



# **Full Control**

**Security Access Control  
For Windows 95/98/NT**

**Installing, Using  
and Mastering**

**Bardon Data Systems**

---

# **Full Control**

**Security Access Control  
For Windows 95/98/NT**

**Installing, Using  
and Mastering  
Full Control 2**

**Bardon Data Systems**

# Full Control: Security Access Control For Windows 95/98/NT Installing, Using and Mastering

## Contents

### 1. Getting Started

Introduction	3
Installing Full Control	6
Quick Start	10
The Setup Password	11
Setup Mode	12
Emergency Passwords	12
Using the Windows Logon Screen	13

### 2. A Tour Of Full Control

Taskbar Tray Icon	15
The Administration Screen	16
Users Screen	17
Groups Screen	18
System Setup Dialog	19
<i>Security Settings Tab</i>	19
<i>Event Log Tab</i>	24
<i>Reports Tab</i>	27
<i>Remote Management Tab</i>	33
<i>Rollback Tab</i>	35
Group Setup Dialog	37
<i>Access Tab</i>	37
<i>Managed Programs Tab</i>	41
<i>Interface Tab</i>	44
<i>Input Control Tab</i>	45
<i>Time Control Tab</i>	49
<i>Window Control Tab</i>	50
<i>File Control Tab</i>	53
Advanced Program Settings	56

### **3. Security And Administration**

System Administration With Full Control	59
Security Considerations	60
How To Clone A Computer	61
Per-Computer Display Restrictions	63
Reset Mode	64
Using Internet Software	66

### **4. Companion Software**

Remote Administration Manager	67
<i>Time Control screen</i>	71
<i>Programs screen</i>	72
<i>Registry screen</i>	73
<i>Other Settings screen</i>	74
<i>Reports screen</i>	75
<i>Version Update screen</i>	76
License Meter Manager	77
The fcRunApp Utility	79
Logoff Applet	80

### **Appendix A: File Formats**

Log File Formats	81
License Manager File Format	84

### **Appendix B: Miscellaneous**

Software License and Warranty	85
Frequently Asked Questions	87
Notices	88
Index	89



# Getting Started

---

## Introduction

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

Full Control is a complete Windows 95/98/NT systems management solution. It includes security access control, time limits, logging, web-browser tracking, remote administration, and many flexible configuration options. Full Control provides effective, reliable access management and remote administration while still allowing use of the regular Windows desktop. With Full Control, businesses can let employees use authorized applications, yet monitor all activities and prevent them from accessing or installing other programs ... stores, schools, and libraries can allow public access to their computers, yet safeguard computers against tampering ... and parents can control which programs and websites their children use.

**Access Control:** Full Control provides reliable security coverage, even in Safe Mode. It lets you specify exactly what programs can be run, by whom, and for how long -- even communications programs for the Internet or online services. It allows full access to authorized software, 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 or folders. Full Control can also control keyboard and mouse activity, boot-time behavior, shutdown options, file-save directories, and more.

**Web browser and application oversight:** Full Control monitors all World Wide Web browser activity by name, location, and time, providing a complete audit trail of all Web activity. It also logs all software usage, attempts to access locked files or folders, 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.

**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, have you ever thought, "if only I could roll back the system configuration to before I installed that program"? Well, you can. The Rollback feature allows you to undo any unintended or malicious system configuration changes when misguided users, flawed applications or incomplete uninstallers make a mess of your computer. Configuration checkpoints are saved on your schedule, and can be restored even if Windows won't run.

**Remote administration:** Full Control's system administration capabilities can maintain any size setup, from a single home PC to multi-computer networked installations. All networked computers can be managed from one central location. This includes the ability to remotely monitor, update, logoff, shut down, reboot or reconfigure Full Control stations. Full Control also includes network-based license metering. This lets you purchase only a few licensed copies of some program, yet allow that program to be run from any station on your network.

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 distributions across the network or do any other mass-manipulation chores.

**Logon validation:** Full Control can validate users at logon, even on laptops and other stand-alone Windows computers -- no network or NT server is required. Unlike the standard-issue Windows logon screen, which is easily bypassed by pressing Escape or in other ways, Full Control ensures that only valid users can log on. If you do have a network server, Full Control can coordinate with it and ensure that no user can log on, even just onto the local computer, unless validated by your server.

**What it looks like:** By default, Full Control 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.

**What's included:** Full Control includes everything you need in one purchase: client-side monitoring software, central administration utilities, event logging, built-in reports, license metering, and all the other utilities.

**Setup and configuration:** Click the tray icon to access the setup options. If the tray icon is hidden, type the hotkey or run Full Control's companion Reset program to access the setup options. These options are grouped by functional area onto two tabbed screens, Group Setup and System Setup.

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. If the Windows logon name is not listed, Full Control uses its Default Group settings. Or you can set up Full Control so unknown users are not allowed to log on at all.

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

**Installing:** To install Full Control, run the program *install.exe* that comes with Full Control. It will ask you which folder you would like to install into and what Start button group name you prefer. The installer will not put anything into any folder other than the one you specify, other than NT drivers which are installed into NT's "drivers" folder. It will not change any system files, other than the Registry (per Microsoft standards). In NT, the logged-on user must have Administrator rights for the install to be successful.

**Administration Tools:** In a regular interactive install you will be asked whether you want to install the helpfile and remote administration tools, *metermgr.exe* and *adminmgr.exe*. In an unattended automated install, they will be installed only if you use the */admin* parameter (see below for more on automated installation). These tools should only be installed to the administrator's computer, so it can monitor and control the other computers.

**Default Group and Default User:** The first time you run Full Control after installing, Full Control creates a Default Group with a few managed programs and other settings. It also creates a Default User who is in this Default Group. This lets you use Full Control and get a feel for what it can do.

**Cloning While Installing:** If you have set up one computer with the settings you want, you can transfer these settings to another computer while installing. To do this, export a clone file from the first computer. Copy that clone file into the same directory as the installer. When the installer runs, it will look for a clone file named *clonefc.bds* (the standard default name for clone files) in its own directory. The updated settings are put into effect the next time Full Control starts. For more information, read about [How To Clone A Computer](#).

**Version Upgrade:** If the computer has settings from an earlier version of Full Control, these settings are automatically imported into this new version. Full Control 1.x kept its settings per-user, not per-group. To mimic this arrangement, this version creates a separate group for each old-version user. Each such group will have one user, and the group name will be the same as the user name.

**Upgrade Licensing:** When the old-version settings are automatically imported, it will be an unlicensed version even if the old version was licensed, because the old-version licensing won't apply to the upgrade. This is easily addressed by arranging for upgrade licensing, then distributing the new license key in a clonefile with the actual software upgrade. To do this, first install this new version on one computer. The old-version settings will be automatically imported into that computer. Or load in an old-version clonefile, that works too. Next, enter your new-version license number and create a clone file from that computer as described above. Include it with the install. This will bring in the new license data along with the settings.

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

**Uninstalling:** Full Control's uninstaller is listed with Full Control's icons on the Start menu. It can also be run from the Start menu's Add/Remove Programs list. Please note that to cleanly uninstall, the uninstaller must be used. It is not sufficient to simply delete the Full Control 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 can't be uninstalled while it is running. In NT, 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 installer can be run in an unattended automated mode which requires no user input. The following command-line parameters are used to set this up:

<code>/auto</code>	installer runs in automated mode
<code>/addstart</code>	icons will be added to the Start menu
<code>/admin</code>	also install the helpfile, Meter Manager, Administration Manager
<code>/targetdir=</code>	full path to the folder into which files should be installed
<code>/pausecmd=secs.cmd</code>	seconds to wait, then command to run after install
<code>/defaultinstall=</code>	if used (unlikely), set to LIGHT, MEDIUM, or STRONG

Example: `\\server\c\masterdir\install.exe /auto /addstart /targetdir=c:\somedir\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 runs perfectly well without being listed on the Start menu.

The /admin parameter tells the installer to also include the remote administration tools (metermgr.exe and adminmgr.exe). These administration tools should only be installed to the administrator's computer, so it can monitor and control the other computers.

The /targetdir item is also optional. If it is not given, Full Control will be installed into the default directory, which is the \Program Files\Full Control 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.

The /defaultinstall= parameter is provided for completeness; it will rarely be used. When doing a regular (interactive) install, and a clone file is not provided as part of that install, the installer asks how restrictive to make the initial default settings: LIGHT, MEDIUM, or STRONG. It's unlikely that an automated unattended remote install will not include a clone file with initial settings, but if you choose to do this, you can use the /defaultinstall parameter to specify the level of the initial "generic" settings.

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 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 on each user's computer. First, copy the files on the Full Control 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\fc.exe \\server\c\masterdir\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\fcsetup\install.exe /auto /addstart /targetdir=c:\Full Control
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 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 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.

---

## Quick Start

**Full Control In A Nutshell:** Full Control monitors every user logon and every running program, and can log all activity. If you have set up a particular application as a managed program, Full Control will impose the time limits, password protection, and other control you have specified for it. Non-managed programs can be completely disallowed if desired, so they won't run. Full Control 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. The logged-on user can have overall restrictions and time limits as well. Each user is assigned to a group, and each group can have a different set of restrictions. Full Control looks at the name of the current user (that is, the user name given at the regular Windows logon screen). If that user is listed in a group, the group's restrictions, time limits, and managed programs are applied. If that user name is not found, Full Control imposes its Default Group restrictions.

Full Control 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 logoff, shutdown, and system administration options. If the tray icon is hidden, press the hotkey or run Full Control'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 configure Full Control computers over a network.

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

- Decide if unknown users can log on, or if users must be "known" in order to use the computer. Use the first tab of the System Setup dialog to indicate if users must be validated at startup and what validation criteria will be applied.
- If you want to provide each user with different Full Control 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.) This step is optional, because even if you don't use the logon screen at all, Full Control will work

perfectly well. It will then use its Default Group settings for all users, providing them the permissions and restrictions you have listed as the default.

- Configure systemwide settings with the Administration screen's System Setup dialog. Modify the settings in the first two tabs (Security Settings and Event Log) as needed. The third tab, Reports, displays usage reports and graphs. Use the fourth tab (Remote Management) to set up network-based Full Control 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 in a group, and when that user logs on, that group's settings are put into effect. Full Control comes preconfigured with a number of groups. Or, create new groups using the Administration screen, then specify the group's settings with the Group Setup screen. Add managed applications and configure the new group's restrictions and time limits to your liking. 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. You can also copy managed programs from one group to another, or to all groups at once.
- 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.

**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 every computer at your site. This is especially easy if the computers are networked, but a clone configuration can be replicated on other computers even if a network is not available. A clone file is also a good way of backing up your work. Also, if you will be cloning this computer's Full Control configuration onto other computers, think about which managed programs and users will be monitored on what computers. These can be specified in a number of ways as discussed in the Display Restrictions section.

---

## The Setup Password

The first time you start Full Control, 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 Security Settings tab of the System Setup dialog. Security experts recommend changing your passwords regularly.

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


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

The pre-purchase evaluation version of Full Control 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

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 won't interfere with any program. This makes it easy for the system administrator to modify Full Control 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's companion Reset program.

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

---

## Emergency Passwords

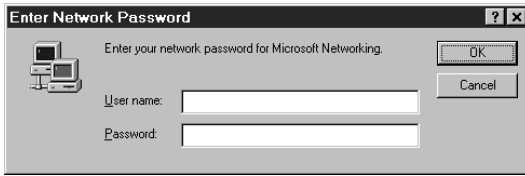
Forgot your setup password? Don't worry, you're not locked out. Each Full Control system has built-in "emergency password" capability. Emergency passwords are secured so that they cannot be used in an unauthorized manner. If you are in a situation where you need one, contact Bardon Data Systems and,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

The "test-drive" version of Full Control 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 restarts. After purchase, this "back door" security hole is no longer active.

---

## Using the Windows Logon Screen



When you boot your computer, do you see a Windows 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 when Full Control starts. If that name matches a username listed in Full Control, that user's set of restrictions and controls will be put into place for this logon.

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

If the logon is valid (or if you're not using logon validation) but does not match any name in Full Control, the Default User restrictions and controls will be put into place for this logon. So 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.

But if you want to use this feature, here are a few ways to tell Windows to display its "log on by user name" screen when Windows starts.

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 configuration files for each user can eat up quite a bit of disk space. For this reason, Full Control 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 with settings under that logon name.

A "back door" way to enable the logon screen is to delete the \*.PWL (Windows

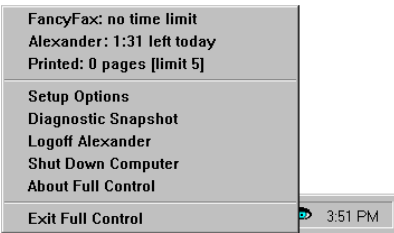
password list) file saved under a user's name. Use Explorer to search for PWL files, and delete the ones named for the necessary users. The next time that username is given at logon, Windows will show its logon screen. At that point you can tell Windows to keep showing that screen at logon. Note, though, that other kinds of passwords are stored in PWL files, for example those for Dial-Up Networking. So if you use this technique, these other passwords will have to be given 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, you can use the password-protected Logoff option on the  Full Control 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.

# A Tour Of Full Control

---

## Taskbar Tray Icon



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

Clicking on the tray icon pops up a menu.

The top few 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 Administration Screen. 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 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.

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

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

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

---

## The Administration Screen



This administration screen is displayed after you click on the Full Control 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's companion Reset program to access the setup options. The setup password is required. Full Control 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.

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

**About:** Full Control version 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.

**System Setup:** This displays the System Setup screen. This dialog has five tabs:

*Security Settings, Event Log, Reports, 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 knows about, and the Group settings to be applied when that user logs on. If an unlisted user logs on (assuming this is allowed) the Default Group settings are applied for that user's session.

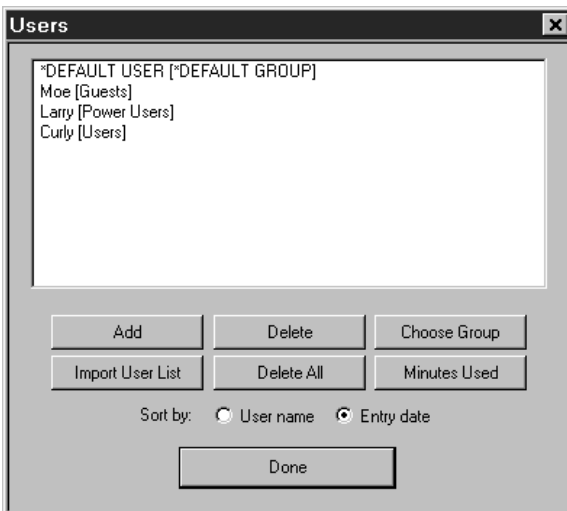
**Reports:** This menu item provides a shortcut to the Reports tab of the System Setup dialog. The administrator can see a wide range of usage and activity reports.

**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 and clears all its access controls.

---

## Users Screen



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

The names shown in this list are the same user names which the user types 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 uses the settings you have given for that user's group. Full Control can perform logon validation in a

number of ways. One way can deny access to any user not named on this list. But if that validation option isn't being used, and no name matches or the user cancels out of the Windows logon screen, Full Control 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. To move a user to another group, highlight that user on the list, click the Choose Group button, and choose the new group. You can select more than one user before you click the Choose Group button. In that case, all the selected users will be moved to the new group.

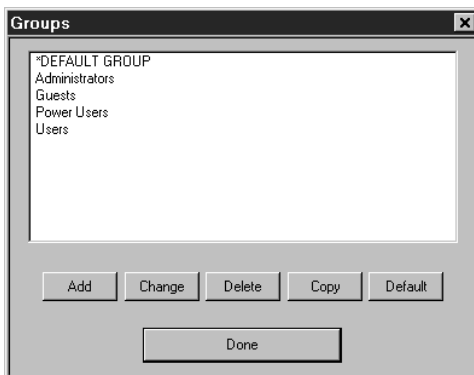
Use the Add button to add one new user at a time. You can also add a group of users by importing a file-based user list. To do this, click the Import User List button and give the name of the file. This is a plain-text file. The user names can be delimited in any way that works for you. They can be separated by commas, or by tabs, or on separate lines, or in CSV (quoted comma-delimited) format. In other words, the delimiter between user names can be a comma, a tab, a double-quote (not a single-quote!), a newline, or any combination of these. Multiple delimiters together (for example the quote-comma-quote between items in a CSV list) are treated as a single delimiter. New users added from an import list are placed initially in the Default Group.

The list can be displayed alphabetically by user name, or in the entry-date order. Sorting by entry date can be very handy. Let's say you import a list of users from a file, and you want all the new users to be added to the Power Users group. Click the radio button to sort by entry date, so all the new users will all be together at the bottom of the list. Then select all the new users, perhaps by "lasso-ing" them with your mouse. Click the Choose Group button, select the desired group, and you're done.

If you want the Windows logon screen to be displayed when Windows starts, set this using the Network applet of the Windows Control Panel.

---

## Groups Screen



The Groups screen is displayed by clicking the Groups button on the Administration menu. A "group" is a set of settings. You set up a group's settings as you prefer, then assign users to that group. When that user logs on, the group's settings are put into effect.

With this screen, administrators can select the group settings to modify. 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:

**Add:** To add a new group to the list, click the Add button. A new group will be created with default settings. The new group's setup screen will be displayed.

**Change:** To change the settings for an existing group, double-click the name on the list, or select that group from the list and click the Change button. That group's setup screen will be displayed.

**Delete:** To delete a group from the list, select that group from the list and click the Delete button. That group will be removed from the list.

**Copy:** To make a copy of a group's settings, select that group from the list and click the Copy button. That group's settings will be copied. 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:** To copy any group's settings into the Default Group's slot, select that group from the list and click the Default button. That group's settings will be copied to the Default Group. 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:

**Security Settings:** systemwide security and preference options

**Event Log:** logfile usage and tracking options

**Reports:** view and print usage reports and graphs

**Remote Management:** network-based configuration control

**Rollback:** save and restore important system configuration files

---

### *Security Settings Tab*

This tab of the System Setup screen is where you give the computer name, password, boot-time options, and other systemwide security settings.

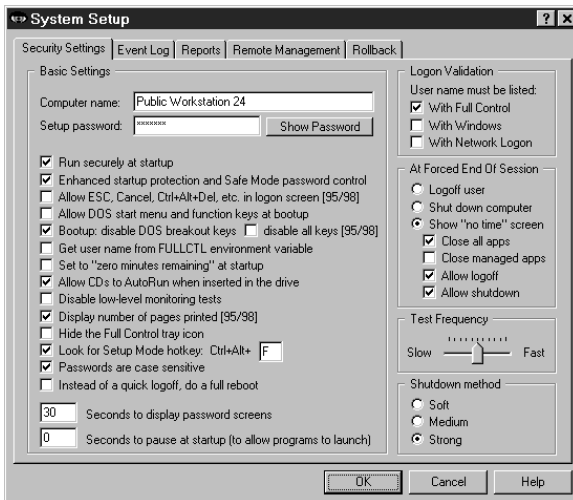
**Computer Name:** The computer name is used in event records, which are saved in the logfile. If you are administering a number of computers, give them each a unique name to help keep your records organized. If your computer doesn't already have a name (most do), the name defaults to *Full Control Computer* plus a

string of numbers, designed so that it is very likely to be a unique name in your environment.

**Setup Password:** This is the administrator password. Like all Full Control passwords, it is initially displayed with asterisks. To see the actual password text, use the Show Password button.

**Other Options:** These options let you further fine-tune Full Control's behavior. They are:

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

Allow ESC, Cancel Ctrl+Alt+Del, etc. in logon screen [95/98]: Unless this box is checked, Full Control disables the Escape key and Cancel button in logon data-entry screens (it allows Escape and Cancel in simple message boxes). 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 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" or "With Windows", or if you haven't checked any of the three logon validation boxes. This option is ignored under NT, 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. 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 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, this option immediately closes the Boot Loader menu by automatically selecting the default choice.

Bootup: disable DOS breakout keys / disable all keys: In Windows 95/98, DOS programs 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 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 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 because in NT, DOS does not load before Windows.

Get user name from FULLCTL environment variable: At startup, Full Control looks for the logon name of the current user. As described above, this name can be validated to control logon access. If there are Full Control settings under this user's name, they are set into place. If not, Full Control uses its Default User settings. But if your network or logon procedure is not fully Windows-aware, and does not place the user's logon name in the standard place, Full Control 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.


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 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.

In addition to checking this box, you must also set the Cumulative Time mode on the Time Control tab to a mode other than *Don't care about cumulative time*. Many people use *Time per logon* for this. Also on that tab, set the *Total minutes allowed* to the maximum amount of "time credit" that that the system can hold at any one time. Many people use a large number like 720 minutes (12 hours).

Allow CDs to AutoRun when inserted in the drive: Standard-issue Windows behavior is that when a CD-ROM is placed in the drive, its designated program runs automatically. Do you want to allow users to launch programs in this way?

Disable low-level monitoring: Full Control 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.

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

Look for Setup Mode hotkey: If this box is checked, Full Control will ask for the Setup Mode password when the designated hotkey is pressed. If the password is given, Full Control 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 to hide the tray icon or the entire taskbar. Note that the hotkey isn't recognized if your current active program is a DOS application.

Passwords are case sensitive: Should passwords be considered 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.

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 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 will wait that many seconds before activating its

security oversight.

**Logon Validation:** When Full Control 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 will logoff Windows. This is a useful feature if you don't have centralized network-based logon validation (through Netware, NT, 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*, 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 and Full Control starts.

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

With Full Control: To log on, the user must give a logon name which is listed on the Choose User screen. If this is checked and the user gives an unlisted name, Full Control logs off Windows. If the user hits Escape or otherwise cancels the Windows logon process, no name is given so (again) Full Control 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 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, which does not allow invalid logons.

With Network Logon: If you have a network with a Netware or NT 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 computer, because on such machines even if the logon fails the network may not prevent access to the local computer. This option will work with NT 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 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 ensures that this is done in a safe way.

**At Forced End Of Session:** Full Control can force a session to end for a number of reasons: user time limits, blockout periods, or a remote command sent across

the network 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 if you want the option to send more time to this computer with the Administration Manager), should Full Control 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 or shut down the computer? Set these options here to suit your preferences.

What if you choose the shutdown or logoff option, and you set Full Control to always "run securely at startup" (see above), and your system runs out of time? That is, if Full Control 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 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's popup menu, then choose the menu's Setup Mode option. If the tray icon is hidden, use the hotkey or run Full Control'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.

**Test Frequency:** How often should Full Control monitor for security violations? Testing more often will provide better security, but the extra overhead may slow down your computer. Testing less often will free the computer to perform other tasks faster. At the slow end it tests about every four seconds.

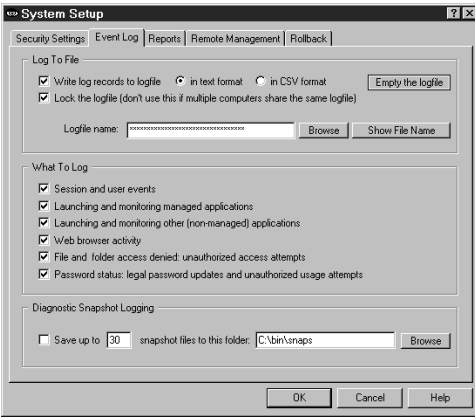
**Shutdown Method:** There are three ways that Full Control can shut down the computer. The most secure method is labeled here as *Strong*. It forces other programs to exit and guarantees a secure shutdown. However, some computers hang at shutdown with the *Strong* method. If yours is one of them, try the *Medium* or *Soft* methods. In the *Medium* method, Full Control "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 then steps back and waits for Windows to handle it all.

---

## *Event Log Tab*

This tab is where you set up logging to file and indicate what events you want to log. Events can be logged in "human-readable" format, or in CSV (comma separated values) format suitable for importing into a spreadsheet or database. Actually, neither format is particularly readable, which is why Full Control features built-in reports. Most of these reports use the logfile as their raw data.

**Web Browser Monitor:** The Full Control Web Browser Monitor lets you log all the websites that are visited while Full Control is active. It's a handy way to see what sites are being accessed, and for how long. To use this feature, set up for logging and check the box labeled *web browser activity*.



**Lock The Logfile:** It's generally a good idea to lock the logfile because a locked logfile cannot be moved, changed, or deleted while Full Control is running. However, don't lock the logfile if it is used by more than one computer. Different computers can share the same logfile, but in general this is not as useful as having separate logfiles for each computer. For one thing, you cannot lock the logfile if it is shared, because only one computer can access a locked logfile. For another thing, a shared logfile can

provide only aggregate reports (on all your logged computers taken together), where separate logfiles can provide reports on individual computers, or they can be merged to provide aggregate reports.

**Per-Computer Logfile Names:** You can use the word %COMPUTERNAME% as part of the logfile name. If you do, Full Control will build the logfile name at runtime using the current computer name as a component. You can also use the words %USERNAME% (user name given through current network or Windows logon), %GROUPNAME% (that user's Full Control group) and %CURRTIME% (a unique number based on the current time) here. For example, let's say you have named the logfile \\server\C\logs%COMPUTERNAME%.log.txt in this tab. Then let's say you clone this computer and distribute the clone setup over the network to dynamically update three computers named Moe, Larry, and Curly. Moe will then save its logfile data to \\server\C\logs\Moelog.txt, Larry will save to \\server\C\logs\Larrylog.txt, and Curly to \\server\C\logs\Curlylog.txt.

**What To Log:** Check the events you want logged. For basic logging, check *Session and user events*, *Launching and monitoring managed applications*, *Launching and monitoring other (non-managed) applications*, *Password status*, and perhaps *Web browser activity*. If you aren't using Full Control's File Control feature, it's unnecessary to check the *File and folder access denied* box.

You can log these events:

**Session and user events:** Each time Full Control started, each time it shut down, user timeouts, and session-related error conditions encountered while Full Control is running.

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.

Web browser activity: Each time a browser accesses a webpage. Logged information includes the title, URL and amount of time on that page.

File and folder access denied: Check this box if you use Full Control'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 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.

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

Tests and diagnostics: These tests can help pinpoint problems in your Full Control configuration. However, they generate logfile entries which are otherwise undocumented, so you should check this box only when you are instructed to do so by Bardon technical support staff.

**Diagnostic Snapshot Logging:** Full Control 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.

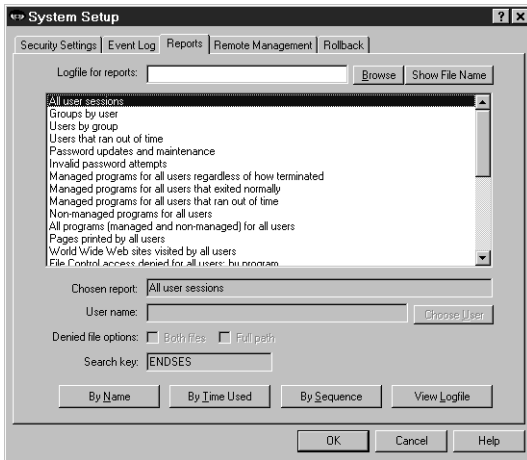
If checked, Full Control will create a snapshot file about once a minute. It will save as many snapshot files as you want, up to 99 files. If the maximum number have already been created, it will delete the oldest file to make room for a new one.

This is a very 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.

---

## Reports Tab



This tab lets you view and print reports based on entries in a logfile, or view the actual logfile data. The logfile can be the local logfile for this computer, or another logfile generated by another computer. You can also run these reports remotely, from the Reports screen of the Administration Manager. Recall that you indicated the events to log in the Event Log tab.

Choose a report, then click a button indicating how you want to view that report's data on the report output screen. For per-user reports, indicate the user name of interest. For *access denied* reports, you can use one or both of the denied-file options. See Usage Tracking Reports for more information on these.

You can view reports by applicable *Name* (usually, user name or program name), by amount of *Time Used* (time used to accomplish the task being reported), or by *Sequence* (each event in the order it happened). Events by *Name* and by *Time Used* are aggregated, so if the same program is run twice its data is added together. Events by *Sequence* are not aggregated.

Not all reports have all three views. When a report's view is not available its button is disabled.

Initially, the report output screen shows your chosen report's data in text form. The window can be resized if necessary so you can see more of the report. Grab a corner and pull.

To see the "top ten" items as a graph, click the *Graph* button on the report output screen. To print the text report, click *Print*. You can also click *Font* to change the text report's printed font. The printed report includes only the text lines, not the graph. However, you can easily import the logfile into a database or spreadsheet and use that application's graphing capabilities.

Reports can be generated from either the "human-readable" text format, or the CSV-format, logfile records. It will work fine even if you changed formats in the middle of the logfile.

Other than the Groups/Users report, all the reports are generated from the logfile

listed at the top of the screen. Initially this is the same logfile listed on the Event Log tab. If you need to see reports based on a different logfile, type it in, or use the Browse button to find it, or drag-and-drop it onto the Reports tab. The logfile name on this tab is only for reports. Changing it will not change the name listed on the Event Log tab.

To generate a logfile-based report, Full Control searches the logfile for a search key. Records containing the correct key are included in the report. When you choose a report, that report's search key is displayed on this screen.

If you need a report not provided here, select one of the *user defined reports* which are at the bottom of the list, and give any search key in which you are interested. See the Log File Format section for more information on which built-in search keys track what events. An external Full Control-aware program may add records to the logfile which use additional search keys. That program's documentation should have more information on those records.

After a report and a view are selected, the output screen appears, displaying that report in the selected view. 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.

Output reports in the current view can be printed or saved to a 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.

**Separate Logfiles vs. One Big Logfile:** Full Control allows you to log all your computers to one central logfile, or to have separate logfiles for each computer. In general, though, it's best to have a separate logfile for each computer. This gives you the option of locking the logfile, which prevents unauthorized changes. It's also faster, because one computer never has to wait for another to write its log information.

Separate files also allow you to see reports based on just one computer's activity. With separate logfiles, it's also easy to see reports based on all computers at once. Simply use the DOS command COPY to copy all the logfiles into one big file, and then the DOS command SORT to put all the lines of the big file into order. Here is how to do this:

```
COPY logfile1 + logfile2 + logfile3 tempfile  
SORT tempfile > biglogfile
```

If all your logfiles can be specified with a wildcard, it's even easier. For example, if all your logfiles have been copied to the same directory, and they all end in ".log" you can do it this way:

```
COPY *.log tempfile
SORT tempfile > biglogfile
```

Actually, you don't need the tempfile. You can pipe the output of COPY directly into SORT. See your DOS manual for details on this.

**Creating Your Own Reports:** If you need a report not provided here, select one of the *user defined reports* which are at the bottom of the list. You can search on any search key in which you are interested. See the Log File Format section for more information on search keys.

**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 logs the titlebar text of the DOS box instead of the filename of the running program, which would otherwise be identical in every case.

**Compatibility:** To generate further views of the data, the logfile can be imported for further analysis into any database or spreadsheet program. The Log File Format page describes the layout of this file.

**Available Reports:** The available reports are as follows. The specified logfile record codes are described on the Log File Format page.

All user sessions: This report shows the amount of minutes used by all users. It tracks ENDSSES logfile records, which are written when the user exits a session voluntarily, or when Full Control terminates that user for timeout reasons.

Groups by user: This report lists the users who are members of each group. It is not generated from logfile data. Groups with no users are not listed.

Users by group: This report lists all users, and the group to which each user belongs. It is not generated from logfile data.

Users that ran out of time: This report shows the ending time and amount of minutes when the user ran out of time. It tracks TIMUSR logfile records, which are written when Full Control forcibly terminates a user session. 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. It does this by tracking all CHPWD records (CHPWDP, CHPWDS, and CHPWDE). 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. It does this by tracking all BADPW records (BADPWX, BADPWM, BADPWP, BADPWV, BADPWC). Since such events take no time, the *Time Used* button is disabled.

Managed programs for all users regardless of how terminated: This report shows all managed programs that were run by any user, whether they were exited normally by the user or forcibly terminated by Full Control. It tracks all ENDAP records (ENDAPT and ENDAPU). These show user timeout, application timeout, and voluntary user exit.

Managed programs for all users that exited normally: This report shows all managed programs, run by any user, which were exited normally by the user. It tracks ENDAPU records, which show voluntary user exit.

Managed programs for all users that ran out of time: This report shows all managed programs, run by any user, which were forcibly terminated because the individual program ran out of time. It tracks ENDAPT records.

Non-managed programs for all users: This report shows all non-managed programs which were run by any user. It tracks ENDANM records.

All programs (managed and non-managed) for all users: This report shows all managed and non-managed programs which were run by any user. It tracks all ENDA records (ENDAPT, ENDAPU, and ENDANM).

World Wide Web sites visited by all users: This report lists each World Wide Web page by URL and title, and shows the amount of time spent at that website. It tracks WEBPGC records, which are written when the webpage URL or title changes, or the browser window is closed.

"File Control access denied" reports: If you have given file/folder names on Full Control's File Control tab, and if you have checked the "file and folder access denied" box on the Security Settings tab, you can use the next four reports to list files/folders which were requested but not allowed. There are two systemwide reports and two user-by-user reports. The same data is shown in both reports of each pair. The only difference is how the data is sorted.

When using any of the *File 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. If using both files, the additional level of detail may cause useful patterns to emerge.

Additionally, when using any of the *File 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.

This report is especially useful when your File Control 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 modify the File Control restrictions and exceptions lists as needed.

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.

File Control access denied for all users: by program: This report lists FILACC records generated for all users, sorted by the program which requested the denied file.

File Control access denied for all users: by filename: This report lists FILACC records generated for all users, sorted by the name of the denied file.

File Control access denied for the named user: by program: This report lists FILACC records generated for the named user, sorted by the program which requested the denied file.

File Control access denied for the named user: by filename: This report lists FILACC records generated for this user, sorted by the name of the denied file.

Window Control file access denied by Allowed Folder restrictions: On the Window Control tab you may have listed Allowed Folders for some of the Target Title windows. Doing so prevents users from opening or saving files to unauthorized locations -- access to locations other than the Allowed Folders is not permitted. If the user attempts such unauthorized access, Full Control denies access and logs the attempt in a format similar to the File Control reports described above.

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 for the restricted program on the Window Control tab.

When using this report, two filenames are involved: the name of the program which requested the file, and the name of the file requested. You can view the 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. If using both files, the

additional level of detail may cause useful patterns to emerge. Additionally, 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.

This report lists FILACD records generated for all users. As with the File Control reports, you must check the "file and folder access denied" box on the Security Settings tab to tell Full Control to log this information.

Managed programs for the named user regardless of how terminated: This report shows all managed programs that were run by the named user, whether they were exited normally by the user or forcibly terminated by Full Control. It tracks all ENDAP records (ENDAPT and ENDAPU). These show user timeout, application timeout, and user (voluntary) exit.

Managed programs for the named user that exited normally: This report shows all managed programs, run by the named user, which were exited normally by the user. It tracks ENDAPU records, which show user (voluntary) exit.

Managed programs for the named user that ran out of time: This report shows all managed programs, run by the named user, which were forcibly terminated by Full Control because the individual program ran out of time. It tracks ENDAPT records.

Non-managed programs for the named user: This report shows all non-managed programs which were run by the named user. It tracks ENDANM records.

All programs (managed and non-managed) for the named user: This report shows all managed and non-managed programs which were run by the named user. It tracks all ENDA records (ENDAPT, ENDAPU, and ENDANM).

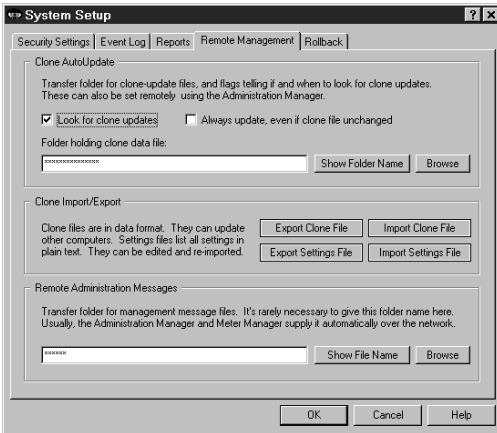
World Wide Web sites visited by the named user: This report lists each World Wide Web page by URL and title, and shows the amount of time spent at that website. It tracks WEBPGC records, which are written when the webpage URL or title changes, or when the browser window is closed.

User defined search for all users: To use this report, you must provide the search key. It will look for any events saved under the search key you enter here, for all users.

User defined search for the named user: To use this report, you must provide the search key. It will look for any events saved under the search key you enter here, for the one named user you specify.

---

## Remote Management Tab



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

**Clone AutoUpdate:** You can dynamically update the entire Full Control configuration from a remote location. To use this feature, give a clone data folder name here and check the *Look for clone updates* box. You can drag-and-drop a directory onto this dialog from Explorer, and its name will appear as the AutoUpdate source folder. Full

Control will look in that directory for a clone data file named *clonefc.bds*. This file is generated by clicking the *Export Clone File* button. Full Control looks for this file at startup. If found, Full Control will overwrite its current configuration with the new data.

Another setting available here controls whether Full Control updates itself with the clone files whenever they are found, or only when they have a different filedate from the last *clonefc.bds* file. Use this option to ensure that Full Control's configuration cannot be changed. Even in the highly unlikely case that someone has bypassed Full Control's security and modified its settings, the program will re-read the clone data file at startup to reconfigure itself as you have specified. Remember, though, that the clone data will replace the entire configuration repeatedly. Even your own "on the fly" setup changes will be replaced!

The settings in this group can be sent over the network via the Remote Administration Manager. This means that it's easy to update any computer at any time, even if that computer was not initially set up with Clone AutoUpdate settings.

**Export Clone File:** Clicking this button sets up to create a clone data file when you click OK to exit from the System Setup screen. By default it is named *clonefc.bds* and is in the named AutoUpdate 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.

**Export Plain-Text Settings File:** Clicking this button sets up to create a plain-text settings file which contains listings for all the options that can be set in Full Control. The file will be created when you click OK to exit from the System Setup screen. You can save this file as a record of your settings. You can also edit this file to modify the settings, and read it back in.

**Import Plain-Text Settings File:** Clicking this button sets up to read a plain-text settings file and update the current computer's configuration. The file will be read when you click OK to exit from the System Setup screen. The administrator has full flexibility in editing this file, a very powerful option. This is very handy, but can lead to unintended consequences if not treated carefully.

**Remote Administration Messages:** If you like, you can pre-designate a directory here for messages from the Remote Administration Manager. However, it's rarely necessary to do so, because the Administration Manager broadcasts over the network the location of the Message Directory it wants to use. Virtually the only time it's necessary to pre-designate this location is when the Full Control computer is in a different NT domain than the computer running the Administration Manager program.

This directory must be able to handle long filenames because Remote Administration filenames often exceed the now-defunct DOS 8.3 filename format. All computers must have read-write access to this folder.

---

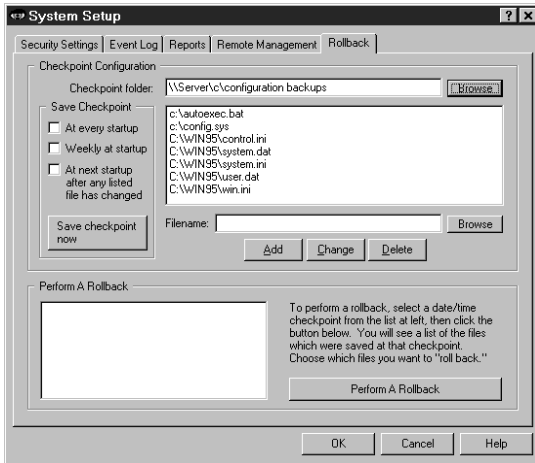
## *Rollback Tab*

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 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 saves a checkpoint. Give the checkpoint folder to which they should be saved. When you install Full Control, a starter list is provided, containing system files which are 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.

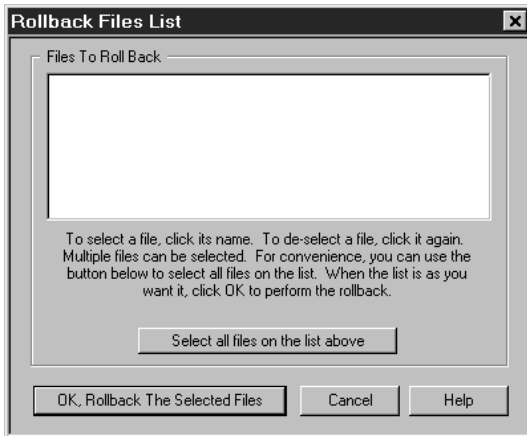
A checkpoint can be saved automatically at every Full Control startup, or once a week at startup, or at the first startup after any listed file has been modified, or

when you click the Rollback tab's "save checkpoint now" button. Also, the Administration Manager can tell a remote networked workstation to save a checkpoint by sending a message to that computer.



When Full Control "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 files (user.dat and system.dat) 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.

The *Rollback Files List* screen appears when you click the "perform a rollback" button on the Rollback tab of the System Setup screen. 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.

Full Control 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 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 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 (user.dat and system.dat). If it can't tell what to do about a particular file, it asks. Full Control can use either method to restore files under Windows 95/98. Under NT, it uses only the first method, due to NT's lack of any automated method to temporarily go to DOS.

---

## Group Setup Dialog

Full Control looks at the name of the user currently logged in to Windows. This user name can be validated at logon if desired, to ensure authorized access. If that user is listed as a member of a Group, that Group's settings will be put into place during the session. If that user's name is not listed as a member of any Group (and if unlisted users are allowed to log on), Full Control uses its Default Group settings for the session. 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.

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

The Group Setup screen has seven tabs:

**Access:** program management, time limits, and interface 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

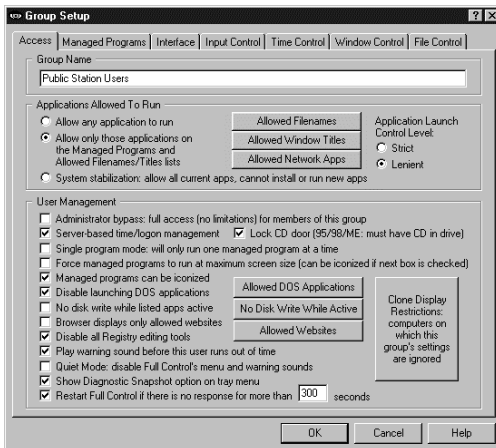
**Time Control:** timeouts and blockouts

**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:** This is the name by which the group is identified. You can rename a group at any time.

**Applications Allowed To Run:** Full Control 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.

You can also set up here to only allow the non-managed programs you specifically list. If the user tries to launch any other programs, Full Control will not let them run. In doing so, should Full Control be strict or lenient about such programs?

Strict: Under this option, the only programs that can be run by this user are Full Control managed programs and those listed under *Allowed Filenames* or *Allowed Network Apps*. This is the tightest possible control. However, Full Control achieves this control by modifying certain low-level Windows settings. They are modified when this user logs on, and cleared when Full Control exits at this user's logoff. Use the *Allowed Filenames* button to list non-managed programs that are allowed to run when this strict control is in place. You need give only the file name itself; the path isn't necessary. So for example to allow *c:\windows\sol.exe* to run, you need only give *sol.exe* as the filename. Remember to list all applications run automatically at startup, in addition to any applications which you allow the user to run.

In general this method works well. However, if for any reason Full Control exits abnormally, the low-level "don't run" settings will still be in place, and almost nothing on your computer will run. This is rare, but computers are not infallible. If it happens, Full Control provides a number of recovery options, which are listed here in the recommended order.

- First, try to run Full Control again; you can exit immediately if you like, because when Full Control exits normally it will clear any leftover control settings.
- If you cannot run Full Control in regular Windows, restart the computer in Safe Mode and launch Full Control while there. The strict security settings are ignored while in Safe Mode, so Full Control will always run. Launch Full Control 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 your prior settings is by restoring the *user.dat* and *system.dat* Registry files. Each time Full Control starts, it saves backups of these two files as *userfc.bds* and *sysfc.bds* in your Windows directory. These backups contain no security restrictions, so using them to restore your *user.dat* and *system.dat* files will clear any restrictions. However, you will lose any system configuration changes you made since they were backed up. In Windows 95/98, you will need to boot to plain DOS ("command prompt only") to copy these files. To restore them, copy *userfc.bds* to *user.dat*, and copy *sysfc.bds* to *system.dat*. All four are hidden, system, read-only files in your Windows directory. Use the DOS command ATTRIB to make these four files visible so you can manipulate them. For example, the Registry files (*user.dat* and *system.dat*) 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. In Windows NT, you can restore the Registry through an Emergency Recovery Disk which you previously created using the NT facilities, or if the computer is set up to allow booting into Windows 95/98 or from a floppy, you can restore the Registry files in that way.

Lenient: This option isn't as strong as the "strict" method. However, it does not create the low-level restrictions of the above method. With this method, Full Control itself enforces the restrictions by monitoring every new window that appears. Therefore, when Full Control isn't running there are simply no restrictions.

In this method, Full Control looks at the titlebar text of all new top-level windows. A window owned by another window is ignored (for example a Save As dialog). If a window doesn't match any titlebar text 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 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 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, 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, 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 runs programs.

Administrator Bypass: If you have set up Full Control to run securely at startup, it will be launched when any user logs on. However you may want to allow users who are members of certain groups to have complete access to the computer, with no interference from Full Control. To do this, check the Administrator Bypass box. With this box checked, when that user logs on and Full Control is run automatically at startup, Full Control will recognize this user as an administrator and immediately close itself. This leaves the computer wide open to be used with no interference. Note that Full Control will terminate itself only for that first, automatic startup. If the administrator needs to run Full Control later (perhaps to modify settings) it will launch and run normally.

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.

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 these two 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, you can allow the user to run "exceptions." To let this user 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.

No disk write while listed apps active: Check this box to accommodate applications that behave badly when another program writes to disk, for example certain scandisk, defrag, or backup programs. When checked, Full Control won't write to disk while any listed program is active. Use this carefully, because it disables Full Control's logging until the listed program exits. To list a program, click the *No Disk Write While Active* button and give that program's full-path filename. When a listed program starts, a STRNWR record is written to the logfile; when it exits, an ENDNWR record is written. Nothing is logged in-between these two events.


Lock CD drive door: Check this box to help prevent valuable CDs from walking away from the computer. In Windows 95/98, there must be a CD in the drive when the user logs on in order to lock the drive. In Windows NT the door is locked

whether or not a CD is present. In 95/98 if you have more than one CD drive on this computer, there must be a CD in every drive, otherwise no CD drive will be locked. In NT, if you have more than one CD drive on this computer you need not have extra CDs loaded in order to lock the drives.

When using this option the computer may pause briefly at logon/logoff, and when entering/exiting Setup Mode, as the CD drives are locked and unlocked.

Warning sound: Do you want Full Control 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.

Quiet Mode: Check this box to disable the "click" menu and button sound, and all other sounds generated by Full Control.

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.

Restart Full Control if no response: Full Control 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 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 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 can't send these "I'm OK" messages, so be sure the time is long enough to bridge any such periods.

---

## *Managed Programs Tab*

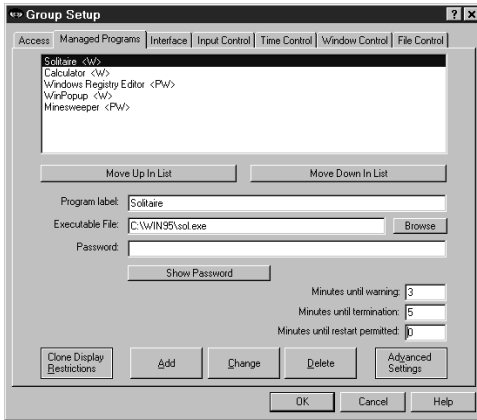
Full Control managed programs are applications set up on this group's Managed Programs tab. They can have a time limit, password, and other access configuration options. You can list any Windows application. However, a DOS application cannot be listed as a managed program. The companion fcRunApp utility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

Full Control monitors all system activity. As the user runs programs (from the Start button, Explorer, or in any other way) Full Control looks at them. If any application is on the managed programs list, Full Control applies its associated settings: password, time limits, license metering, 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 control 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
- M: License meter key name is given
- H: Hang up the phone on exit

**Move Up or 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 will compare its filename to the names on

this list. If a match is found, Full Control 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 group configurations. (The Advanced settings are described in detail elsewhere in this documentation.)

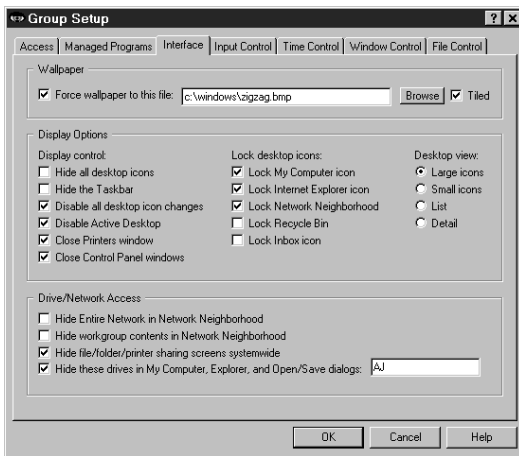
Advanced settings can only be changed for an existing managed program. To set these options for a new managed program you must first *Add* the program using

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 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 information 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 Options:** These options control the Windows desktop icons which are available to this user, and related display permissions.

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

Desktop view: Explorer's right pane can display its icons in any of four "views:" Large Icons, Small Icons, List, and Detail. But in standard Windows, the desktop display is always in the Large Icon view. Full Control adds to the desktop the same flexibility found in Explorer. The other views can be very useful. For example, Small Icon view allows many more desktop icons to be displayed, and Detail view conveys a wealth of information. Note that if Active Desktop is enabled, the default Large Icon view is always used.

**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 Open/Save dialogs unless explicitly specified. The drives and files are not themselves made invisible; only their listings in Explorer, My Computer, and 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, which

makes files and folders so totally invisible that not even Windows itself can see them.

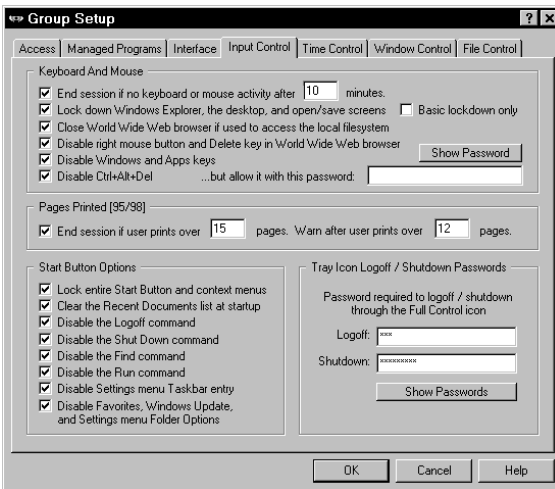
---

## Input Control Tab

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

**Keyboard And Mouse:** Full Control 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 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:** Full Control can test for periods of inactivity, like a screensaver timer, and log off the current user if there has been no activity for a specified number of minutes.



**Lock down Windows Explorer, the desktop, and open/save screens:** If checked, Full Control 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, checking this box will also close the Task Manager and, if you have Service Pack 2 or later, it will remove the File menu in Explorer. 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 catch the use of Cut, and it takes a tiny fraction of a second to catch Delete, but in general it's quite reliable. During the first few seconds after it is launched, Full Control always uses this "fallback" method.

Close World Wide Web browser if used to access the local filesystem: Web browsers can be used to get into the computer's file system. Check this box to close web browsers that are showing files or directories that are on the local hard disk or network. This feature 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 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.

**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 provides other options to disable the elements themselves, including options on the Interface tab, the *Keyboard And Mouse* options described above, Window Control options, and File Control options. Some people prefer to use these other options instead, and leave the Start button alone.

The *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 starts, or when the administrator exits from Setup Mode.

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


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.


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 users' attention and update your systems in a more organized fashion, check this box to disable these entries. Note: due to a bug, Windows 98 and IE4 rebuild the Start menu only at user logon, so to disable these entries on Win98/IE4 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 *Logoff* or *Shut Down*, you may sometimes want to provide this to certain users. You can do this through the  Full Control tray icon's popup menu.

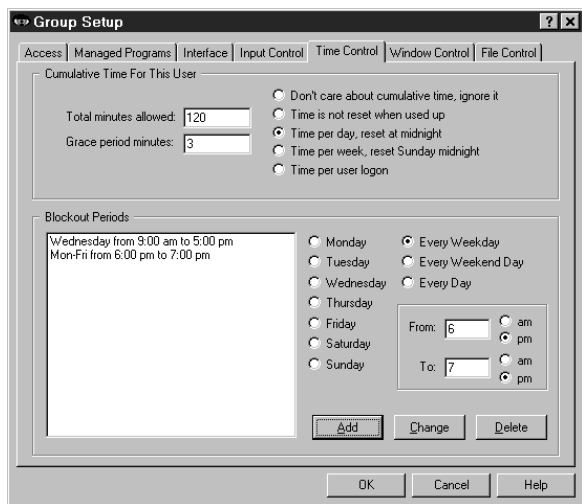
When disabled, a password is required to use the logoff or shutdown items on the  Full Control tray icon's popup menu. This could be the password listed here, or the Full Control setup password. If a command is not disabled, as a convenience the icon menu's logoff or shutdown functions do not require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

---

## Time Control Tab

This tab controls times during which programs can be run by members of this group.

**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 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 this can be changed to whatever you want. Setting it to zero will tell Full Control 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.

**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

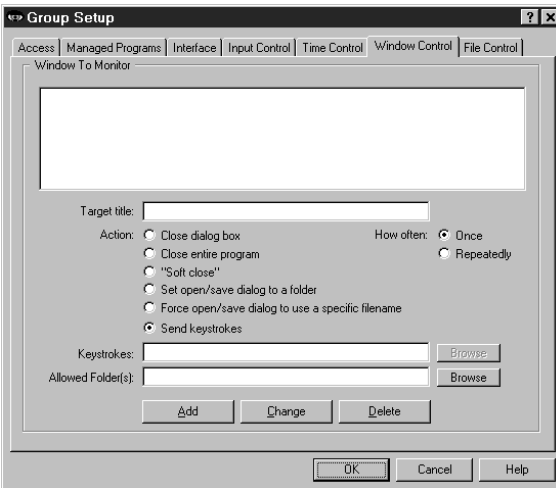
periods as you like. Blockout periods must start and end on the same day. You can't set up a blockout that goes past midnight (for example "Weekdays from 8:00 pm to 8:00 am") but you can achieve the same effect by entering this as two separate blockout periods, one from 8 pm to 11:59 pm, and the other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

---

## Window Control Tab

Window Control lets you control virtually any window or dialog when it appears. What can you do to a window? You can close it (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'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. Also, 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 to match the option 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 group) and %COMPUTERNAME% (the

designated name of this current Full Control computer). These are often handy when constructing forced file or directory names. They can also be used when sending keystrokes.

Let's look at each option in turn.

**Target title:** Full Control 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.

**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.

A report is available on the Reports Tab listing 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.

**How often:** For some of these features, you can perform the action just one time, or perform it repeatedly (every few seconds) to make absolutely sure it is done the way you want.

**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 title 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 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 members of this group. 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 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 set your users to a specific directory, then keep them there.

Note that other Full Control 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 *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 group) and %COMPUTERNAME% (the designated name of this current Full Control computer). 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.

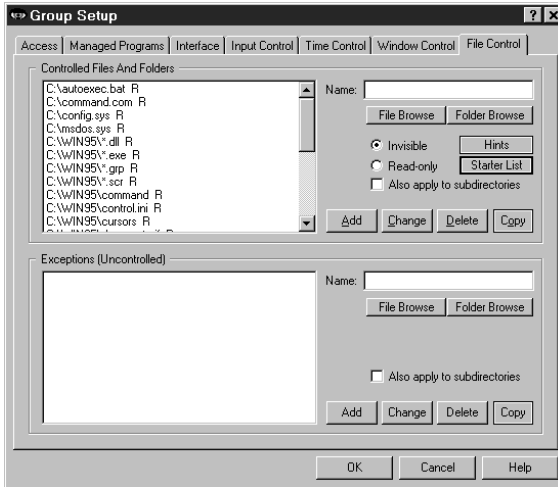
You can also use certain nonprinting characters by giving their name in brackets. Here is a list: {Bksp} {Break} {CapsLock} {Clear} {Del} [End] {Enter} {Esc} {Help} {Home} {Insert} {NumLock} {PgDn} {PgUp} {PrtSc} {ScrollLock} {Tab} {F1} to {F12} {Up} {Down} {Left} {Right}

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.

---

## File Control Tab



With this screen, you can make any file or directory read-only or invisible. Full Control'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. Controlled files and folders are locked to both the user and operating system, so certain files and folders should be controlled only with caution. See below for some hints and suggestions.

**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 user 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 group) and %CURRTIME% (a unique number based on the current time) as part of the file or folder names you enter.

**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*.

**Copy:** You can copy a list to another 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 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, so be careful! Here are some examples:

Windows Directory: If everything in the Windows directory is invisible or read-only, 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 Directory: It's not necessary to protect Full Control'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's own built-in protection.

Entire Drive: On most computers if you control your entire C:\ drive (including all subdirectories), 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 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 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's file protection, use Full Control's access-denied reports to see which required files were unavailable, and what programs requested them. Then list those files or folders as Exceptions.

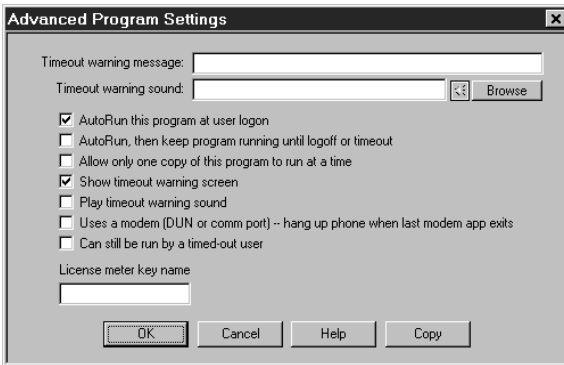
A listing on the File Control tab restricts all running programs, at all times that a user from this group is logged on. Another option might be to use the Allowed Folders option on the Window Control tab to limit access only when an Open or Save As screen is displayed, and only while a program displays its 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 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.



**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 plays its built-in warning sound. No sound is played if the Quiet Mode option has been selected.

**AutoRun this program at user logon:** Check this box if you want the program to run automatically when the user logs on.

**AutoRun, then keep program running until logoff or timeout:** If this box is checked, the program will run automatically when the user logs on, and in addition it will be restarted as necessary to ensure that it is always running. If you check this box it is unnecessary to also check "AutoRun at logon" (though it causes no problems if you do so).

**Allow only one copy of this program to run at a time:** By default, Full Control 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 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 plays its built-in warning sound.

**Uses a modem -- hang up the phone on exit:** If you tell it to, Full Control will disconnect modem-using apps and hang up the phone. Check this box if you want Full Control to hang up the phone and reset the modem when this program exits. It will work if this app uses Dial-Up Networking, or the old-style DOS "direct to the COM port" communications method. If Full Control sees that Dial-Up Networking is active when this program exits, it will check to see if any other running managed programs have this box checked before closing Dial-Up Networking. You don't want Full Control hanging up the phone if another program is still using it! So, unlike DOS "direct to the COM port" modem apps, Full Control will allow any number of DUN-using managed programs to run simultaneously. Full Control will disconnect Dial-Up Networking only after the last of these programs closes.

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

**License Meter Key Name:** Perhaps your organization has purchased only a few licensed copies of some program, yet you want to allow that program to be run from any workstation on your network. Full Control to the rescue! Full Control is designed to ensure that the number of simultaneous users never exceeds the number of licensed copies of the software. To set this up, first install the program normally, making sure it can be run from each workstation. Then set up that application as a managed program on all desired Full Control computers on your network.

When this is set up, choose a License Meter Key Name. This can be any word or name you prefer, though it's probably best if the key name helps you remember which program it is monitoring! So, for example, if you have licenses for Microsoft Word For Windows 95, you might choose to use the key name "Word 95". You must use this same key name with all entries for the associated program, on all Full Control computers on your network. When the user runs that program, Full Control will ask the License Meter Manager program if there is a license "slot" available under the key name "Word 95". If a license is available, the Meter Manager program will add the new user, and allow the program to be run. When the user exits from the monitored program, Full Control asks the Meter Manager to release the license "slot" making it available to other users. As you might imagine, the Meter Manager program must be running throughout this entire process. It can

be active on any machine on your network from which it can receive messages from this computer.

To meter a software suite, give all the programs in the suite the same License Meter Key Name. If a user is already running one component of a suite, Full Control will allow that user to launch any other metered program that uses the same License Meter Key Name. So, for example, if you want to meter the Microsoft Office suite, set up separate managed program entries for Word, Excel, etc., and give them all the same License Meter Key Name. You might give them all the key name of "Microsoft Office Suite Component." Programs that have the same License Meter Key Name all use the same license "slot" when run on the same computer. The license "slot" is taken up when the first such program launches, and is released only when the last such program is closed.

**Copy Button:** 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.

# Security And Administration

---

## System Administration With Full Control

The concept of Full Control 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 are especially intended to be handy when managing more than one Full Control-enabled computer, perhaps on a network.

Full Control 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 Full Control's companion programs to reconfigure that computer and modify its settings on the fly. You can query the status of the remote computer, send popup text messages to the user at that computer, and even logoff or shut down the computer remotely. Full Control's Remote Administration Manager and License Meter Manager are designed specifically to allow administrators to dynamically modify settings and control access and activity on networked computers.

---

## Security Considerations

Full Control provides very thorough security control for your computer. Here are some things you can do to help Full Control, 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'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 members of this group log 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.

**Disable booting from floppy disk:** If your computer is booted to DOS from a floppy, Full Control 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'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.

---

## How To Clone A Computer

Full Control's cloning feature takes a "snapshot" of the computer's Full Control setup, so it can be copied to another computer or saved as a backup. The data is saved in a clone file when you click the *Export Clone File* button on the Remote Management tab of the System Setup dialog. The clone file contains all the information that defines this computer's configuration, including licensing information and any display restrictions that you've set up to control which programs or users are monitored on what computers when the clone file is distributed.

You can also export this data to a plain-text file that you can read and edit, and re-import after changing it. To do this, click the *Export Text File* button on the Remote Management tab. A clone file can be used to AutoUpdate your remote computers, but a text file cannot.

**How to clone:** To clone a computer, first set up one master computer with your chosen groups, users, managed programs, passwords, logfile, sounds, display restrictions, and whatever else you want to specify. Then open the System Setup screen on that master computer, and on the Remote Management tab click the *Export Clone File* button.

There are three ways 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 a clone data file named *clonefc.bds* to the same directory as the Full Control installer (floppy disk or network install directory), with the other Full Control files. Run the Full Control installer in the usual way. When the installer sees the data file, it will offer to copy the clone data onto the new machine.

When performing an automated "quiet" install, if a clone data file is found, its settings are always read. Full Control is then launched by the installer. As soon as Full Control launches it will set up any options, including any "logon validation" and "run at startup" options specified in the cloned settings.

Updating manually: To update manually, enter Full Control's setup mode on the computer you want to update, go to the Remote Management tab, and click its *Import Clone File* button. Name the clone file to be read, and that Full Control computer will immediately update itself. In this case, the clone file does not need to be named *clonefc.bds* because you are explicitly pointing Full Control to the file you want it to use. You can also update manually using a plain-text "settings" file.

AutoUpdate: To dynamically update an already-installed remote client computer, copy a clone file named *clonefc.bds* to the directory in which that client computer

looks for clone data files. This was specified in that computer's System Setup dialog on the Remote Management tab. On the next restart, the computer will see the new data file in that directory, read it, and replace the old data with the new data. For security reasons, you might want to just give the client machine read-only permission in that directory through the usual network facilities.

**Clone customization techniques:** If you are cloning one master computer and you want the target computer(s) to use a different logfile than the master computer, when you set up your master configuration use the word %COMPUTERNAME% as part of the logfile name. At runtime this will be replaced with the actual computer name to build a unique logfile name for this computer. You can also use the words %USERNAME% (user name given through current network or Windows logon), %GROUPNAME% (that user's Full Control group) and %CURRTIME% (a unique number based on the current time) here but they are not as useful. See the Event Log description for more information on this. Generally, it's a good idea for each computer to have its own logfile.

You can also use the %USERNAME% and %GROUPNAME% options to provide each user their own private work area on the computer. See the File Control description for details.

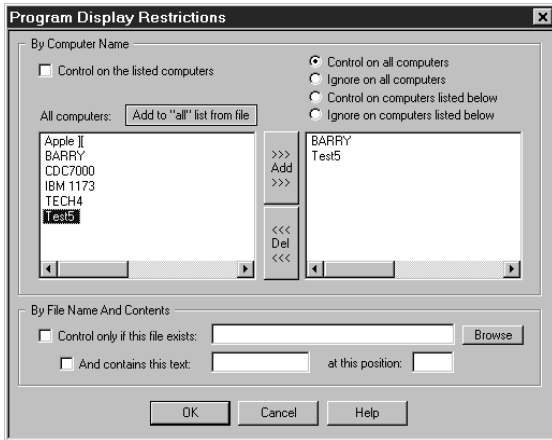
Another useful tool for cloning is Full Control's Display Restrictions feature (see below). This lets you control the computers on which a user or managed program is monitored. When setting up your master computer, you can give information for each individual user and managed program. At runtime Full Control 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 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 per-user settings. Full Control'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 file and program access by computer and user throughout the enterprise.

---

## Per-Computer Display Restrictions

Let's say you are setting up Full Control on one master computer, and you intend to clone this setup and distribute it to other computers at your site. In this situation, you sometimes need to specify which managed programs and users 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 screen. If you come in from the Managed Programs tab, you can specify the computers on which that application will be treated as a managed program. If you come in 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 set the group to be ignored on this

computer, Full Control'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 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 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 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 look for the named file to decide whether to monitor this managed program or group. 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 to test the text characters contained in the file. In this test, Full Control 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 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 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 will find and read its saved-data list, and include any computers that Administration Manager knows about. Running 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 import your own list of computers. Click the "add from file" button, and give the name of your file. This is a plain-text file. The computer names can be delimited in any way that works for you. They can be separated by commas, or by tabs, or on separate lines, or in CSV (quoted comma-delimited) format. In other words, the delimiter between computer names can be a comma, a tab, a double-quote (not a single-quote!), a newline, or any combination of these. Multiple delimiters together (for example the quote-comma-quote between items in a CSV list) are treated as a single delimiter.

---

## Reset Mode

Reset Mode is a fail-safe mechanism built into Full Control. It lets you start Full Control and use its setup screens while not actually launching the security protections which those screens define, which 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 is running.

**Using Before Full Control Starts:** To start Full Control in Reset Mode, run the Full Control Reset program (reset.exe) from Explorer, or in any other convenient

way. When used before Full Control starts, reset.exe must be in the same directory as the Full Control program itself. Another way is to start Full Control in reset mode from a command prompt with the /reset parameter (c:\somedir\otherdir\fc.exe /reset).

**Using While Full Control Is Running:** Reset Mode is also used to access Full Control's configuration options while Full Control is running, for example when you have set (on the Security Settings tab) that its tray icon should be hidden. If Full Control is already running when you start in Reset Mode, Full Control will ask for its setup password, then go into setup mode and displays its Administration 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 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 normally.

**Using 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 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 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, fcerset.exe will wait 180 seconds before asking Full Control 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's strongest security settings are not in effect. In this mode, Full Control 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 members of this group; exit if a user's time has run out; process remote clone files or administration messages; use license metering; 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 Internet Software

Full Control is designed to provide reliable management oversight to Internet software.

**Web Browser Monitor:** The Full Control Web Browser Monitor lets you log all the websites that are visited while Full Control is active. It's a handy way to see what sites are being accessed, and for how long. To activate this feature, use the Event Log tab to set up Full Control for logging, and check the box on that tab labeled *Web browser monitor*. Full Control will log the website URL, title, and the number of minutes at each site, for all websites visited through Netscape or Internet Explorer version 3 or later. This information can be viewed through Full Control's built-in reports. It can also be viewed remotely through the Administration Manager.

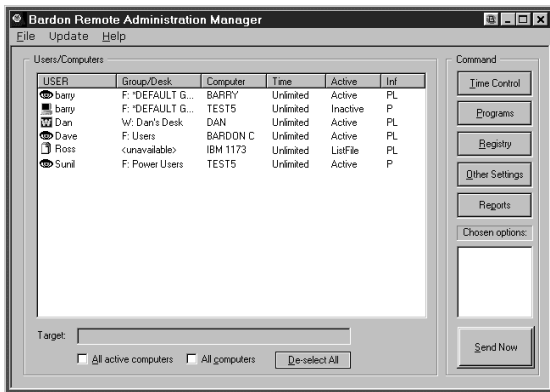
Browsers can have multiple windows open at the same time. Full Control can track up to 500 open browser windows simultaneously. Pages which are visited for just a few seconds are ignored.

Also, on the Access tab you can set Full Control to close web-browser windows that are accessing files on the local computer.

**Preventing access to local files:** By default, most web browsers can access the local computer's file system just as easily as a website halfway around the world. If security is your goal, you may want to prevent this. On the Group Access tab you can set Full Control to close browser windows that are accessing local files.

# Companion Software

## Remote Administration Manager



The Administration Manager lets the administrator, at another station on the network, reset the current time limits, list running programs, close programs, start new programs, modify the Registry, change clone-update settings, remotely logoff any user, shut down the remote computer, initiate 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 Command buttons to bring up these screens.

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

The remote stations can be running Full Control 2.x or WinU 5.x.

**Setting Up The Remote Computers:** In most cases, nothing special must be done to set up the remote computers to be managed by the Administration Manager. During operation, WinU and Full Control announce their presence over the network. The Administration Manager will hear this, and the computer's listing will appear in the "Users/Computers" list. This automatic process works fine under Novell Netware, Windows 95 peer-to-peer networking, and NT-based networking within a single domain.

If a target computer is in a different NT domain than the Administration Manager's computer, it can still be managed remotely. Under the File menu, choose "Set Message Command Folder" and choose a folder that is visible to both the Administration Manager and the remote computer. You then list this same folder on the Remote Management tab of the target computer. The remote computer can then communicate with the Administration Manager. Using this method, you can even send management messages by email.

**The Message Command Folder:** The "Message Command Folder" allows the exchange of data files and other large messages between the Administration Manager and the remote computers. If WinU or Full Control has been installed on this computer, and if a "Remote Administration Messages" folder has been named on the Remote Management tab, that folder is used. If not, you will be prompted for a folder at startup. Typically this directory will be on a server, where it can be seen by both the remote computers and the Administration Manager. All computers must have read-write access to this folder.

**Using The Remote Administration Manager Program:** The administrator can run the Remote Administration Manager from anywhere on the network that can access the "Message Command Folder". The network must be enabled for long file names. If WinU or Full Control has been installed on this computer, its setup password is required in order to run the Administration Manager. So, if you want the Administration Manager to be password-protected, install WinU or Full Control on your administration computer. You don't have to run it, just install a licensed copy.

The "Users/Computers" list shows information about who is and isn't logged on, and the current state of those computers. The columns list the current logged-on user's name, the currently active WinU desktop or Full Control 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.

*Group/Desk:* This is the active Full Control group or WinU desktop. As an aid to sorting by this column, the first letter indicates which platform is active on the listed computer. If this is a Full Control computer, the line starts with "F" and lists the currently active group. If this is a WinU computer, the line starts with "W", and lists the currently active WinU desktop. If this line's data was read in from a ListFile and has not yet been updated through an actual logon by that user on that computer, the Group/Desk is listed as "unavailable."

*Computer:* This is the WinU/Full Control name for the computer. Usually this is the same as the Windows name for that computer, however the computer name can be changed from the System Setup screen.

*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).

*Active:* If this user/computer is currently logged on, it is listed as "Active" here, and the left-edge computer icon is lit up. If this user/computer is not logged on, it is listed as "Inactive" here, and the left-edge computer icon is dark. If this user/computer was read in from a ListFile and has not yet ever become active, it is listed as "ListFile" here, and the left-edge icon is a file image.

*Inf:* Informational flags for this entry. They can be as follows:

- P a password is available for this line
- L this is a licensed copy, not an evaluation version
- N computer is in NoWrite mode (set on the Access tab)

A computer's setup password is required in order to send a command to that computer. The Administration Manager obtains this automatically from active computers, and retains it for inactive computers. Therefore, the only time this will not be available is when a user/computer was read in from a ListFile, and that user has not ever logged on, and that ListFile line's entry did not include the optional password. See below for more on how to use a ListFile.

**Building A Command:** To build a command, first choose one or more computers from the Administration Manager's list. To send the same message to multiple computers, use the Control and Shift keys just as in Explorer (and everywhere else in Windows) to select multiple list entries, or check the "all computers" or "all active computers" box. Next, set up the command to send. The command messages are set up on the Time Control screen, the Programs screen, the Registry screen, and the Other Settings screen. Use the Command buttons to bring up these screens. As you add each command, a brief note is added to the "Chosen Options" list to remind you of which you have selected. You can clear a "Chosen Option" by selecting it from the list, then using the File menu option to "Delete Selected Chosen Option" or of course you can also go back into that option's Command screen and change it there.

**Sending A Command:** After a command is built, click the "Send Now" button to send it immediately, or use the "Send Now" option on the File menu.

You can also schedule a message to be sent at a later time. To do this, choose the "Send Later" option from the File menu. Also on the File menu is an option to "Send Command To Another Folder." This saves the command as a file, and puts it in your chosen folder. At some future time, you could then manually copy that

file to the "Message Command Folder" where it can be seen by the target computer.

A messages that is sent by file, such as a "send later" or "other folder" message, is named for the computer to which it is addressed. For example a file might be named "My Full Control Computer.fct" and saved in the target directory. If there is already a file named "My Full Control Computer.fct" then the new file will replace the old one. WinU or Full Control will delete the file immediately after it is read. To transmit files, your network must support long file names so as to accommodate a computer name that might exceed the now-defunct DOS 8.3 filename standard.

**Delete Selected Computers/Users:** Entries on the list are saved even after they go inactive. To clean up the list, select the lines you want to remove and choose this item from the File menu.

**Delete Selected Chosen Options:** As you build a command, entries are added to the Chosen Options list to remind you of what you have set up. If you change your mind, these options can be deleted by selecting one or more in the Chosen Options box and using this item from the File menu. It's just like un-checking options on the Command screen, except faster and easier.

**Read Computer/User List From File:** This menu item on the File menu lets you read in a "starter list" of users, computers, and (optionally) passwords. Here is a small sample file:

```
[userlist]
dave=Esmerelda
tom=Fortuna,telephone
sharon=Cowbox
craig=Fish1,tuneful
```

The first line of the file must be [userlist]. The rest of the file lists the data to be entered, one entry per line. Each line consists of a user's logon name, an equals sign, a computer name, and optionally a password for that user/computer entry. If there is a password it must be preceded by a comma.

**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 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 members of this group can only log on to one computer at a time. The Administration Manager must be running to coordinate this feature.

**Version Update:** You can use the Programs screen to run any command on a remote computer, and these commands might include installers, uninstallers, and similar update components. In such a case, WinU or Full Control are the active agents that make sure your command runs and the update takes place. But how can the agent replace itself? That is, how can you get WinU or Full Control to update themselves when a new version is released? The answer is to copy all the new-version files to a shared, visible folder on the network and then choose this Version Update menu item, which tells all selected computers to go to that folder and update themselves using the files at that location. You'll be prompted for the folder with the new-version files.

**An example:** Here is one way the Remote Administration Manager might be used. A station can sit there with zero time available until a patron arrives. Then you can remotely set the time limit to some value, letting the patron use the computer. If the patron chooses to add more time, this can be done from the administration station and the patron does not have to log off first. Or if necessary to handle certain kinds of situations, you can force a logoff, shutdown, or reboot at any point, remotely from the administration station.

Let's say a customer arrives and sits at a computer. There is zero time available. From the administration station, you remotely send some time to that computer, perhaps 30 minutes. The customer uses the computer for the allotted 30 minutes as the counter ticks down.

Perhaps the customer leaves while there is still unused time. If so, you can clear any remaining time remotely. Or maybe the inactivity monitor triggered a logoff. Either way, reset it to zero and the computer is immediately ready for another patron.

Or perhaps the customer isn't done yet, and wants to add time to this session. You can remotely send more time to that computer. Within seconds, the customer sees the tray icon menu change, showing the new time limits.

Or perhaps it's time to close, and the customer doesn't want to leave. You can remotely logoff or shut down the computer, because you have ... Full Control.

---

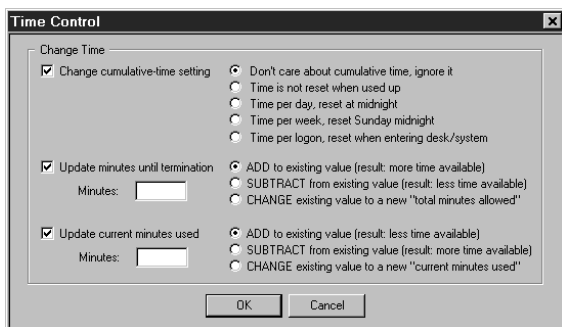
### *Time Control screen*

The main Administration Manager screen displays the time settings for the currently active WinU desktop or Full Control user and group. Options are available from the Administration Manager's Time Control 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 this might be to set the public computer to "no time left" when Full Control 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 will warn the customer in advance of expiration. You then use the Administration Manager to send the machine more time.

---

## Programs screen

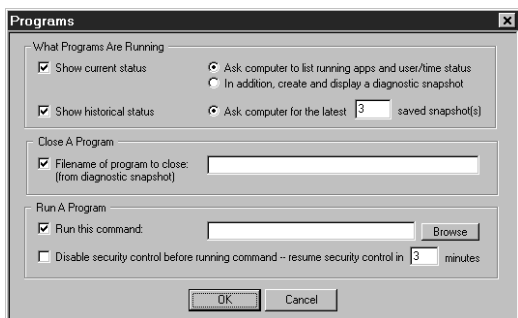
Options are available from the Administration Manager Programs screen which can list all active programs, close currently running programs, or launch new programs.

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.



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.

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?

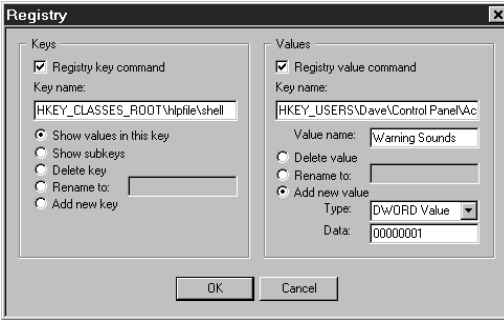
---

## Registry screen

Options are available from the Administration Manager 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. 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.

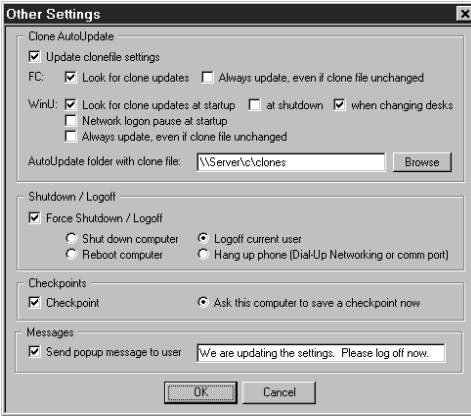
Warning: don't modify the registry unless you know what you are doing! The registry holds the computer's basic configuration settings. Windows provides virtually no error checking for registry modifications, making the registry a remarkably easy component to break. Be careful!

---

### Other Settings screen

Options are available from the Administration Manager Other Settings screen which allow you to change the Clone AutoUpdate settings on the remote computer, logoff or shut down a computer, ask it to save a checkpoint, or send it a message to be displayed to the user.

Clone AutoUpdate: This sets the same options described on the Remote Management tab, which allow you to update a computer's clone data folder name and check the *Look for clone updates* box. WinU or Full Control can look in that directory at startup, shutdown and (for WinU) when changing desks, for a clone data file named *clone.bds* (for WinU) or *clonefc.bds* (for Full Control). If found, Full Control will overwrite its current configuration with the new data. You can also set whether the clone update is performed whenever a clonefile is found, or only when it has a different filedate from the last clonefile. The settings for WinU and Full Control are slightly different. Both are provided here. There's no problem using both the WinU settings and the Full Control settings at the same time.



**Shutdown / Logoff:** *Logoff* will immediately set the target computer to the default WinU desk, or log off the current Full Control user. *Shutdown* and *Reboot* act the same on some computers. For those computers that can handle the distinction, both choices are provided here. *Hang up* will terminate any open Dial-Up Networking or old-style DOS comm port modem connection and hang up the phone. Maybe you'll want to send this message to all your computers at the end of the day to make sure all your

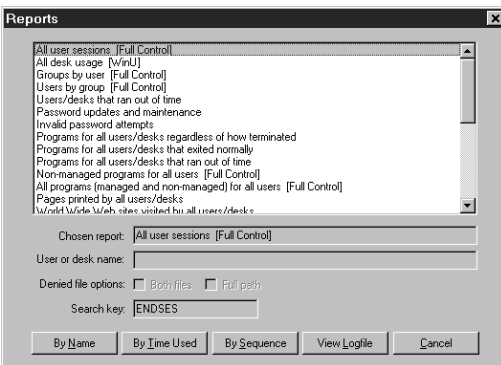
phone lines are disconnected before closing up shop.

**Checkpoint:** Select this to ask the computer to save 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 or Full Control is first installed.

**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 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 little delay.

---

## Reports screen



These reports can be run from the Administration Manager to show activity on the remote computer. They are essentially the same reports that can be run against a local computer's logfile from the System Setup screen's Reports tab, and are described in detail on the Usage Tracking Reports page. As with all the Administration Manager options, you can select as many computers as you want on the

main Administration Manager screen. A report will be run against each selected computer. So, for example, if you select a report on "all users" or "all desks",

each computer's report will display information on all the Full Control users or WinU desks known to that one specific computer. Similarly, when running "per-user" or "per-desk" reports from the Administration Manager, the User Name is set to CURRENT ACTIVE USER/DESK indicating that the report will display information about the active Full Control user or WinU desk currently logged in to that computer.

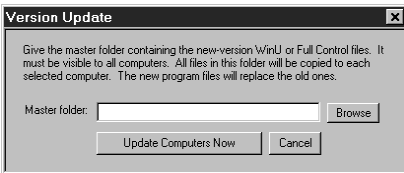
Most of these reports are applicable to a remote computer running either WinU or Full Control. A few reports are specific to one or the other, though, and these reports have the target program's name on the report description line in the list.

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.

---

### *Version Update screen*

If you have a new-version update of Full Control to upgrade all your current Full Control computers, you can't simply run the installer. Full Control 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. So how do you update all your computers?



Here's how. Copy all the new-version files to a shared folder on your file server. Make sure these are the only files in the folder. Next, select the computers to update from the Administration Manager's list of users and computers. Finally, click on the Update item

in the Administration Manager's menu. This will display the Version Update dialog. Give the name of the server directory holding the new-version files, then click the "update computers now" button.

A message will be sent to all selected computers asking them to update their files with the contents of the "master folder" you chose. Each target computer will copy every file found in the "master folder" to its own "home" directory. By doing this, all the old files will be overwritten with the new files.

The only exception is ".sys" files under NT, which will be copied to the target computer's designated Drivers directory only if this user has permission to do so. See below for more on this.

After updating, Full Control will be restarted. This will run the new version from the updated files.

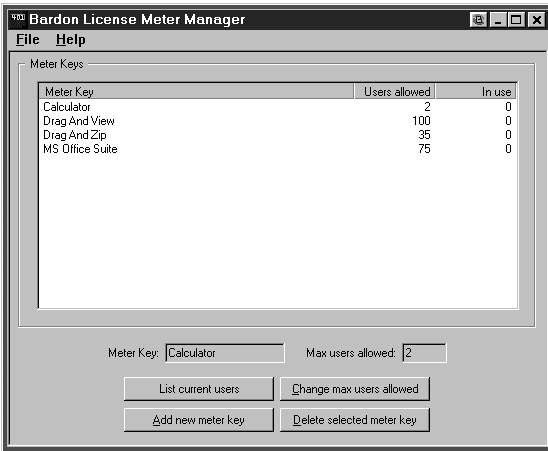
**NT Drivers:** To update the Bardon NT driver files, the currently logged on user must have permission to copy files to NT's System32\Drivers directory and overwrite files already there. Members of NT's "Administrators" group generally have this privilege; other groups may also, depending on your NT 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, then reinstall it using any of the remote-management "quiet-mode install" options listed in the Installing And Uninstalling section. Because you can supply a clone data file with the re-install, no settings will be lost. Again, however, the install must be done while the computer is logged on to an Administrator account.

---

## License Meter Manager



WinU and Full Control include network-based license meter management. This lets you control how many users can simultaneously run any program. You'd use this feature if your organization has purchased only a few licensed copies of some program, yet you want to allow that program to be run from any workstation on your network.

To set up WinU's license management, first set up the application to run from a program

button. To set up Full Control's license management, first set up the application as a managed program.

Next, choose a license meter key name. This can be any word or name you prefer, though it's probably best if the key name helps you remember which program it is monitoring! So, for example, if you have licenses for Microsoft Word For Windows 95, you might choose to use the key name "Word 95". Give this license meter key name on each relevant program's Advanced Settings screen. Naturally, you must use the same key name with all programs that run the same application on all WinU or Full Control computers on your network.

When the user runs that program, WinU or Full Control will ask the Meter Manager to see if there is a license "slot" available under the key name you've given ("Word 95" in our example). If that key's licenses are not all currently in use, the Meter Manager will update the license metering information to add the new user, and will allow the program to be run. When the user exits from the monitored program, the Meter Manager releases the license "slot" making it available to other users.

**Software Suites:** To meter a software suite, give all the programs in the suite the same license meter key name. If a user is already running one component of a suite, that user will be allowed to launch any other metered program that uses the same license meter key name. So, for example, if you want to meter the Microsoft Office suite, set up separate managed program entries for Word, Excel, etc., and give them all the same license meter key name. You might give them all the key name of "Microsoft Office Suite Component." Programs that have the same license meter key name all use the same license "slot" when run on the same computer. The license "slot" is taken up when the first such program launches, and is released only when the last such program is closed.

**How To Use The License Meter Manager Program:** The system administrator uses the License Meter Manager program to add or change license meter key names and the numbers associated with those names.

First, use the File menu to tell the Meter Manager where the license meter data file is located. You only have to do this once; the file's name and location will be saved.

Selecting a file reads all its keys. To work with an existing key, choose it in the list and click the appropriate button below. You can add a new key, change a key's settings, or delete one altogether. If a key shows that some of its licenses are currently in use, you can list its current users .

The Meter Manager stores its information in the license meter data file. Use the File menu to provide the name of this file. If you don't, the Meter Manager will ask for the name of this file. For security reasons, this file must not be in a shared directory available to the public. Client computers do not need access to this file. Only the Meter Manager program needs to have access to it.

The administrator can run the Meter Manager from anywhere on the network that can access the "Message Command Folder" (see below). The network must be enabled for long file names. If WinU or Full Control has been installed on this computer, its setup password is required in order to run the Meter Manager. So, if you want the Meter Manager to be password-protected, install WinU or Full Control on your administration computer. You don't have to run it, just install a licensed copy.

**The Message Command Folder:** The "Message Command Folder" allows the exchange of certain kinds of messages between the Meter Manager and the remote computers. If WinU or Full Control has been installed on this computer, and if a "Remote Administration Messages" folder has been named on the Remote Management tab, that folder is used. If not, you will be prompted for a folder at startup. Typically this directory will be on a server, where it can be seen by both the WinU and Full Control computers, and the Meter Manager station.

**Installing Metered Software:** The license monitoring is designed to work equally well whether you install a single copy of the monitored software on a network server, or install separate copies on every workstation (perhaps far more installations than you have actual licenses). In either case, it is designed to ensure that the number of simultaneous users never exceeds the number of licensed copies of the software. This lets you use your network to monitor and control a limited number of licenses for a program, even if the program isn't "network friendly" and insists on being run from the local machine. (Check with the software vendor before installing more copies than you have licenses.)

---

## The fcRunApp Utility

The fcRunApp program can run a DOS application when DOS apps are otherwise disabled by Full Control. 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:\dir1\dir2\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 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 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 allow it to run. You can have as many fcRunApp shortcuts as you like, each running a different DOS command. If Full Control isn't running 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. Click on the Shortcut tab. In the middle of the screen is the Target line, which runs fcRunApp. Put your cursor at the end of that line and add

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

to the end of the line. Click OK to save the shortcut.

Now you need to tell Full Control that it's all right for fcRunApp to run list.com. Start Full Control, 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 add

```
/cmd=c:\somedir\otherdir\list.com myfile.txt otherfile.txt another.txt
```

to the end of the line. Same command but with its parameters. Note that in Full Control you only need to add the actual executable file name c:\somedir\otherdir\list.com to the Allowed list, you don't list parameters there.

---

## Logoff Applet

On some computers, the Start button or desktop options don't clear when Full Control exits, and you need to log off to get everything back in sync. But what if the Start button's logoff item is itself hidden? In that case you can use this little applet (logoff.exe).

Put this in your C:\Windows\Start Menu folder so you will always have a Logoff menu item. Don't worry, it won't log off while Full Control isn't allowing logoff.

If you want to name it something different, or give it a different icon, put the program elsewhere on the computer, and put a Shortcut to logoff.exe in your C:\Windows\Start Menu folder, then change the name or icon of the Shortcut.

# File Formats

---

## Log File Formats

Full Control provides file-logging options that can be set in the System Setup screen's Event Log tab. The log file records can be saved in one of two formats. In *Text format*, Full Control records all actions to a log file in a more or less "human-readable" format. If *CSV format* is chosen, Full Control logs all actions in comma-separated-values format suitable for importing into a database or spreadsheet.

The logfile is also the source of the data used to generate Full Control's usage reports. These reports don't care whether the logfile uses the *Text* or the *CSV* format. You can even change format in the middle of the file; the reports will still be accurate.

The "human-readable" records are of this form:

```
dd-mm-YYYY HH:MM:SS nnn: fffffff, num, computer, user, app, msg
```

The comma-separated values records are of this form:

```
"dd", "mm", "YYYY", "HH", "MM", "SS", "nnn",  
"ffffff", "num", "computer", "user", "app", "msg"
```

The abbreviations used in the above description forms are:

dd	two digit day (01-31)
mm	two digit month (01-12)
YYYY	four digit year (ex: 1997)
HH	two digit hour in 24 hour time (00-23)
MM	two digit minute (00-59)
SS	two digit second (00-59)
nnn	three digit current user number (1-500)
ffffff	six-character "action flag" code (see below)
num	usually, minutes in program or user logon (see below)
computer	the computer name of this Full Control machine
user	current user name (text)
app	usually, title of this managed application (see below)
msg	explanatory message

The "action flag" code is six characters long. It indicates the action that generated this log record. The associated message can be any length. This table shows all action flags, the "num" flag, and the explanatory messages associated with them:

Code	Num	Message
ADVSRY	S	Advisory message, or internal action flagged
BADPWC	S	Invalid password for Ctrl+Alt+Del
BADPWM	S	Invalid password for setup mode
BADPWP	S	Invalid password for program launch
BADPWV	S	Invalid password for reset mode
BADPWX	S	Invalid password for Full Control exit
CHPWDE	S	Used emergency password N to gain access
CHPWDP	S	Program Password Changed
CHPWDS	S	Setup Password Changed
ADVSRY	S	Full Control component load failed: <component>
ENDAPT	M	Managed Program Terminated: Program/User Timeout
ENDAPU	M	Managed Program Terminated By User
ENDANM	M	Non-managed Program Terminated
ENDNWR	S	NoWrite App Terminated: logging active again
ENDSES	S	End Of Full Control Session
ESETUP	S	Entered Setup Mode
FILACC	S	File Control access denied
FILACD	S	Window Control file access denied due to Allowed Folder restrictions
MTRSBD	S	<metered-app startup bad, see its error message>
MTRSNS	N	Metered app startup denied: no more allowed
MTRSOK	N	Started metered application (now has N users)
MTRXBD	S	<metered-app exit bad, see its error message>
MTRXOK	N	Terminated metered application (now has N users)
STRAPP	Z	Managed Program Started
STRANM	Z	Non-Managed Program Started
STRNWR	S	NoWrite App Started: no logging until it exits
STRSES	Z	Start Of Full Control Session
TIMUSR	S	Users that ran out of time
USRNME	S	Logon name of user: from FULLCTL env variable
USRNMR	S	Logon name of user: from Registry
USRNMW	S	Logon name of user: from Windows (normal method)
WEBBRN	Z	A new Web browser window was opened
WEBBRX	W	Web Browser Exit: browser window closed
WEBPGC	W	Web Browser Page Change: title of page
XSETUP	S	Exited Setup Mode

The "num" field generally, though not always, shows the number of minutes at the time this log record was generated. The meaning of the "num" field is:

S: minutes in session

M: minutes in managed program

N: current number of users running metered application

T: logon program switched Full Control to this target user number

W: minutes in browser window (WEBBRX) or at website (WEBPGC)

Z: will always be zero for this record type

For WEBxxx records, the App field contains the URL and title of the visited website logged by this record.

If the Event Log "tests and diagnostics" box is checked, the logfile may contain further information useful to Bardon support personnel in diagnosing problems.

---

## License Meter Manager File Format

The license meter data file is plain text, and can be edited by hand. However, it is much easier to use the License Meter Manager program to manipulate this file. The file format information given here is for reference and to describe how the data can be used. WinU and Full Control do not manipulate this file directly, and it should not be in a location visible to anything except the License Meter Manager program. Consider this license file:

```
[Word 95]
maxAllowed=125
currInUse=2
Full Control computer name 1023452=1
Some other Full Control computer name=1
```

```
[Lotus]
maxAllowed=30
currInUse=2
Some other Full Control computer name=1
Another Full Control computer=1
```

```
[Netscape]
maxAllowed=50
currInUse=1
Another Full Control computer=1
```

As you can see, each entry is in its own section, each with its own header. The sections do not have to be sorted by application name. Below the header are the section's entries; there are two permanent entries per section, plus the names of the computers that are currently using a license. Blank lines between entries are acceptable. However, there can be no blank spaces at the beginning of a line, or surrounding the equals-sign.

The text in brackets is the section header. This is the license key name, the lookup key for this licensed application which is specified as the meter key in the monitored program's Advanced Settings screen. Perhaps this is the name of the program, but it can be any text you choose.

The two entries *maxAllowed* and *currInUse* show the maximum and the current number of users. The *maxAllowed* entry is a fixed number. The *currInUse* entry is kept up-to-date by the License Meter Manager to reflect the number of users who are simultaneously running this program at the present time. If a launch request comes in but there are no "slots" left, the associated program will not be allowed to run. In the above example, no more users can access Netscape until one of the current users exits.

This method can with equal ease monitor license counts for applications loaded from a server or from a local workstation. You can even monitor an Office-type suite of applications. To meter a software suite, give all the programs in the suite the same license key name. If a user is already running one component of a suite, that user will be allowed to launch any other metered program that uses the same license meter key name.

# Miscellaneous

---

## Software License and Warranty

Your use of Full Control confirms your agreement to be bound by this license and warranty. As used here, Full Control ("the software") means all or any portion of the computer application contained in this package, and all updates. The software is owned by Bardon Data Systems and is protected by United States and international copyright and trade secret laws, and international trade provisions. You must treat it like any other similarly protected material. This license and your right to use Full Control terminate automatically if you violate any part of this agreement. In the event of termination, you must immediately destroy all copies of the software or return them to Bardon Data Systems.

1) You are welcome to use the "test-drive" evaluation version of the software for 30 days. That is, you can run the program 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. This gives you plenty of time to try Full Control on your own system. 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 these conditions: a) none of the files in this package may be modified or deleted; and b) distributors must stop distributing the software if asked to do so by Bardon Data Systems.

2) After purchasing, Bardon Data Systems grants you a non-exclusive license to use one copy of the software, on one computer, and make one copy of it for archival purposes. For purposes of this section, "use" means loading the software into RAM, as well as installation on a hard disk or other storage device. You may access the software from a hard disk, or any other method you choose, so long as you otherwise comply with this agreement. 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 arranged in advance for a 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 such that the software is exploited in a commercial way; or sublicense, rent, lease, or otherwise market the software. You may permanently transfer the software to another owner only by providing written notice of such transfer to Bardon Data Systems.

3) An upgrade replaces a previous version. It does not provide an additional license. When upgrading you must cease using the previous version, and also ensure that it is not used by anybody else.

4) The software can be returned for refund within thirty days of the purchase date, when accompanied by a return authorization number which has been obtained from Bardon Data Systems. Shipping/handling fees are not refundable.

Bardon Data Systems warrants that the software distribution disk will remain free from defects for 90 days after you have received the software. In the event of a breach of this warranty, Bardon Data Systems will, at its option, either replace the disk or refund the software purchase price. Bardon Data Systems 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.

This warranty is in lieu of all other warranties, either expressed or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to the software, or the documentation, or fitness for a particular purpose. Bardon Data Systems shall not be liable in any event for special, incidental, or consequential damages in connection with, or arising out of, the furnishing, performance, or use of the software, including any lost profits or lost data, even if Bardon Data Systems has been advised of the possibility of such losses or damage.

Some states do not allow the limitation or exclusion of liability for incidental or consequential damages. If so, the above limitations may not apply to you. In no case shall any liability exceed the purchase price for the software.

This agreement shall be governed by the laws of the State of California and shall inure to the benefit of Bardon Data Systems and any successors, administrators, heirs and assigns. Any action or proceeding brought by either party against the other arising out of or related to this agreement shall be brought only in a State or Federal Court of competent jurisdiction located in Alameda County, California. The parties hereby consent to in personam jurisdiction of said courts.

Bardon Data Systems may revoke any permissions granted here, by notifying you in writing. All rights not expressly granted here are reserved to Bardon Data Systems. This agreement can be modified only in writing by a document signed by both you and Bardon Data Systems.

**U.S. GOVERNMENT INFORMATION:** Use, duplication, or disclosure by the U.S. Government of the computer software and documentation in this package shall be subject to the restricted rights applicable to commercial computer software as set forth in subdivision (b)(3)(ii) of the Rights in Technical Data and Computer Software clause at 252.227-7013 (DFARS 52.227-7013). The Contractor/manufacturer is Bardon Data Systems, 1164 Solano Ave #415, Albany CA 94706.

---

## **Frequently Asked Questions**

There is an extensive list of Frequently Asked Questions on the Bardon website ([www.bardon.com](http://www.bardon.com)), covering both configuration and troubleshooting. The digital format makes it easy to find the information you need. We hope you will find this information of interest.

---

## Notices

**VERSION:** Full Control version 2.11

**SYSTEM REQUIREMENTS:** Requires Windows 95, 98, ME, NT, 2000, Or XP. If using Windows NT, Service Pack 3 or higher is strongly suggested.

**TECHNICAL SUPPORT:** For technical support, contact Bardon Data Systems through Internet email ([support@bardon.com](mailto:support@bardon.com)), the World Wide Web (<http://www.bardon.com>), U.S. mail (Bardon Data Systems, 1164 Solano Ave. #415, Albany CA 94706), fax (510-526-1271), or telephone (510-526-8470). Telephone support is available during normal business hours, 9 to 5 weekdays California time.

Software and documentation protected by trade secret provisions and copyright 1998,2003 Barry Smiler, Bardon Data Systems, 1164 Solano Ave. #415, Albany CA 94706.

---

## Index

### %

%COMPUTERNAME%, 25, 50, 52, 62  
%CURRTIME%, 25, 50, 52, 53, 62  
%GROUPNAME%, 25, 50, 52, 55, 62  
%USERNAME%, 25, 50, 52, 53, 55, 62

### A

Active desktop, 44, 45  
Administration manager, 4, 6, 8, 21, 23, 27, 33, 34, 35, 40, 47, 59, 64, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76  
Administration screen, 16  
Administrators, 16, 18, 20, 59, 85  
AutoRun, 22, 42, 56, 65

### B

Blockout periods, 37

### C

CD-ROM, 22, 32, 40, 41, 65, 82  
Checkpoint. See Rollback  
Cloning, 4, 7, 8, 9, 11, 25, 33, 42, 43, 59, 61, 62, 63, 65, 67, 74, 76  
Computer name, 19, 25, 62, 63, 64, 66, 68, 70, 81, 83  
Control panel, 10, 13, 18, 45, 65  
Ctrl+Alt+Del, 4, 20, 21, 22, 27, 47, 48, 65, 73, 82

### D

Default group, 5, 7, 10, 17, 18, 19, 37, 60, 63  
Default user, 7, 13, 17, 21  
Desk access, 37

Desk setup, 37  
Desktop icons, 10, 37, 44, 45, 47  
Diagnostic snapshot, 4, 15, 27, 41  
Diagnostic snapshot logging, 4, 27  
Display restrictions, 4, 11, 42, 43, 62, 63, 64  
DOS, 6, 7, 20, 21, 22, 29, 31, 34, 35, 36, 38, 40, 41, 57, 60, 65, 70, 73, 74, 79, 80

### E

Emergency passwords, 12, 30, 82  
Enhanced startup protection, 20, 23  
Event logging, 3, 4, 5, 19, 24  
Explorer, 8, 10, 13, 25, 33, 41, 44, 45, 46, 47, 48, 52, 60, 64, 66, 69

### F

File control, 3, 17, 22, 26, 31, 32, 37, 45, 47, 51, 53, 55, 60, 62, 82  
File formats, 81  
FULLCTL environment variable, 21, 82

### G

Group setup, 3, 5, 11, 17, 37, 56, 63, 70, 71, 79

### H

Hotkey, 5, 10, 12, 16, 22, 24

### I

Input control tab, 37, 45  
Installation, 3, 4, 6, 7, 8, 9, 10, 13, 22, 35, 57, 61, 68, 70, 73, 75, 76, 78, 85  
Interface tab, 44  
Internet software, 66

## L

License meter management, 4, 6, 57, 58, 59, 77, 78, 83  
Logging, 3, 4, 5, 6, 8, 9, 10, 11, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 32, 33, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 55, 56, 57, 59, 60, 61, 62, 63, 65, 66, 67, 68, 69, 70, 71, 72, 74, 75, 76, 79, 80, 81, 82  
Logoff, 4, 14, 16, 48, 74, 80  
Logoff applet, 79, 80  
Logon, 3, 4, 5, 9, 10, 13, 17, 18, 20, 21, 22, 23, 25, 37, 40, 41, 42, 47, 48, 49, 50, 52, 53, 56, 60, 61, 62, 63, 65, 68, 69, 70, 72, 81, 82  
Logon validation, 13, 17, 20, 23, 63  
Long file names, 34, 68, 70, 78

## M

Managed programs 3, 7, 10, 11, 15, 17, 22, 24, 26, 30, 32, 34, 37, 38, 40, 41, 42, 43, 49, 51, 56, 57, 58, 59, 61, 62, 63, 65, 77, 82  
Meter manager, 8, 57, 77, 78, 84

## N

Netware, 23, 67  
Networks, 4, 5, 9, 10, 11, 13, 14, 18, 19, 20, 21, 22, 23, 25, 33, 34, 35, 37, 45, 46, 47, 50, 52, 53, 54, 57, 59, 61, 62, 66, 67, 68, 70, 71, 74, 75, 77, 78, 84  
NT, 2, 3, 4, 6, 8, 20, 21, 23, 30, 34, 36, 39, 40, 46, 47, 67, 75, 76

## P

Passwords, 3, 4, 10, 11, 12, 13, 14, 15, 16, 19, 20, 22, 23, 24, 26, 30, 35, 38, 41, 42, 43, 47, 48, 60, 61, 65, 68, 69, 70, 78, 82  
Printer, 4, 5, 19, 24, 25, 26, 28, 30, 33, 45, 66, 82

## R

Registry, 4, 6, 7, 35, 36, 38, 67, 69, 73, 74, 82  
Remote administration, 4  
Remote management, 19, 33, 35  
Reports, 3, 4, 5, 10, 11, 16, 17, 19, 24, 25, 26, 27, 28, 29, 31, 32, 51, 55, 59, 66, 67, 72, 75, 81  
Reset mode, 64  
Reset program, 5, 6, 10, 12, 16, 22, 24, 64  
Right mouse, 46, 47  
Rollback, 3, 4, 11, 16, 19, 35, 36  
Run securely at startup, 20

## S

Safe Mode, 3, 10, 20, 23, 38  
Security considerations, 60  
Send keystrokes, 52  
Settings, 3, 5, 7, 8, 9, 10, 11, 12, 13, 17, 18, 19, 21, 24, 33, 34, 35, 37, 38, 39, 41, 42, 43, 44, 45, 47, 48, 51, 52, 54, 56, 58, 59, 60, 61, 62, 63, 65, 67, 68, 71, 73, 74, 76, 78  
Setup mode, 3, 12, 16, 17, 20, 22, 24, 41, 44, 48, 64, 82  
Setup password, See Password  
SMS, 8, 9  
Start button, 6, 10, 14, 16, 37, 41, 44, 47, 48, 65, 80  
System administration, 4, 10, 12, 59, 64, 78  
System setup, 3, 5, 10, 11, 16, 17, 19, 34, 36, 61, 66, 68, 75, 81

## T

Taskbar, 3, 4, 10, 14, 15, 16, 22, 39, 40, 44, 47, 48  
Time control, 37, 49  
Tray icon, 4, 10, 12, 14, 15, 16, 22, 24, 41, 42, 48, 65, 71

## **U**

Uninstall, 4, 6, 7, 8, 70, 76

## **W**

Web browser, 3, 5, 10, 24, 26, 46,  
47, 55, 56, 66, 82

Window control, 37, 50