and distribute clone settings.

Clones Menu: *WinU Internet Clone Settings*
Clones Menu: *Full Control Internet Clone Settings*

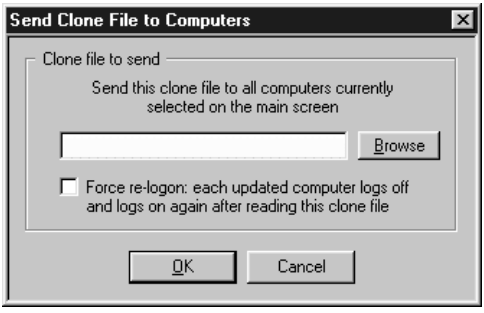
This launches WinU Internet or Full Control Internet in Administration Manager Setup Mode. This allows you to specify settings right from the Administration Manager, then save them as a clone to update your client computers. You specify these settings in the same way as is done in regular Setup Mode in WinU Internet or Full Control Internet. However, these settings changes are for the Administration Manager and clone creation only, they will not be used by WinU Internet or Full Control Internet when they are actually run on this computer.

To use Administration Manager Setup Mode WinU Internet or Full Control Internet must be installed on the Administration Manager computer.

Clones Menu*: Default Clone Files*

Set the default WinU Internet or Full Control Internet clone file that will be sent to a managed client if their local data is invalid or corrupted.

Clones Menu*: Send A Clone File*



With this screen you can send a new clone data file with updated settings to all selected computers. Settings are put into effect immediately. If any of your changed settings require a re-logon, check the *Force re-logon* box.

Be sure to send only WinU Internet clones to WinU Internet, and Full Control Internet clones to Full Control Internet. One easy way to do this is to sort the main screen by the Group/Desk

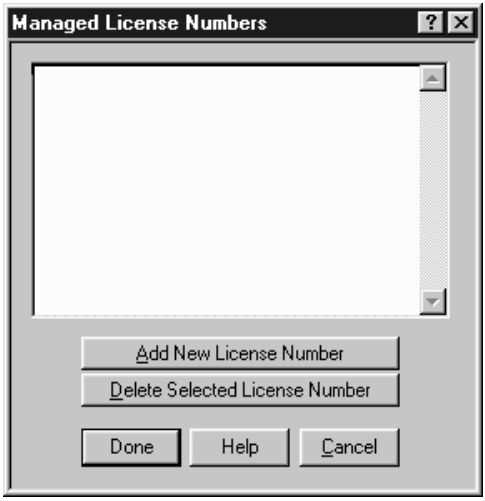
column. This will put all the Full Control Internet computers together, and all the WinU Internet computers together, making it easy to select the right computers for this clone data file.

WinU 5 and Full Control 2 clone data files cannot be sent. However they can be converted into WinU Internet or Full Control Internet clone files and then sent. This is done using the *Import Clone File* button on the Remote Management tab.

Licensing Menu Overview

There are only two items on the Licensing menu.

Licensing Menu: *Managed License Numbers*



To distribute licenses to your connected computers, enter them on this screen. The license(s) will be sent to the client computers as they connect to the Remote Administration Manager.

Licenses can also be entered directly into the client software, either in Setup Mode or by importing a clone file into that computer. If the client reports to the Remote Administration Manager a valid license number that is not yet listed in this screen, it will be added to the list.

Licenses are for a number of computers ("seats") and could be temporary licenses which expire after a certain period of time. Multiple license numbers allow you to run the total of their licensed seats. Licenses can be deleted, but it is not really necessary to delete temporary licenses from this screen because after a license expires, the Remote Administration Manager will simply remove it from the list by itself.

Licensing Menu: *Show License Number*

Select one computer from the main screen list, then click this to display the license number being used by that computer.

Appendix A

Miscellaneous

Log File Format

Events are logged to your chosen database format. This can be the Bardon Default logging format or to the format of various third party tools.

Bardon Default logging format: The Bardon Default format is intended for use in modest installations where other formats are not available and the size of the collected data is expected to be small. For this reason, its format contains less columns than are used in third party databases (see below).

In the Bardon Default format, the event log consists of a data file *bdslog.dpb* and an index file *bdslog.dpi*. Both files start with an eight byte header consisting of "DPB1" followed by the log file version. For example, if the version is 0, the header on both the data file and index file would be DPB10000. Following the header are the event records. Each event generates a separate record (row) in the log data file. Each record (row) consists of 11 cells (columns) of data. A cell consists of:

- The column number as a 4 byte int. There are 11 columns so this can be from 0 to 10.
- The length in bytes of the succeeding data as a 4 byte int (supports the variable length data field)
- The cell's actual data, as a variable length field

The 11 cells (columns) in each data row are as follows:

- 1: A C time_t (4 bytes) indicating the date and time of the event
- 2: A word (2 bytes) indicating the event type. High byte is event group, low byte is event subset number. A listing of event types is given below.
- 3: The logged-on user name as a null terminated string
- 4: The computer name as a null terminated string
- 5: The group or desk name as a null terminated string
- 6: An int (4 bytes) indicating the group or desk number
- 7: An int (4 bytes) usually indicating the number of minutes into this session, see below for exceptions
- 8: A null terminated text title which names the event, as given in the table below
- 9: A null terminated text string giving details of the event

- 10: Where needed, a second null terminated text string giving more details of the event. Most events do not use this field.
- 11: An int (4 bytes) with the numeric event flag indicating if the event is alertable (bit 1 is set) and which component generated the event: Administration Manager (bit 5 is set), Full Control Internet (bit 6 is set), or WinU Internet (bit 7 is set)

The Bardon Default format log index starts with the eight byte header. This is followed by one index entry for each data-file entry. These are fixed length records in the following format:

- A word (2 bytes) with the same event code as is used in Cell 2 of the log data file.
- An int (4 bytes) with the same date and time as is used in Cell 1 of the log data file.
- A ULARGE_INTEGER (8 bytes) indicating the offset of that particular event entry in the log data file.

You can view the event log using the built-in capabilities of the Remote Administration Manager.

Third party database logging format: In third party databases (Access, Excel, SQL, etc.) the 'full' format is used. The 14 cells (columns) in each data row are as follows:

- 1: A SQL datetime indicating the date and time of the event (same data as #2 but different format)
- 2: A C time_t indicating the date and time of the event (same data as #1 but different format)
- 3: Event group, indicating the general type of event. This is the high byte of the event code given in the table below.
- 4: Event number, indicating the specific event in its group. This is the low byte of the event code given in the table below.
- 5: Six-letter event mnemonic, as given in the table below
- 6: The logged-on user name
- 7: The computer name
- 8: The group or desk name
- 9: The group or desk number
- 10: Usually, the number of minutes into this session, see below for exceptions
- 11: A text title which names the event, as given in the table below
- 12: A text string giving details of the event
- 13: Where needed, a second text string giving more details of the event. Most events do not use this field.
- 14: A numeric event flag indicating if the event is alertable (bit 1 is set) and which component generated the event: Administration Manager (bit 5 is set), Full Control Internet (bit 6 is set), or WinU Internet (bit 7 is set)

You can view the event log using a third party tool which can read files of that type.

Events: Each record (row) logs one event, with its event code in hexadecimal. In the row entries for most of these events, the *Minutes* column (Cell 7 in the Bardon format, cell 10 elsewhere) lists the session time when an event took place. Exceptions to this are:

- Browser events (type 0x13xx) which list the amount of time that page was displayed
- Application events (type 0x16xx, 0x17xx, or 0x18xx) which list the number of minutes that application has been running
- Foreground Window events (type 0x09xx) which list the number of minutes the window has been the active foreground application

The table below lists all events which might be logged:

Event#	Mnemonic	Title
0x0101	ADVSRY	Advisory: general unexpected condition
0x0201	AMUNLC	Computer unlicensed by Administration Manager
0x0202	AMLICN	Computer licensed by Administration Manager
0x0203	PCUNLC	Computer unlicensed by client computer
0x0204	PCLICN	Computer licensed directly by client computer
0x0205	CLUNLC	Computer unlicensed by clonefile
0x0206	CLLICN	Computer licensed by clonefile
0x0207	AMILNR	Expired license number removed from AMI list
0x0301	BADPWA	Invalid password for drag-drop file program add
0x0301	BADPWC	Invalid password for Ctrl+Alt+Del
0x0302	BADPWM	Invalid password for setup mode
0x0303	BADPWP	Invalid password for program launch
0x0304	BADPWV	Invalid password for reset mode
0x0305	BADPWX	Invalid password for client app exit
0x0306	BADPWK	Invalid password for desk deletion
0x0307	BADPWJ	Invalid password for copying desks
0x0308	BADPWI	Invalid password for adding desks
0x0309	BADPWE	Invalid password for running Explorer
0x0401	CHPWDE	Emergency password was used to gain access
0x0402	CHPWDP	Managed program password changed
0x0403	BADPWL	Invalid password for desk logon
0x0403	CHPWDD	WinU Internet desk password changed
0x0403	CHPWDS	Setup Mode password changed
0x0404	BADPWH	Invalid password for help
0x0501	ENDWUD	Exit from WinU Internet desk
0x0502	HIDDSK	Attempt to logon to disallowed hidden desk
0x0503	BDCKPT	Could not save desk time checkpoint
0x0601	ENDSES	End of session
0x0701	ERRPSH	Error calling system/group/desk setup screen
0x0801	SETUPE	Enter setup mode
0x0802	SETUPX	Exit setup mode
0x0901	FGPRGM	Active foreground program
0x0a01	DENACC	Application access denied
0x0b01	FILACC	File access denied
0x0b02	FILACD	File access denied by Allowed Folder restrictions
0x0c01	KEYTYP	Keystrokes typed by user
0x0c02	KEYTYN	New forground window for keystrokes typed by user
0x0d01	RBNOCF	Can't do rollback, required data not in checkpoint

0x0d02	RBNOTD	Can't create directory needed for rollback
0x0d03	RBNOBF	Can't create temp file to set up for rollback
0x0d04	RBRBOK	Rollback completed successfully
0x0d05	RBNORT	Can't find root dir of boot drive to do rollback
0x0d06	RBERR1	Can't set up for rollback generally
0x0d07	RBBOOT	Computer is rebooting to complete the rollback
0x0d09	RBCPOK	Checkpoint saved successfully
0x0e01	STRANM	Non-managed program started
0x0e02	STRAMG	Managed program started
0x0f03	STRSES	Start of session
0x1001	TBMOVE	User tried to move taskbar: not allowed
0x1002	TBTERM	Session terminated: taskbar move not allowed
0x1003	TBWARN	User warned: taskbar move not allowed
0x1101	TIMUSR	Session/desk terminated: user timeout
0x1102	TIMADD	Removed the timeout lock from session/desk
0x1201	USRNMW	Logon name of new user received by AdminMgr
0x1301	WCCAPP	Application closed by Window Control
0x1302	WCCDLG	Dialog closed by Window Control
0x1303	WCCSOF	Window soft-closed by Window Control
0x1304	WCKEYS	Keystrokes sent by Window Control
0x1305	WCSDIR	Directory location set by Window Control
0x1306	WCSFIL	Filename set by Window Control
0x1307	WCDONO	Window found by Window Control (do nothing)
0x1401	BRWNEW	New web browser window
0x1402	BRWEXI	Web browser window closed
0x1403	BRWPGC	Web browser page changed
0x1404	BRWGOB	PageGoBack message sent to web browser
0x1405	BRWQUI	Close-window message sent to browser
0x1501	SNDFER	Unable to send a file
0x1502	SNDFNF	Requested file not found
0x1503	SNDFCR	Error creating file to receive
0x1701	APPEXD	Exited from a DOS application
0x1702	APPEXW	Exited from a Windows application
0x1801	ENDMAU	Managed program terminated by user
0x1802	ENDMAT	Managed program terminated by program/user timeout
0x1901	ENDANM	Non-managed program terminated

Used only by Administration Manager internally, not sent by the client:

0x3a01	AMNODB	Unable to initialize database
0x3a02	AMDBIT	Database initialized successfully
0x3b01	EMLERR	Email alert error
0x3c01	CONREJ	Attempted TCP/IP connection rejected
0x3d01	USMXEX	Number of clients exceeds max, closing socket
0x3d02	USMXBL	Number of clients now below max, reiniting socket
0x3d03	SOCERR	Error reiniting socket after connected clients falls below max

Software License And Warranty

SOFTWARE LICENSE AGREEMENT

IMPORTANT-READ CAREFULLY: THIS IS A LEGAL AGREEMENT BETWEEN YOU (AN INDIVIDUAL OR A SINGLE ENTITY) ("YOU" OR "LICENSEE") AND BARDON DATA SYSTEMS ("LICENSOR") PERTAINING TO THE SOFTWARE (AND/OR DOCUMENTATION WHICH MAY BE PROVIDED THEREWITH) YOU ARE ABOUT TO INSTALL, COPY, ACCESS OR OTHERWISE USE (THE "SOFTWARE"). LICENSOR LICENSES THE SOFTWARE TO YOU ONLY UPON THE EXPRESS CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS SOFTWARE LICENSE AGREEMENT (THE "AGREEMENT"). YOU SHOULD CAREFULLY READ THE FOLLOWING TERMS AND CONDITIONS BEFORE INSTALLING THE SOFTWARE. BY INSTALLING, COPYING, ACCESSING OR OTHERWISE USING THE SOFTWARE, YOU ACCEPT THESE TERMS AND CONDITIONS AND UNDERSTAND THAT THEY WILL BE LEGALLY BINDING ON YOU. IF YOU DO NOT AGREE TO THE TERMS, THEN LICENSOR IS UNWILLING TO LICENSE THE SOFTWARE TO YOU. IF YOU DO NOT AGREE WITH THE TERMS, OR DO NOT WANT THEM BINDING ON YOU, YOU MUST NOT INSTALL, ACCESS, OR COPY THE SOFTWARE.

1. Grant of License. The Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. Subject to the terms and conditions of this Agreement, including, but not limited to, Sections 2 and 1(c) herein, the Software is licensed, not sold, as follows:

a) "Test Drive" Evaluation. As to the pre-purchase evaluation version of the Software, Licensor hereby grants and you accept a non-exclusive license to run the Software for evaluation purposes for thirty (30) days. That is, you can run the Software for evaluation purposes on 30 different dates. These dates do not have to be consecutive calendar days. If you don't run the Software on a particular date, it doesn't count against your 30 days. After the trial period, you must either purchase the Software or remove it from your system. Anyone is welcome to distribute the "test-drive" evaluation version of the software, in its entirety as distributed with this file, subject to this Agreement's terms and these conditions: a) none of the files in this package may be modified or deleted; and b) distributors must stop distributing the Software immediately upon Licensor's request; and c) all proprietary notices, product branding, trademarks and similar notices and identifiers may not be altered, obfuscated or removed.

b) Purchased Licenses. Upon your purchase of the Software license, Licensor grants you and you accept a non-exclusive license to use one (1) copy of the software, on one (1) computer, and make one (1) copy of it for archival purposes. If your purchased license expressly allows you to use the Software on more than one (1) computer, your purchased license terms supercede the previous

sentence to govern the number of computers on which you can use the Software. For purposes of this section, "use" means loading the Software into RAM, as well as installation on a hard disk or other storage device.

c) Additional Restrictions. You may not install the purchased version of the Software onto a network server or in any other way make it available to more than one user at a time unless you have purchased an appropriate multi-user license; make copies of the Software other than one backup copy solely for archival purposes; sell, furnish, transmit, or give away the Software in exchange for any monetary payment, other software, or any other consideration whatsoever; or sublicense, rent, lease, or otherwise market the software. You may permanently transfer the Software to another licensee, provided, however, that you promptly give written notice of such transfer to Licensor and the new licensee agrees to be bound by this Agreement's terms and conditions.

d) Upgrades. An upgrade replaces a previous version and terminates your license to use the previous version. An upgrade does not provide an additional license. Upon upgrading you must cease using the previous version, and also ensure that it is not used by anybody else. Installing an upgrade indicates your agreement to the Software License and Warranty included with that upgrade.

e) Returns. The Software can be returned for refund within thirty (30) days of the purchase date, when accompanied by a return authorization number which has been obtained from Licensor. Shipping/handling fees are not refundable. A restocking fee may apply.

f) Technical Support. If you have purchased technical support from Licensor, such support only covers Licensor's products and not those of any third party. Should you request that Licensor provide diagnostic or other support services, and should such services show, in the sole opinion of Licensor, that the issues raised were not caused by Licensor's products, Licensor reserves the right to bill for, and you agree to compensate it for, its diagnostic or other support services at its then-current rate for third-party product support services. Licensor reserves the right to withhold technical support and other services from customers whose bills are past due.

g) Other Rights. All rights not expressly granted to you are hereby reserved by Licensor.

Unauthorized copying of the Software or failure to comply with the above restrictions, will result in automatic termination of this Agreement. Unauthorized copying or distribution of the Software constitutes copyright infringement and may be punishable in a federal criminal action by a fine of up to U.S. $250,000 and imprisonment up to five (5) years. In addition, federal civil remedies for copyright infringement allow for the recovery of actual damages based on the number of copies produced or statutory damages of up to U.S. $150,000 for willful copyright infringement.

2. Title and Copyright. It is hereby understood and agreed that as between

Licensor and you, Licensor is the owner of all rights, title and interest, including the copyright, to the Software recorded on the media on which the Software is furnished and all subsequent copies thereof, regardless of the media or form in which the Software or copies thereof may exist. Except as expressly provided herein, you do not acquire any rights to the Software through the purchase of licenses to the Software.

3. Term. This Agreement shall continue for as long as you use the Software licensed herein or until terminated by Licensor, whichever occurs first. Without prejudice to any other rights, this Agreement will terminate if you fail to comply with any of its terms or conditions. You agree, upon termination, to destroy all copies of all Software.

4. LIMITED WARRANTY. LICENSOR WARRANTS THAT THE SOFTWARE DISTRIBUTION DISK WILL REMAIN FREE FROM DEFECTS FOR NINETY (90) DAYS AFTER YOU HAVE RECEIVED THE SOFTWARE. IN THE EVENT OF A BREACH OF THIS WARRANTY, LICENSOR WILL, AT ITS OPTION, EITHER REPLACE THE DISK OR REFUND THE SOFTWARE PURCHASE PRICE. THE SOFTWARE IS FURNISHED "AS IS" AND WITH ALL FAULTS. LICENSOR DOES NOT WARRANT THAT THE SOFTWARE WILL FILL YOUR REQUIREMENTS; OR THAT THE SOFTWARE WILL OPERATE WITHOUT INTERRUPTIONS; OR THAT THE SOFTWARE IS FREE FROM ERRORS. LICENSOR DOES NOT WARRANT THAT THE SOFTWARE IS FAULT-TOLERANT. IT IS NOT INTENDED FOR USE IN ENVIRONMENTS REQUIRING FAIL-SAFE PERFORMANCE, SUCH AS NUCLEAR FACILITIES, AIR TRAFFIC CONTROL, OR LIFE SUPPORT EQUIPMENT, IN WHICH THE FAILURE OF THE SOFTWARE COULD LEAD DIRECTLY TO DEATH, INJURY, OR SEVERE PHYSICAL OR ENVIRONMENTAL DAMAGE. LICENSOR MAKES, AND YOU RECEIVE, NO OTHER WARRANTIES, EXPRESS, IMPLIED, STATUTORY, OR IN ANY COMMUNICATION WITH YOU. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, LICENSOR, ITS SUPPLIERS, AND EVERYONE ELSE INVOLVED IN THE CREATION, PRODUCTION OR DELIVERY OF THIS PRODUCT DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AND/OR ANY WARRANTY THAT OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE WITH REGARD TO THE SOFTWARE, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES. IF THE SOFTWARE WAS PURCHASED IN THE UNITED STATES, THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU SINCE SOME STATES DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES. IN ADDITION TO THE ABOVE WARRANTY RIGHTS, YOU MAY ALSO HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE. THE ENTIRE RISK ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE PRODUCT REMAINS WITH YOU.

5. LIMITATION OF LIABILITY. THE LIMITATION OF LIABILITY IS TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL

LICENSOR OR ITS SUPPLIERS BE LIABLE FOR DAMAGES, WHETHER ARISING IN CONTRACT OR TORT AND INCLUDING, BUT NOT LIMITED TO, ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR OTHER DATA, COST OF COVER, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR THE FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ACKNOWLEDGE THAT THE LICENSE FEE AMOUNT REFLECTS THIS ALLOCATION OF RISK. IN ANY CASE, LICENSOR'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS AGREEMENT SHALL BE LIMITED TO THIRTY PERCENT (30%) OF THE LICENSE FEE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

6. U.S. GOVERNMENT INFORMATION. The Software is provided with RESTRICTED RIGHTS. Use, duplication, or disclosure of the Software by the U.S. Government is subject to the restrictions set forth in DFARS 227.7202 and FAR 12.212 and 48 CFR 52.227-19 as applicable, and any successor regulations thereto. The manufacturer is Bardon Data Systems Inc., 1164 Solano Ave #415, Albany CA 94706.

7. Indemnification. In the event the Software is modified (including, but not limited to any changes to the Software's initialization file[s]) or is installed or used contrary to this Agreement or Licensor's warnings, instructions, or recommendations, you agree to defend and indemnify and hold Licensor harmless from and against all claims of any kind for any expense, injury, loss, or damage arising out of, or connected with, or resulting from the use of this software.

8. Equitable Relief. You acknowledge that, at the time this Agreement is entered, it would be impossible or inadequate to measure and calculate all of Licensor's damages for the breach of certain provisions of this Agreement and that it would require a court of competent jurisdiction to ascertain Licensor's damages. Accordingly, if you breach or threaten to breach any of your obligations, other than payment when due, Licensor shall be entitled, without showing or proving any actual damage sustained, to a stipulated temporary restraining order, and shall thereafter be entitled to apply for a preliminary injunction, permanent injunction, and/or order compelling specific performance, to prevent the breach of your obligations under this Agreement. Nothing in this Agreement shall be interpreted as prohibiting Licensor from pursuing or obtaining any other remedies as otherwise available to it for such actual or threatened breach, including recovery of damages.

9. Governing Law/Jurisdiction. This Agreement shall be governed by and construed under the laws of the State of California without reference to principles of conflicts of laws. Any action or proceeding brought by either party against the

other arising out of or related to this agreement shall be resolved exclusively in the appropriate state court in Alameda County, California or federal court for the Northern District of California, U.S.A. You consent to exclusive jurisdiction in such venue and expressly waive any objection to same.

10. General. This Agreement sets forth the entire agreement and understanding of the parties relating to the subject matter herein and merges and supersedes all prior agreements, writings, commitments, discussions and understandings between them. No modification of or amendment to this Agreement, nor any waiver of any rights under this Agreement, shall be effective unless in writing signed by the parties. If any term of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, then this Agreement, including all of the remaining terms, will remain in full force and effect as if such invalid or unenforceable term had never been included. This Agreement shall be construed within its fair meaning and no inference shall be drawn against the drafting Party in interpreting this Agreement.

Notices

VERSION:
Full Control Internet version 1.3

SYSTEM REQUIREMENTS:
Windows 95, 98, ME, NT, 2000, or XP

TECHNICAL SUPPORT:
Email: support@bardon.com
Web: www.bardon.com
Phone: 510-526-8470
Fax: 510-526-1271
Telephone support is available during normal business hours, 9 to 5 weekdays California time.

NOTICES:

Index