Full Control Help

Choose a topic on which you'd like more information:

Introduction

Full Control is a complete Windows 95/98 security access control system. It includes software access management, time limits, logging, web-browser tracking, remote administration, and many flexible configuration options. Full Control provides effective, reliable access control while still allowing use of the regular Windows 95 desktop. With Full Control, businesses can let employees use authorized applications, yet 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.

Solid security protection: Full Control provides reliable security coverage for your Win95 computer, 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 the number of pages that can be printed, 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. It also logs all software usage, the number of pages printed from each workstation, 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 rollback: Full Control can track changes to the Registry, system files, or applications, allowing you to "roll back" your system configuration 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.

Full Control works very well with Bardon's free Remote Commander utility, with which administrators can run commands from one central location on any Full Control computer on the network -- installers, maintenance programs, batch files, or any other software. The Remote Commander is available from the Bardon Data Systems website (http://www.bardon.com). It is also included with all purchased copies of Full Control.

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, number of pages printed and maximum pages allowed, and a menu with password-protected setup and session options. Full Control can also display a User Information window listing the current time control and pages-printed statistics.

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 a number of other utilities, including our free Remote Commander add-on, with which administrators can run commands from one central location on any Full Control computer on the network.

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

The User Setup screen controls per-user options. Each user can have different time limits, locked or hidden directories, allowed applications, desktop look-and-feel options, printer limits, and more. The user logs on at the regular Windows logon screen. If Full Control has per-user settings listed under the name given at logon, those settings are put in place for that user. If the Windows logon name is not listed, Full Control uses its Default User settings.

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.

How To Order Full Control

Thank you for trying Full Control. You are welcome to test the evaluation version for 30 days. These 30 days do not have to be consecutive calendar dates. If you don't run Full Control 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 Full Control or remove it from your system.

Click Here To
Print An Order Form

Full Control can also be purchased from distributors in:
AUSTRALIA: Comput-Soft
ENGLAND: The Thompson Partnership
GERMANY: Vogel Datentechnik
NETHERLANDS / BELGIUM: CopyCats
NEW ZEALAND: PC Support Services

When you order, you'll get a disk with the most recent version of Full Control, a printed manual, and a license number that will unlock the software.

Quantity discounts and educational pricing are available. Contact Bardon Data Systems for further information on this.

To order, send $49.95 for each copy (plus $5 shipping/handling) to:

Bardon Data Systems
1164 Solano Ave. #415
Albany, CA 94706

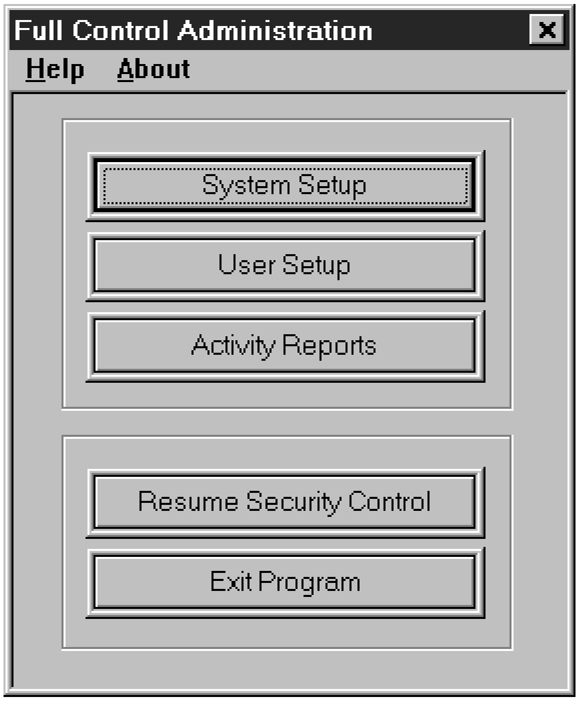
We also offer a **Maintenance Plan** which includes all Full Control upgrades for one year, plus other benefits. $24.95 per single copy, less in quantity. Contact Bardon Data Systems for further information on this.

Payment: You can pay with cash, check, money order, or major credit card (MasterCard, Visa, American Express, or Discover/Novus). We accept checks in US Dollars, drawn on a US bank and requiring no additional collection or currency-conversion fees.
Shipping: Please enclose $5 for shipping and handling.
Sales Tax: California residents please add 8.25% sales tax ($4.12).
Purchase Orders: Purchase orders are accepted from most organizations within North America. Terms are net 30 days from date of order, unless arranged otherwise in advance. For orders under $100, please add an additional $10 processing fee if using a purchase order.

More Ways To Order: With a credit card you can also order Full Control by **phone** at 510-526-8470 or on our **tollfree *ORDERS-ONLY* line** at 800-92-BARDON [800-922-2736] weekdays 9 to 5 California time, or by **fax** at 510-526-1271 24 hours a day. Order on the **World Wide Web** at the Bardon Data Systems homepage at **http://www.bardon.com**. The webpage is also the best place to get the very latest version of Full Control, as well as other software from Bardon Data Systems. With a credit card you can also send email to **orders@bardon.com** with your credit card number, expiration date, and name as it appears on the card.

If you order **with a credit card by phone, you'll be given your license number immediately** so you can get rid of the reminder screens and limitations right away. Or simply mail in your credit card number and expiration date.

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, 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 temporarily suspended. This makes it easier for the administrator to configure the system. To return the system to its previous security mode, choose Resume Security Control.

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

About: Full Control version and other information

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

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

Activity Reports: This menu item provides a shortcut to the Reports tab of the System

Setup dialog.

Resume Security Control: This exits from Setup Mode.

Exit Program: This closes Full Control and clears all security access restrictions.

Notices

VERSION: Full Control version 1

SYSTEM REQUIREMENTS: Requires Windows 95 or Windows 98

TECHNICAL SUPPORT: For technical support, contact Bardon Data Systems through Internet email (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 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.

Installing And Uninstalling

To install Full Control, run the program **install.exe** that comes with Full Control. It will ask you the folder you would like to install into and the Start button group name you prefer. The installer will not put anything into any folder other than the one you specify. It will not change any system files other than the Registry (per Microsoft standards). If you choose to uninstall, simply run the uninstaller program.

Full Control installs the following files to the folder you choose:

fc.exe	the Full Control program, file 1
fc2.exe	the Full Control program, file 2
fc3.exe	the Full Control program, file 3
fc4.dll	the Full Control program, file 4
fc5.dll	the Full Control program, file 5
fc6.exe	the Full Control program, file 6
fc7.dll	the Full Control program, file 7
bardon1.vxd	another part of the Full Control program
fcreset.exe	companion Reset program
uninfc.exe	the Full Control uninstaller
fc.hlp	the documentation, in Windows helpfile format
fc.cnt	another part of the Windows helpfile
validm.dll	license meter management engine
readme.txt	overview and installation instructions
license.txt	terms of Full Control's usage license
homepage.url	shortcut to Bardon's website
msgmgr.exe	Message Manager program
metermgr.exe	License Meter Manager program
adminmgr.exe	Remote Administration Manager program
extract.exe	Data Extractor builds files used by Full Control tools
logoff.exe	Logoff applet

Remote Commander: Full Control works very well with Bardon's free Remote Commander utility, with which administrators can run commands from one central location on any Full Control computer on the network -- installers, maintenance programs, batch files, or any other software. The Remote Commander is available from the Bardon Data Systems website (http://www.bardon.com). It is also included with all purchased copies of Full Control. It's best to install it to the same directory as Full Control itself, so the Remote Commander can use the regular Full Control helpfile. To do so, simply copy the program (remcmdr.exe) to the Full Control directory.

Default User: The first time you run Full Control after installing, Full Control creates a Default User with a few managed programs. This lets you use Full Control and get a feel for what it can do.

Registry Backup: At the start of each session, Full Control backs up the current Registry files to *userfc.bds* and *sysfc.bds* in your Windows directory (c:\windows on most computers). These are backup copies of *user.dat* and *system.dat*, the two files which contain the Windows Registry entries. In addition, the first time you run Full Control, it creates the files *userfc.1st* and *sysfc.1st* in your Windows directory. 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 to *user.dat* and *system.dat* in your Windows directory.

Uninstalling: When you install, Full Control's uninstaller is added to Full Control's icons on the Start menu. It can also be run from the Start menu's Add/Remove Programs list. Before uninstalling, remember to set back any systemwide options (such as desktop shortcuts or options access) as you prefer them. Please note that to cleanly uninstall, the uninstaller must be used. It is not sufficient to simply delete the Full Control files.

Automated Unattended 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:

/auto if parameter is given, installer runs in automated mode
/addstart if parameter is given, icons will be added to the Start menu
/targetdir= full path to the folder into which files should be installed

Example: install.exe /auto /addstart /targetdir=c:\somedir\otherdir\finaldir

Command-line parameters can be given by running the installer from a batch file, Shortcut, etc. Tools such as SMS can run such a batch file or Shortcut on remote computers across the network. Without such a tool, one way to do an unattended network install is to copy the files on the Full Control disk (or download) to a network directory, then place in each remote computer's Startup folder a batch file similar to the following:

```
        \\server\c\temp\fcsetup\install.exe /auto /addstart /targerdir=c:\Program Files\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.

Full Control Quick Start

Overview: 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 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 95 logon screen) to see if it has a set of restrictions, time limits, and managed programs specified for that user. If that user name is not found, Full Control imposes its Default User 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, run Full Control's companion Reset program to access the setup options.

System Administration: 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.

Here's how to quickly set up Full Control:

- Can unknown users log on, or must users 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 details on this.) You don't have to tell Windows to save a different configuration for each user; all that is needed is the logon name screen itself. But even if you don't use the logon screen at all, Full Control will work perfectly well. It will then use its Default User 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.

- Create new users by clicking the Administration screen's User Setup button. This displays the Choose User screen. Click the Add button and Full Control will create a new user with default settings, then display the User Setup screen. Use this screen to add managed applications and configure the new user's restrictions and time limits to your liking. Later, you can use the User Setup screen to update this user's settings at any time.

- You may want to make a copy of this user, including all configuration settings, and use the copy as a base which can be modified to suit some different need.

- You may want to copy managed programs from one user to another, or to all users at once.

- When the computer is configured as needed, you may want to create a clone configuration 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. However, 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.

- If you will be cloning this computer's Full Control configuration and replicating this cloned 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.

Using the Windows Logon Screen

When you boot your computer, do you see a logon screen 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.

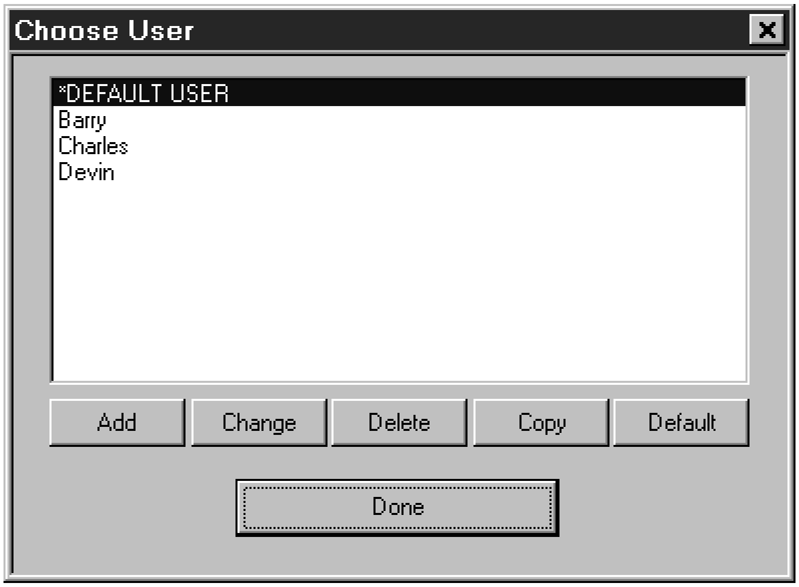
To set this up, open the Network applet of the Windows Control Panel. As your Primary Network Logon, choose anything other than Windows Logon. For standalone computers or those using Windows networking, *Client for Microsoft Networks* is a good choice. If it's not already on the list, click the Add button 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, choose *Shut Down*, and 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.

Choose User



The Choose User screen is displayed by clicking the User Setup button on the Administration menu. This screen lists all users whose logon names have been given individual settings. It also provides access to Full Control's default-user settings.

With this screen, administrators can select the user settings to modify. Select the desired user, 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 names shown in this list are the same user names which the user types in at the regular Windows 95 logon screen. If the name given at the Windows 95 logon screen matches a name on the Choose User list, Full Control uses the settings you have given for that user name. One way of using Full Control's logon validation 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 95 logon screen, Full Control uses its Default User settings. The Default User settings can be modified, but they cannot be deleted.

If you want the Windows 95 logon screen to be displayed when Windows starts, set this using the Network applet of the Windows 95 Control Panel.

The functions available on the Choose User screen are as follows:

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

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

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

Copy: To make a copy of a user's settings, select that user from the list and click the Copy button. That user's settings will be copied. The name of the new user will be "Copy of <the original name>". The new user's setup screen will be displayed, allowing you to change this name or any other settings.

Default: To copy any user's settings into the Default User's slot, select that user from the list and click the Default button. That user's settings will be copied to the Default User. Unlike the Copy button, a new user is not created. Clicking the Default button simply copies the selected user's setting to the Default User.

Frequently Asked Questions

These questions often come up when configuring Full Control.

How do I add a new user?

To add a user, bring up the Choose User screen and click the Add button. After giving your setup password, a new user will be created with default settings, ready for you to modify as needed.

How can I control which users can log on?

Use the logon validation options on the first tab of the System Setup screen. You can set this to allow access only to users know to Full Control, or only to users known to Windows.

How do I set time limits for a user?

On the Administration screen, click the User Setup button and choose a user. Go to the Time Control tab. In the Total Minutes Allowed box enter the number of minutes allowed for this user. In the Current Minutes Used box enter the number of minutes currently used up for this use (you will generally set this to zero). In the Grace Period box enter the number of minutes before timeout at which Full Control will show its warning screen and play its warning sound. Both the warning screen and the warning sound can be disabled from any program's Advanced screen, which is helpful if that program cannot tolerate sounds or popup messages from other applications. Choose how often the maximum time will be reinitialized. Every day at midnight? Every week at Sunday midnight? Every time the user logs on to the user? Never? Up to you.

What should happen when a user runs out of time? Use the Security Settings tab of the System Setup screen to choose whether to logoff the user, shut down the computer, or display a "no time left" screen and prevent access to anything other than that screen.

How can I prevent users from using Ctrl+Alt+Del?

Full Control can completely disable Ctrl+Alt+Del, or password-protect it. To set this up, select the user to which you want to add this protection. On the Input Control tab, check the box to disable Ctrl+Alt+Del. If you don't give a password, when the user presses Ctrl+Alt+Del nothing will happen. If you do give a password, when the user presses Ctrl+Alt+Del the password box is displayed. If the user gives the Ctrl+Alt+Del password, the regular Close Programs box appears.

How can I prevent users from using Safe Mode?

Full Control can password-protect Safe Mode. To set this up, go to the Security Settings tab of the System Setup screen. Check the box to run Full Control securely at startup, then check the box next to it which controls Safe Mode protection. With these in place, the Full Control setup password is required to use Safe Mode.

How can I prevent users from starting the computer in DOS?

There are two parts to preventing a user from starting the computer in DOS. The first of these is to set up Full Control to disable the keyboard at startup. The second part is to change your computer’s boot sequence in your CMOS so it tries to boot from your C: drive before your A: drive. To disable the keyboard at startup, start Full Control and go to the Security Settings tab. Make sure the option to *Allow startup menu and function keys to be used at bootup* is not checked. Click OK to save your settings.

Changing the computer’s CMOS boot sequence is system dependent. Accessing your CMOS is usually accomplished by pressing the DELETE or F10 key during the boot-time system memory test (the first screen you see when your computer starts). Once in setup look for ‘boot sequence’ or ‘boot order’. This specifies the order in which your drives are accessed. Change the boot sequence from A,C to C,A. This will cause a boot disk in the A drive to be ignored at boot-time (unless there is no C drive). You should also password protect your CMOS to prevent anyone from changing these settings back. Be very careful when changing your CMOS settings. Doing the wrong thing can render your computer inoperable. If you are not comfortable doing this yourself, you may want to contact your computer manufacturer or an experienced hardware service technician.

What is a managed program?

A managed program is one that is listed on a user's Managed Programs tab. It can have a password, time limits, restart control, and other settings. If it uses a modem, Full Control can hang up the phone on termination. If desired, Full Control can terminate managed programs when the user runs out of time.

What is a non-managed program?

A non-managed program is any running application which is not listed on a user's Managed Programs tab. Non-managed programs are logged when they start and end, but no other control is imposed. If desired, Full Control can terminate non-managed programs when the user runs out of time.

How do I add a managed program to a user's settings?

Start Full Control and click on the Full Control tray icon (next to the clock on the taskbar). Select *Setup Options* from toe popup menu to go into Setup mode. If the tray icon is hidden, run Full Control's companion Reset program to access the setup options. Choose a user and click Change to open the User Setup screen, then flip to the Managed Programs tab. Enter the Program Label, the Executable File, and any other settings you want, then click the Add button at the bottom of that tab.

What is an Allowed Application?

Full Control can restrict the programs which can be run by a user. Applications listed as Managed Programs are always allowed to run, subject to their individual time and password restrictions. As for other programs, if the User Access tab's restrictions have been activated, other ("non-managed") programs can be run only if they are listed on that tab as Allowed Applications. See the discussion of that tab's features for more options when setting up Allowed Applications.

How do I clone a Full Control computer's entire configuration onto another machine?

You can easily clone Full Control installations. Set up Full Control once, on one machine, the way you want it with all desired settings and programs. Then use the clone feature on the Remote Management tab of the System Setup screen to take a "snapshot" of that installation and save it as a *clonefc.bds* file. You can install that "snapshot" setup to other machines in a single step. Of course, to use the same managed programs the other machines have to have the same applications in the same-named directories, etc.

How do I save a computer’s Full Control configuration "snapshot" to a clone data file?

To create a file which contains all the settings of the one master computer (the one you want to copy), first set up the master computer with all the users and settings you want. On the Remote Management tab of the System Setup dialog, click *Export Clone File Now*. After exiting the setup dialog, the clone data file will be saved into the named AutoUpdate folder, or to the Full Control program’s directory if no AutoUpdate folder has been specified. By default this file will be named *clonefc.bds* which is the name needed by Full Control's AutoUpdate processing.

How do I use a clone data file to copy settings to a second computer during installation from a floppy disk?

Using Windows Explorer (or any other method) copy a clone data file named *clonefc.bds* to the Full Control install floppy disk. Make sure there is enough extra room on the floppy disk for the installer to create a few small temporary files. Install Full Control from the Full Control install disk. Because you have copied *clonefc.bds* to the same directory as the install program (install.exe), you will be asked during installation if you wish to copy the clone information to the new computer. After installation, the new computer will have the same Full Control settings as the master system.

How do I install Full Control from a network? Can I use a clone data file to copy settings while installing?

You want to run the Full Control installer from a network directory which is visible on the target computer (the one you want to install onto). If a *clonefc.bds* file is in the same directory as the installer, the installer can copy that clone file's settings to the new computer. To do this, copy all the Full Control files (from the install disk or download) to a network directory which is visible on the target computer. On the target computer, change to that network directory. Double-click on install.exe. The installation process will begin. At one point you will be prompted for the directory to which you wish to install. You must choose a directory on the target computer. Full Control will not run if installed to a network directory. If you have also placed a clone data file named *clonefc.bds* into the same directory as the Full Control installer program, you will be asked during installation if you wish to copy the clone information to the new computer. Note that if copying settings from one computer to another, all programs/files must be in the same location on each machine. For example, if Full Control on one computer lists FancyFax as a managed program using c:\program files\fancyfax.exe as the 'Executable File', each computer must have the FancyFax executable under c:\program files\fancyfax.exe.

How do I use a clone data file to dynamically update all my site's computers in a networked environment?

You want to make a clone data file named *clonefc.bds* visible to all the target computers, and set up the target computers to update themselves when they see the *clonefc.bds* file. To do this, save the settings of the master computer (the one you want to copy) to a clone data file. This is described above. Make sure the target computer (the computer to be updated) is monitoring a network folder for clone update files. To do this, on the Remote Management tab check the *Look for clone updates* box and give the data-source folder name. This computer will now monitor that folder for *clonefc.bds* files whenever you start Full Control.

On the Remote Management tab, what's the difference between *Look for clone updates* and *Always update*?

Look for clone updates will update Full Control's settings whenever a new clone file (named *clonefc.bds*) is placed in the AutoUpdate folder. *Always update* will update Full Control's settings at every startup regardless of whether the clone file has been read previously.

After doing a clone update, what settings remain from the previous configuration?

A clone update replaces most settings, but not all. If a new AutoUpdate folder is not given in the clone information (or is given but doesn't exist) the old name is retained.

The filetime of the last timefile is retained so it will not be re-read. The Full Control computer name will not be changed. Remember that the logfile name can be dynamically created from the Full Control computer name at runtime by using the word %COMPUTERNAME% as part of the logfile name. You can also use the words %USERNAME% (user name given through current network or Win95 logon) and %CURRTIME% (a unique number based on the current time) here but they are not as useful.

How do I monitor World Wide Web usage?

Full Control can monitor all websites that are visited while Full Control is running. To activate this feature, use the Event Log tab to set up Full Control for logging, and check the *web browser monitor* box on that tab. 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. This information can be viewed through Full Control's built-in reports.

Can I give times of day when no programs can be run?

Yes. In addition to the restart control and cumulative time testing, you can also set per-user blockout periods, for example "Every Tuesday 9 pm to 11 pm" or "Every weekday 7:30 pm to 8:30 pm". A user can have any number of blockout periods. During these periods, no programs will run while that user is logged in, except those managed programs you have specifically allowed to run for a timed-out user.

How do I set time limits for a program?

Use the Administration screen to bring up the user that contains the program for which you wish to set a time limit. Go to the Managed Programs tab and select the application for which you wish to set a time limit. In the Minutes Until Warning box enter the number of minutes Full Control should wait before a time-out warning is issued. In the Minutes Until Termination box enter the number of minutes you would like the application to run. This number must be higher than the Minutes Until Warning. If you want the application to be inaccessible for a period of time after termination you can set the Minutes Until Restart Permitted. Click Change to update this program's settings.

When a program runs out of time, how do I prevent the user from just starting it again?

You can set up restart control for any managed program. This is done from the Managed Programs tab of the User Setup screen. Full Control won't let the user restart a program sooner than the restart time you've set up for that program. If this is set, then after a program is exited (or forcibly terminated by Full Control), it cannot be restarted again until that much time has passed. Program restart control, cumulative time limits, and blockout periods keep track of program and user usage regardless of logons and logoffs.

I want a certain program to run, but remain minimized. How do I do this?

To start a program at logon and keep it running throughout the user's session, set it as a Managed Program and, on the Advanced screen for that program, check the box labeled *AutoRun, then keep program running until logoff or timeout*. You can also, of course, put the program in the computer's Startup folder, but this can be bypassed by the user, and it does not keep the program running throughout the session.

To keep the program minimized, set Full Control's Window Control to look for that program's titlebar text and send such a window the keystrokes % N (percent, space, letter N). This sends an Alt+Spacebar to bring up its System menu, then N to activate the System menu's Minimize command.

How do I track system usage?

You can set up Full Control's built-in logging to track usage to the level of detail which is of interest to you. From the Administration screen choose System Setup and go to the Event Log tab. Indicate whether you want your logging records saved to a file, printed as they occur, or if you want only brief usage summary records printed. If saving to a file, give the logfile name. If the file does not exist it will be created. If printing log records, give the printer name. Select events to track under What To Log. Generally you will always want to check *Session and user events, Launching and monitoring managed applications, Launching and monitoring other (non-managed) applications, Password status,* and perhaps *Web browser activity*. You only need to check the other boxes if you are using the Full Control features they monitor.

How do I log all pages printed?

Full Control includes built-in logging which can track printer usage. From the Administration screen choose System Setup and go to the Event Log tab. Give a logfile name and set up to track system usage as described above. Check the *pages printed* box. If you simply want a total count of all pages printed from all printers, click the *Log all printers* button. This will provide a one-line report at each user logoff showing how many pages were printed by that user. If you want to know how many pages were printed from each printer, or if you want to track only certain specific printers, click the *Select printers* button and choose the printers of interest from the list that appears. This will provide a separate one-line report for each logged printer showing how many pages were printed from that printer by that user.

How do I limit the number of pages that can be printed?

To limit the number of pages that a user can print during each session, use the Input Control tab's *Pages Printed* controls. List the maximum number of pages that can be printed during each session, and the pagecount after which a warning will be displayed to the user.

How long do Full Control's message screens stay visible?

By default, Full Control's password screen will time out and go away after thirty seconds, but you can set this to a different value if you like. Full Control's big-font popup messages time out and go away after two minutes.

How do I prevent people from using Windows "common dialogs" as little Explorer windows?

Most Windows programs use the standard Windows "common dialogs" to open or save files. Presenting the same dialogs in all programs means that the user does the same thing in the same way in all programs. This is good. However, by default these Open and Save dialogs let the user right-click on any displayed file or program and change its attributes, or even run it. They also let the user delete selectd files with the Delete key. This is bad. To plug these security holes, Full Control can disable right-click menus and the Delete key in these common dialogs. They are also disabled in Explorer, on the Windows desktop, and in the most popular web browsers, for similar reasons.

Can I control whether the user can shut down or restart the computer from Full Control?

Yes. Go to the User Setup screen's Input Control tab. In the Start Button Options section, check the box labeled *Disable the Shut Down command*. If you want to allow password-protected logoff or shut down, provide passwords on the Input Control tab which can be used with Full Control's tray icon menu. Also, the setup password will always allow access to these menu items.

How do I know who ran what program? How can I see reports?

Full Control features detailed logfile tracking of events. It also has built-in usage reports and pie-chart graphs which summarize logfile information to let you see who is doing what. These reports can be viewed and printed.

When I try to run a program’s Help screen, Full Control closes the Help window. How do I fix this?

You have set up this user to not allow non-managed windows by window title. You need to list the titlebar text of one or more helpfiles as Allowed Applications, so Full Control allows them to run. To add this, start Full Control and choose User Setup. On the User Access tab click the button labeled *Allowed Window Titles*. In the Title textbox enter the actual title bar text of the helpfile you want to allow. To allow all standard helpfiles, enter *help* so the wildcards allow all windows with the word *Help* in their title. (Some helpfiles don't have the word *Help* in the title bar, for example some of the Microsoft Office helpfiles. In this case, add text that does appear in the title of such helpfiles.) Click Add, then click OK. Click OK again. Help should now run.

I had to do an abnormal reboot and now nothing will run.   What do I do?

If you have controlled Allowed Applications with the *strict* option, and if for any reason Full Control does not exit normally, 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.   They are listed below in the recommended order.

First, generally Full Control itself will still run, so just start Full Control and exit (immediately if you like).   Doing so will clear any leftover control settings.

If you cannot run Full Control in regular Windows 95, start your 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 95 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.   You may need to boot from a floppy disk to a DOS prompt 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 both sets of files visible so you can manipulate them.

My computer doesn't shut down properly.   What should I do?

Full Control offers three ways it can shut down your computer.   Strong Shutdown is the most secure, however some computers hang at exit when using the Strong method.   If this happens, try the Medium or Soft shutdown method.

A program acts cranky when Full Control is running.   How can I get Full Control to totally ignore it?

Full Control totally ignores system components such as the Taskbar or desktop. Sometimes it’s useful to treat an application as if it were a system component too (for example a fax monitor, proxy software, or antivirus application) if it doesn't respond well to Full Control's oversight monitoring.   To leave such a program completely undisturbed by Full Control, go to the first tab of the User Setup screen and list it as an *Allowed Filename* or *Allowed Window Title*.   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.

The Setup Password

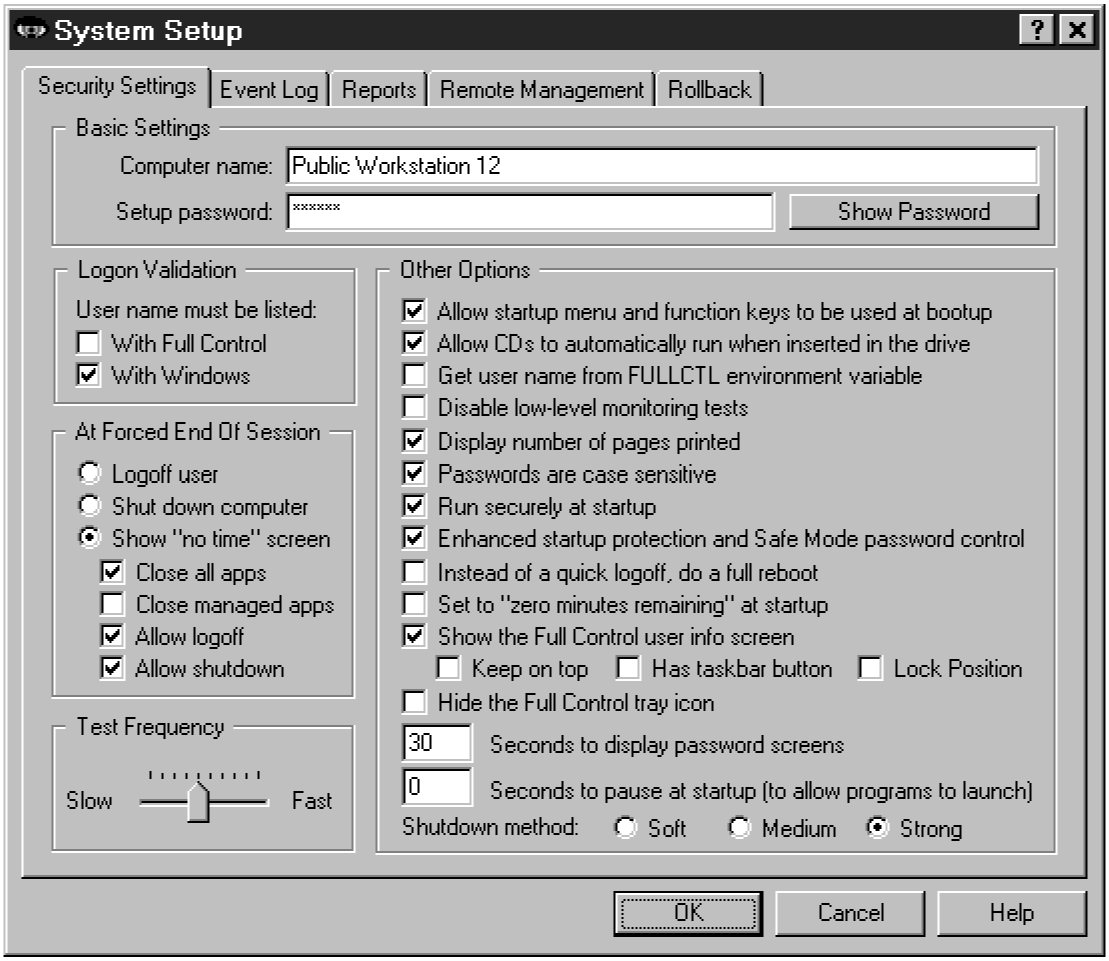
Setup Password: The first time you start Full Control, it asks you for a setup password. This password is saved permanently so you never need to enter one again if you don't want to. However, you can change the password at any time with the Security Settings tab of the System Setup dialog. Security experts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

The *case sensitive* setting of the Security Settings tab controls whether this password is case sensitive.

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."

System Setup Dialog



Basic Settings

Computer name: Public Workstation 12

Setup password: ******

Logon Validation

User name must be listed:

- ☐ With Full Control
- ☑ With Windows

At Forced End Of Session

- ○ Logoff user
- ○ Shut down computer
- ● Show "no time" screen
  - ☑ Close all apps
  - ☐ Close managed apps
  - ☑ Allow logoff
  - ☑ Allow shutdown

Test Frequency

Slow — Fast

Other Options

- ☑ Allow startup menu and function keys to be used at bootup
- ☑ Allow CDs to automatically run when inserted in the drive
- ☐ Get user name from FULLCTL environment variable
- ☐ Disable low-level monitoring tests
- ☑ Display number of pages printed
- ☑ Passwords are case sensitive
- ☑ Run securely at startup
- ☑ Enhanced startup protection and Safe Mode password control
- ☐ Instead of a quick logoff, do a full reboot
- ☐ Set to "zero minutes remaining" at startup
- ☑ Show the Full Control user info screen
  - ☐ Keep on top ☐ Has taskbar button ☐ Lock Position
- ☐ Hide the Full Control tray icon

30 Seconds to display password screens

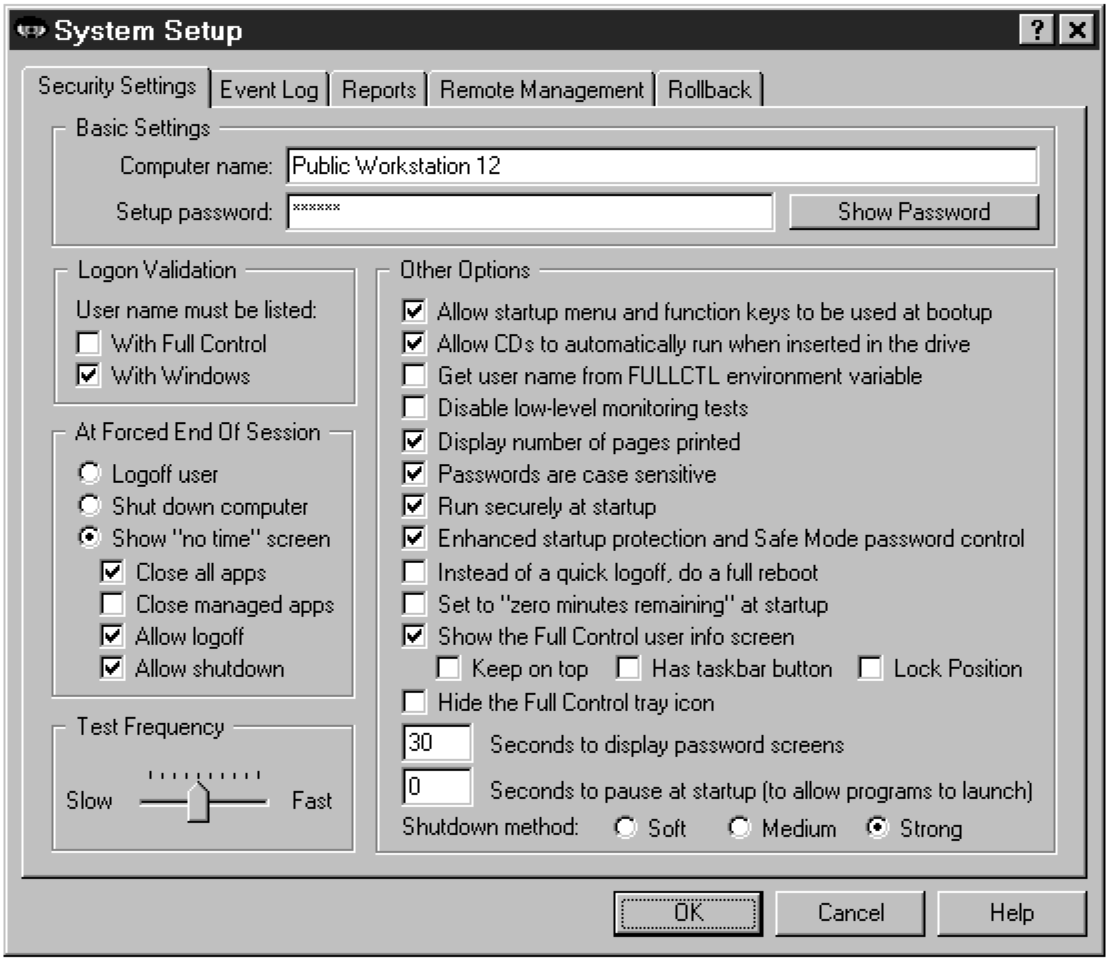
0 Seconds to pause at startup (to allow programs to launch)

Shutdown method: ○ Soft ○ Medium ● Strong

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 remote management, messaging, and configuration update
Rollback: save and restore important system configuration files

Security Settings Tab



Basic Settings

Computer name: Public Workstation 12

Setup password: ******

Logon Validation

User name must be listed:
☐ With Full Control
☑ With Windows

At Forced End Of Session
○ Logoff user
○ Shut down computer
● Show "no time" screen
☑ Close all apps
☐ Close managed apps
☑ Allow logoff
☑ Allow shutdown

Test Frequency

Slow Fast

Other Options
☑ Allow startup menu and function keys to be used at bootup
☑ Allow CDs to automatically run when inserted in the drive
☐ Get user name from FULLCTL environment variable
☐ Disable low-level monitoring tests
☑ Display number of pages printed
☑ Passwords are case sensitive
☑ Run securely at startup
☑ Enhanced startup protection and Safe Mode password control
☐ Instead of a quick logoff, do a full reboot
☐ Set to "zero minutes remaining" at startup
☑ Show the Full Control user info screen
☐ Keep on top ☐ Has taskbar button ☐ Lock Position
☐ Hide the Full Control tray icon

30 Seconds to display password screens

0 Seconds to pause at startup (to allow programs to launch)

Shutdown method: ○ Soft ○ Medium ● Strong

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 or written to the designated printer (or both). If you are administering a number of Full Control-equipped 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.

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 the box on this tab labeled *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 two ways that Full Control can validate this name. You can use one or both 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 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 password mechanism. If the user name was set up within the last 30 minutes, 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.

If either of these boxes is checked, Full Control does not let the user press Escape at logon, or bypass the logon process in any other way, such as pressing Ctrl+Esc to bring up the Task Manager, clicking on the Cancel button, or pressing Alt+F4 to exit.

At Forced End Of Session: Full Control can force a session to end for a number of reasons: per-user time limits, blockout periods, exceeding the maximum-pages printing limits, 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 below), 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, 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.

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

Allow startup menu and function keys to be used at bootup: This option 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 95 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.

Allow CDs to automatically run when inserted in the drive: Standard-issue Windows 95 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?

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.

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, disabling Ctrl+Alt+Del, and counting pages printed. Also, control of the Windows keys is not as strong.

Display number of pages printed: If checked, the Full Control tray icon's popup menu and the User Information screen (if displayed) will list the printed pagecount's running total and any maximum pages-printed limits you have set up.

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

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 starting in Safe Mode or pressing the Shift key when Windows comes up. If this box is checked, Full Control does not let the user press Escape at logon, or bypass the logon process in any other way, such as pressing Ctrl+Esc to bring up the Task Manager, clicking on the Cancel button, or pressing Alt+F4 to exit.

Enhanced startup protection and Safe Mode password control: Safe Mode is a special mode built in to Windows 95 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; if the password is not provided, the computer will reboot. Also, 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 comes up (as described above). And when this box is checked, an “extra” logon is not required to display the user’s allowed desktop icons which were set on the Interface tab (as described in that section).. To see this in action, try it both checked and unchecked. You’ll find the logon and desktop display process goes much more smoothly when this box is checked. Also, if this box is checked, Full Control does not let the user press Escape at logon, or bypass the logon process in any other way, such as pressing Ctrl+Esc to bring up the Task Manager, clicking on the Cancel button, or pressing Alt+F4 to exit.

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 computers on at the start of the day, and no one can use them until time is sent to the computer externally.

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.

Show the Full Control user info screen: If checked, Full Control displays a small screen showing program and user time limits, printed pagecount totals and printer limits. This screen is initially displayed in the upper right corner of the monitor. Checking the Lock Position box will keep it there. You can also keep the screen "on top" (visible above other windows) whether it is active or not, and control whether this screen has a taskbar button.

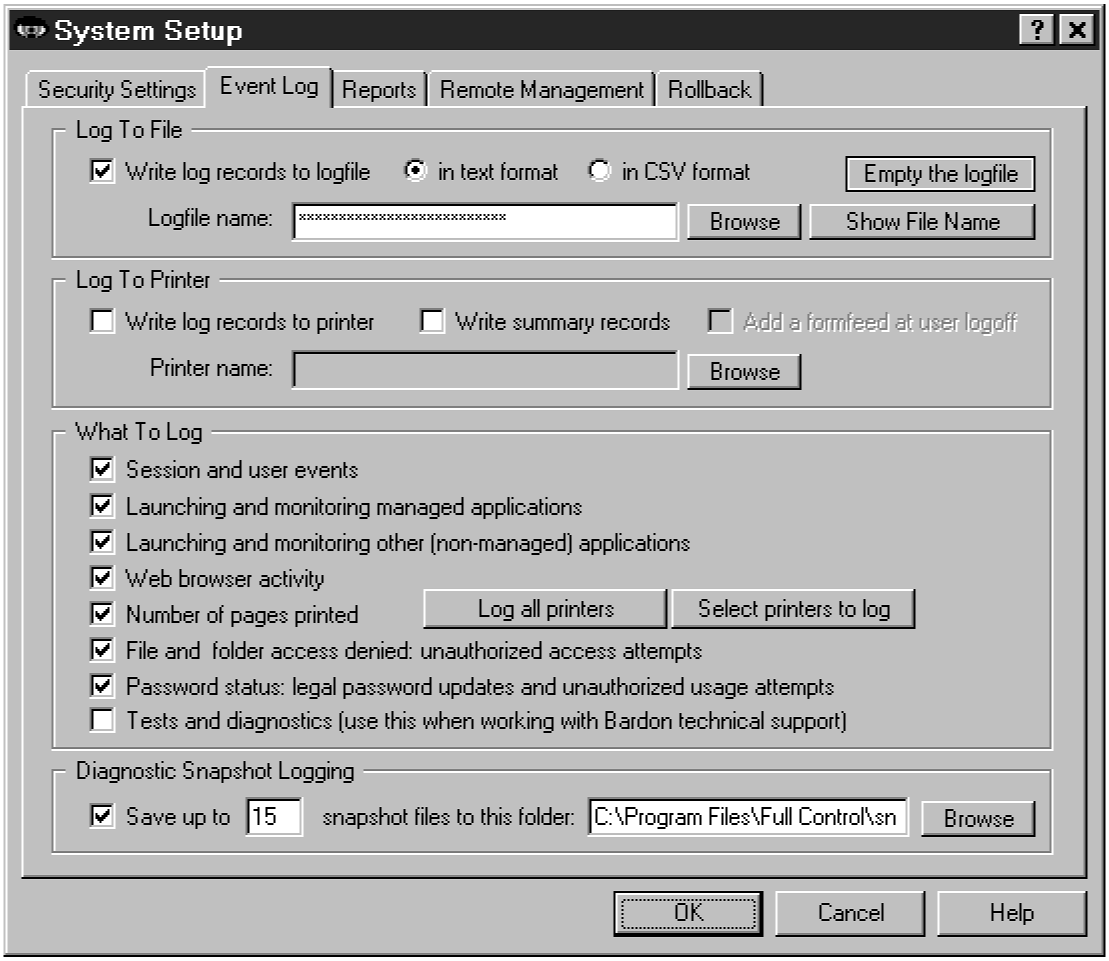
Hide the Full Control tray icon: With the tray icon hidden, there is no on-screen indication that Full Control is running. However, there is also no access to the tray icon's popup menu, so to configure Full Control when the tray icon is hidden run the Full Control Reset program (fcreset.exe), or start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

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.

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



System Setup

Security Settings | Event Log | Reports | Remote Management | Rollback

Log To File

☑ Write log records to logfile ● in text format ○ in CSV format [Empty the logfile]

Logfile name: ************************** [Browse] [Show File Name]

Log To Printer

□ Write log records to printer □ Write summary records □ Add a formfeed at user logoff

Printer name: [Browse]

What To Log

☑ Session and user events

☑ Launching and monitoring managed applications

☑ Launching and monitoring other (non-managed) applications

☑ Web browser activity

☑ Number of pages printed [Log all printers] [Select printers to log]

☑ File and folder access denied: unauthorized access attempts

☑ Password status: legal password updates and unauthorized usage attempts

□ Tests and diagnostics (use this when working with Bardon technical support)

Diagnostic Snapshot Logging

☑ Save up to 15 snapshot files to this folder: C:\Program Files\Full Control\sn [Browse]

[OK] [Cancel] [Help]

This tab is where you set up logging to file or a printer, 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. 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*.

Log To File: You can send logged events to any file on your computer or network. There are three ways to indicate the log file name to use. You can type in its name, use the *Browse* button, or "drag and drop" any file from Explorer onto this dialog. It will appear as the log file name. If you don't specify a full path to the logfile, your named file will be created in the same directory as the Full Control program.

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) and %CURRTIME% (a unique number based on the current time) here, but they are not as useful.

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.

Log To Printer: You can also send logged events to a printer so they can be seen as they happen. For example, if you have "public" computers on a network, which you need to track as they are used, you could have all the computers print their log records to one printer, perhaps at your front counter. One reason there is a computer name as well as user names is so you can tell the source of such "merged" log records. Note that log records can be wider than 80 characters, so you will need either a wide printer or a narrow print font (or both). See Full Control Log File Formats for more information.

For narrow printers, or when less detail is required, try the *summary logging* option. This provides just a few lines of information, including the amount of time and the number of pages printed. You can even have Full Control add a formfeed to eject the page at user logoff.

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.

Number of pages printed: Each page printed by this user, or each page printed to one or more specific printers, can be logged. Select printers to track by using the buttons provided. For a one-line report showing how many pages were printed by this user, click the *Log all printers* button. To provide a separate one-line report for each logged printer, click the *Select printers* button and choose the printers of interest.

File and folder access denied: You only need to check this box if you use Full Control's File Control feature. When using File Control, 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.

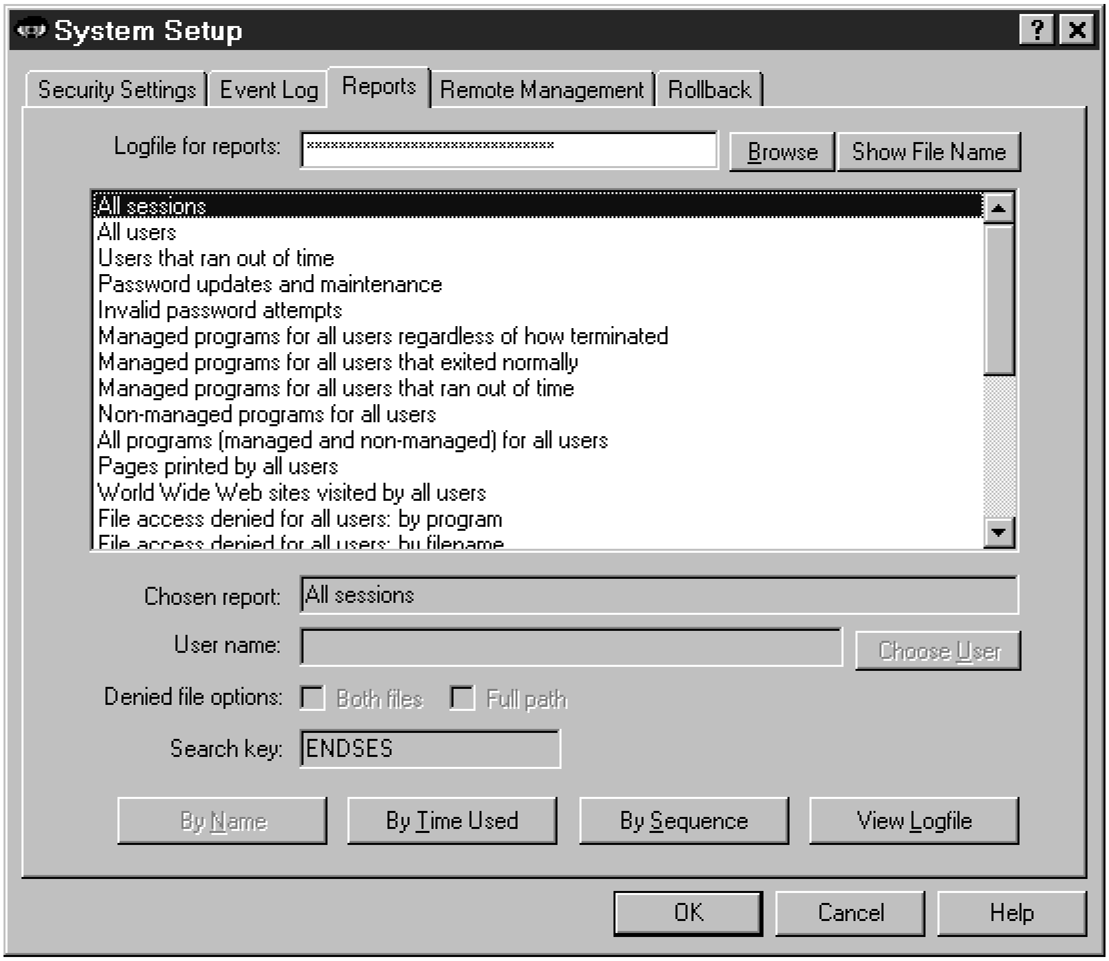
Password status: Check this box to have Full Control log each time a password was changed, and each time anyone attempted to use an invalid password.

Tests and diagnostics: These tests can help pinpoint problems in your Full Control configuration. However, they generate logfile entries and audio feedback which is otherwise undocumented, so this option is primarily intended to be used when working with 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 threads created, modules (files) loaded, and amount of memory used. 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 of files 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.

Reports Tab



Logfile for reports: ********************************

All sessions
All users
Users that ran out of time
Password updates and maintenance
Invalid password attempts
Managed programs for all users regardless of how terminated
Managed programs for all users that exited normally
Managed programs for all users that ran out of time
Non-managed programs for all users
All programs (managed and non-managed) for all users
Pages printed by all users
World Wide Web sites visited by all users
File access denied for all users: by program
File access denied for all users: by filename

Chosen report: All sessions

User name:

Denied file options: □ Both files □ Full path

Search key: ENDSES

This tab lets you view and print reports based on entries in the logfile, or view the actual logfile data. 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.

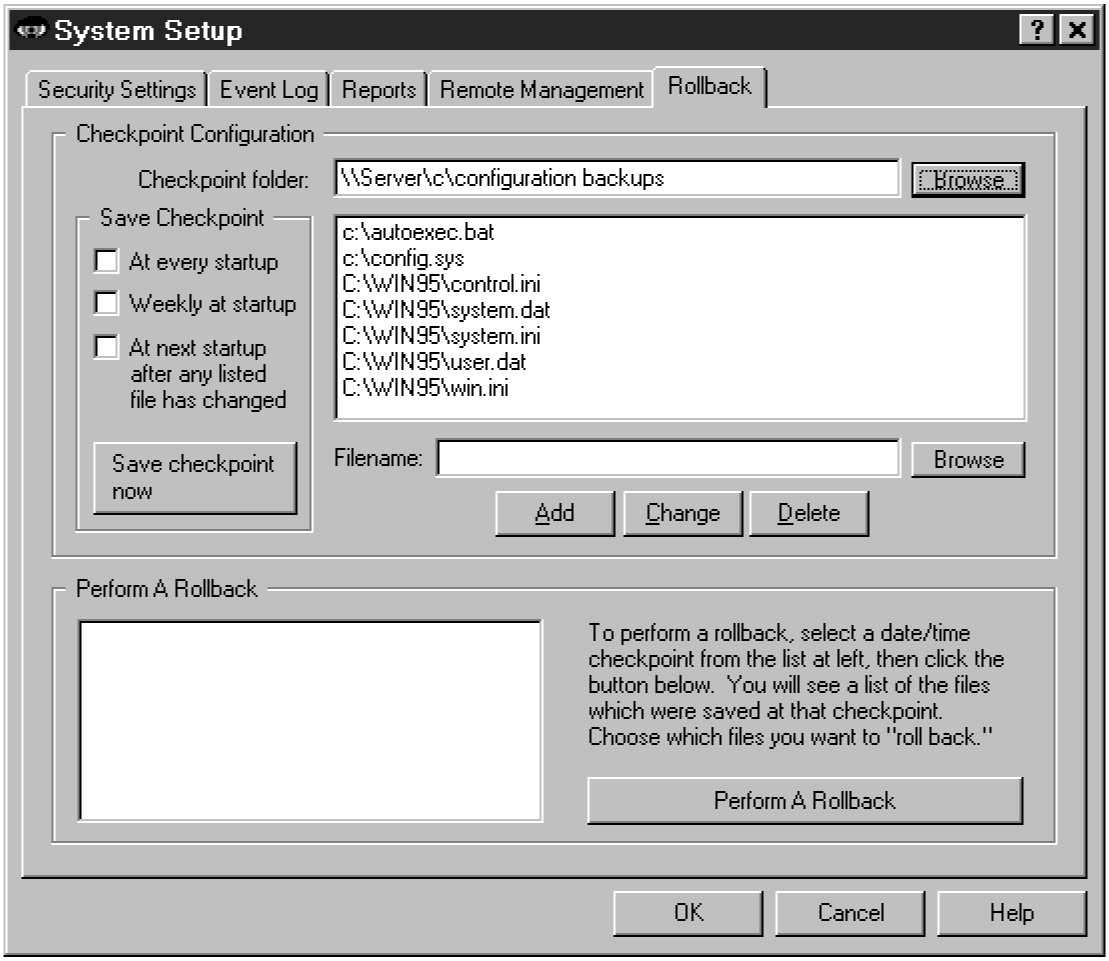
Reports are generated from the logfile listed at the top of the screen. Initially this is the same logfile listed on the Event Log tab. If you need to see reports based on a different logfile, type its name, or use the Browse button to find it, or drag-and-drop it onto the Reports tab. The filename which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

To generate a report, Full Control searches the logfile for a search key. Records containing the correct search 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.

For detailed descriptions of all search keys, reports, and views, see Usage Tracking Reports.

Rollback Tab



Checkpoint Configuration

Checkpoint folder: \\Server\c\configuration backups

c:\autoexec.bat
c:\config.sys
C:\WIN95\control.ini
C:\WIN95\system.dat
C:\WIN95\system.ini
C:\WIN95\user.dat
C:\WIN95\win.ini

Save Checkpoint

□ At every startup
□ Weekly at startup
□ At next startup after any listed file has changed

Save checkpoint now

Filename:

Perform A Rollback

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

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.

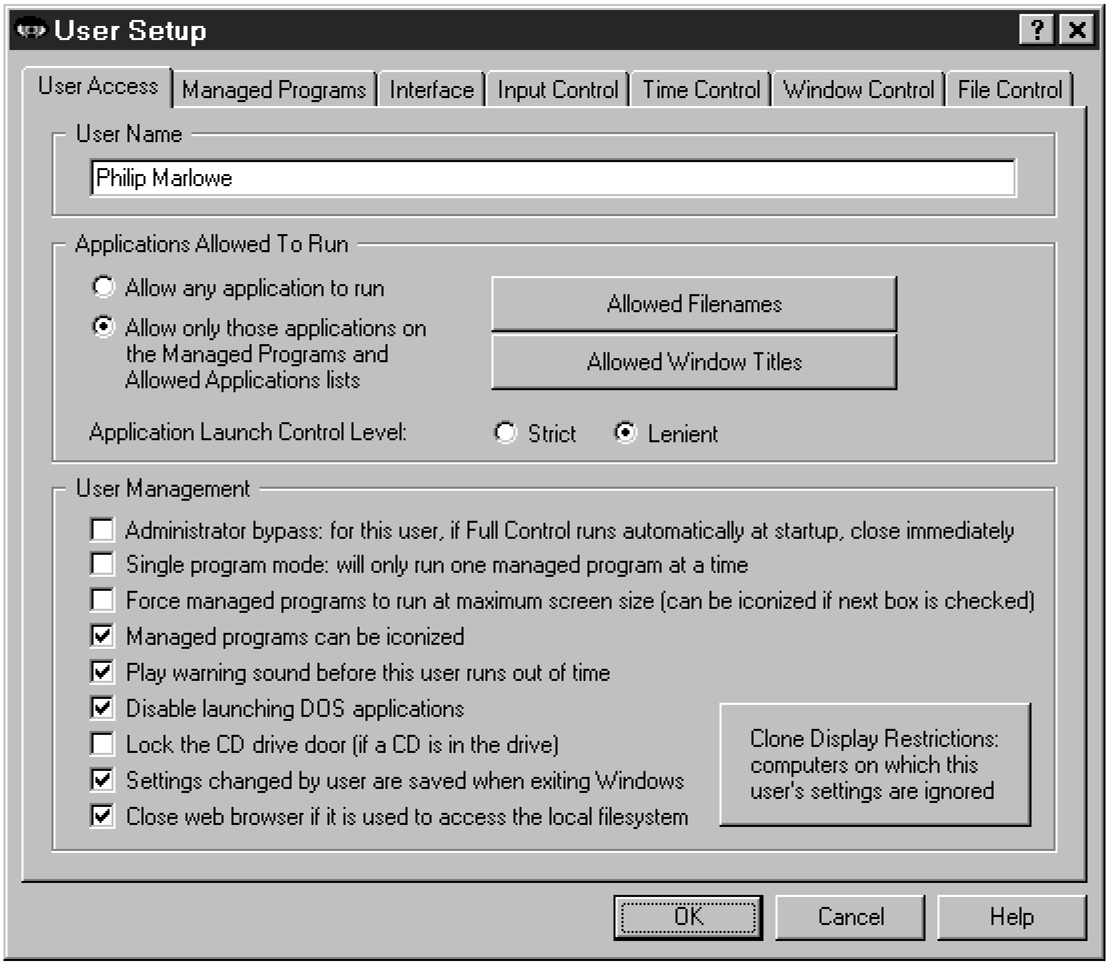
A checkpoint can be saved automatically at every Full Control startup, or once a week at startup, or at the first startup after any listed file has been modified, or when you click the Rollback tab's "save checkpoint now" button. Also, the Administration Manager can tell a remote networked workstation 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.

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.

User Setup Dialog



User Name

Philip Marlowe

Applications Allowed To Run

○ Allow any application to run

● Allow only those applications on the Managed Programs and Allowed Applications lists

Application Launch Control Level: ○ Strict ● Lenient

User Management

□ Administrator bypass: for this user, if Full Control runs automatically at startup, close immediately

□ Single program mode: will only run one managed program at a time

□ Force managed programs to run at maximum screen size (can be iconized if next box is checked)

☑ Managed programs can be iconized

☑ Play warning sound before this user runs out of time

☑ Disable launching DOS applications

□ Lock the CD drive door (if a CD is in the drive)

☑ Settings changed by user are saved when exiting Windows

☑ Close web browser if it is used to access the local filesystem

Full Control looks at the name of the user currently logged in to Windows 95. This user name can be validated at logon if desired, to ensure authorized access. If security settings have been set up in Full Control under that user's logon name, those settings will be put into place during the session. If settings for a valid user have not been provided, Full Control uses its Default User 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.

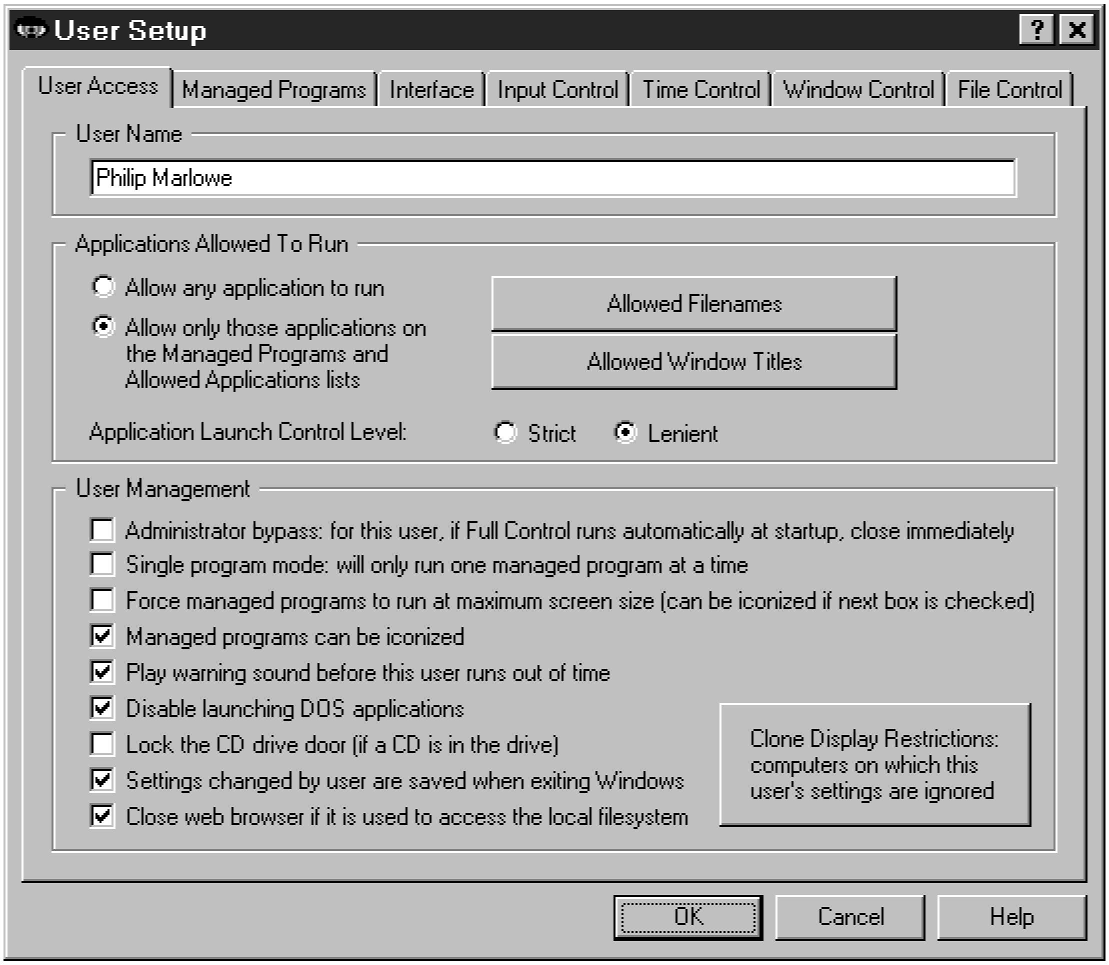
To set up options for each individual user, launch the User Setup tabbed dialog from the Administration screen.

The User Setup dialog has seven tabs:

User Access: program management, time limits, and interface options
Managed Programs: applications with time limits and other controls

Interface: hide desktop icons, drive/network access, and other restrictions
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

User Access Tab



User Name

Philip Marlowe

Applications Allowed To Run

○ Allow any application to run

● Allow only those applications on the Managed Programs and Allowed Applications lists

Application Launch Control Level: ○ Strict ● Lenient

User Management

□ Administrator bypass: for this user, if Full Control runs automatically at startup, close immediately

□ Single program mode: will only run one managed program at a time

□ Force managed programs to run at maximum screen size (can be iconized if next box is checked)

☑ Managed programs can be iconized

☑ Play warning sound before this user runs out of time

☑ Disable launching DOS applications

□ Lock the CD drive door (if a CD is in the drive)

☑ Settings changed by user are saved when exiting Windows

☑ Close web browser if it is used to access the local filesystem

This tab lets you set the user name, user management options, and ways that programs will and won't run when launched by this user.

User Name: This is the name under which the user logs on through the standard Windows logon screen. It is used to validate user logon access, and in the logfile. Though Full Control allows it to be identical to another user's name, this is usually not a good idea. You can rename the user at any time.

Applications Allowed To Run: Full Control can restrict the programs which can be run by this user. 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*. 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 when this user logs off. 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. 1) First, try to run Full Control; you can exit immediately if you like. When Full Control exits normally it will clear any leftover control settings. 2) If you cannot run Full Control in regular Windows 95, 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 95 and you'll be back to normal. 3) 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. 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.

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.

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 certain users to have complete access to the computer, with no interference from Full Control. To do this, set up that user's logon name in Full Control, and 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 (perhaps to modify settings) it will launch and run normally.

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 <u>can</u> be minimized, if the "can iconize" box is checked.*

<u>Warning sound:</u> 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.

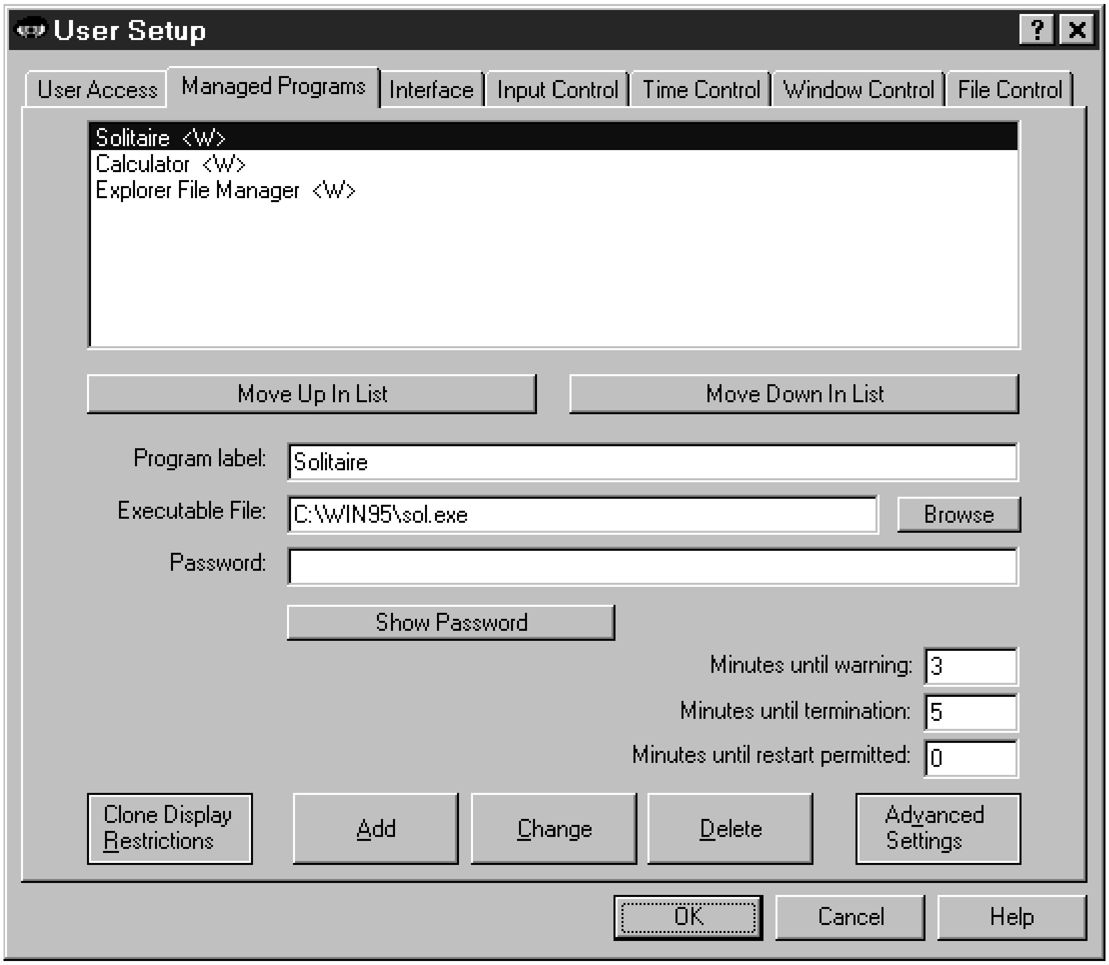
<u>Disable launching DOS applications:</u> Check this box if you do not want to allow this user to run any DOS programs.

<u>Lock CD drive door:</u> Check this box to help prevent valuable CDs from walking away from the computer. If this user logs on with no CD in the drive, the door will remain unlocked. That is, you can lock a CD into the drawer, but if there is no CD in the drawer it doesn't lock.

<u>Settings changed by user are saved when exiting Windows:</u> Check this box if you want certain configuration and interface changes made by this user to be saved on exit. Actually, on most computers this switch has little effect.

<u>Close web browser if it is used to access the local filesystem:</u> 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 3 or 4 and Internet Explorer 3 or 4.

Managed Programs Tab



Solitaire <W>
Calculator <W>
Explorer File Manager <W>

Program label: Solitaire
Executable File: C:\WIN95\sol.exe
Password:
Minutes until warning: 3
Minutes until termination: 5
Minutes until restart permitted: 0

Full Control managed programs are applications set up on this user'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.

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 User Access tab has been set up to permit this.

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

Applications List: The list at the top of the dialog shows all managed programs for this user. 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 dialogs themselves, but they are handy to quickly see which flags are set. The one-letter codes are as follows:

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
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, user info screen, 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 the 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.

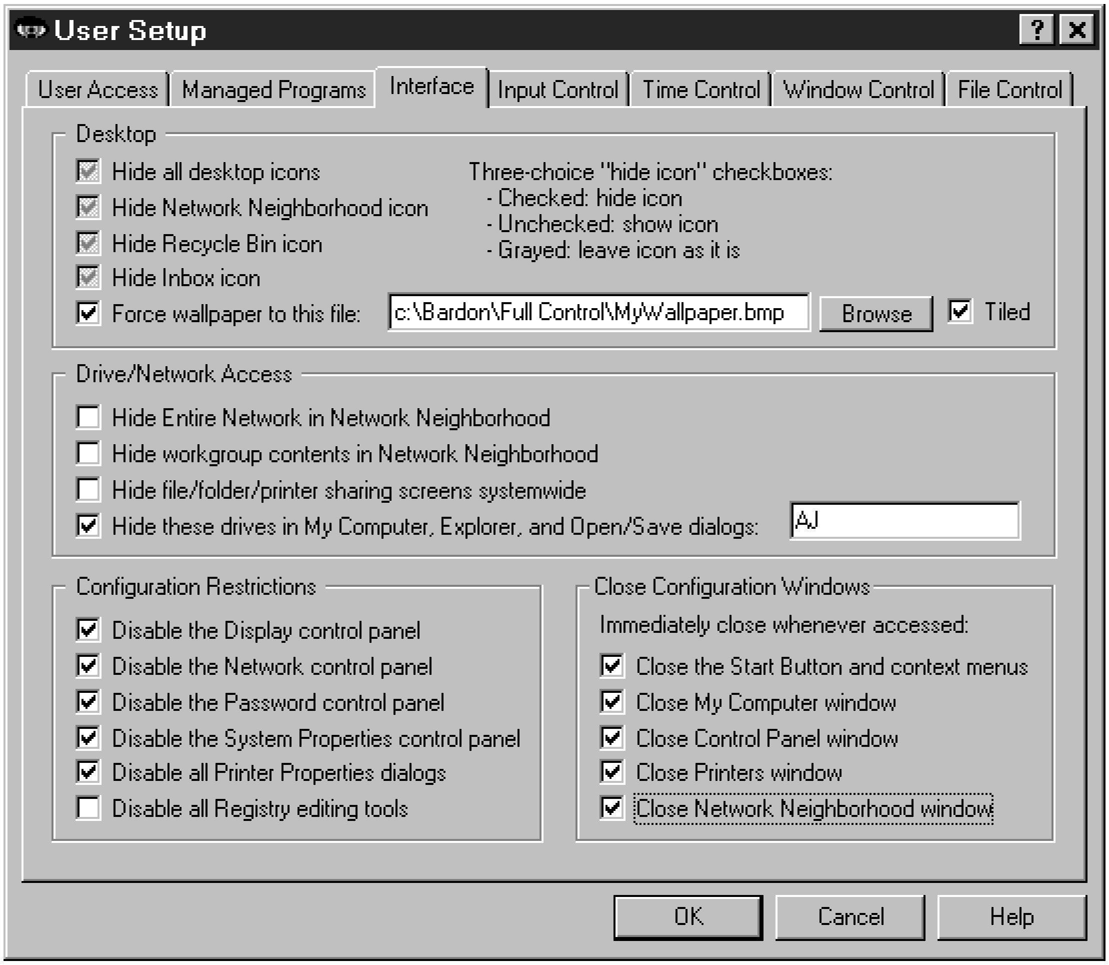
Minutes Until Restart Permitted: It's sometimes useful to be able to set a "waiting period" before an application can be restarted after termination. For example, if a parent sets up Junior's game with 30 Minutes Until Termination, what's to prevent Junior from simply restarting the game right away? 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 user configurations.

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



Desktop

☑ Hide all desktop icons
☑ Hide Network Neighborhood icon
☑ Hide Recycle Bin icon
☑ Hide Inbox icon
☑ Force wallpaper to this file: c:\Bardon\Full Control\MyWallpaper.bmp ☑ Tiled

Three-choice "hide icon" checkboxes:
- Checked: hide icon
- Unchecked: show icon
- Grayed: leave icon as it is

Drive/Network Access

☐ Hide Entire Network in Network Neighborhood
☐ Hide workgroup contents in Network Neighborhood
☐ Hide file/folder/printer sharing screens systemwide
☑ Hide these drives in My Computer, Explorer, and Open/Save dialogs: AJ

Configuration Restrictions

☑ Disable the Display control panel
☑ Disable the Network control panel
☑ Disable the Password control panel
☑ Disable the System Properties control panel
☑ Disable all Printer Properties dialogs
☐ Disable all Registry editing tools

Close Configuration Windows

Immediately close whenever accessed:

☑ Close the Start Button and context menus
☑ Close My Computer window
☑ Close Control Panel window
☑ Close Printers window
☑ Close Network Neighborhood window

This screen lets you specify how Windows will look and act whenever this user is logged on. (Related settings can be specified on the Input Control tab.) All options except *Close Configuration Windows* change settings within Windows itself. If you haven't checked *Enhanced Startup Protection* on the Security Settings tab of the System Setup screen, the first four Desktop settings may require that Windows restart when they are changed. On most computers, changing any of the other settings will not require a restart. However, if you change a setting here and the Windows interface does not change, restarting the computer will get everything back in sync. The companion Logoff Applet is a good way to do this.

Desktop: The first four options control the Windows 95 desktop icons which are available to this user. These four boxes are "three choice" checkboxes. If a "three choice" box is checked, its icon is hidden when this user is logged on. If the box is not checked, its icon is visible. If the box is grayed out, Full Control will neither force the icon to show, or force it to be hidden -- it will leave the icon in its current state. Because these four options change settings within Windows itself, they remain in effect whether Full Control is running or not. To restore them, come back to this tab and modify these settings.

On the Security Settings tab of the System Setup screen is a box labeled *Enhanced startup protection and Safe Mode password control.* At logon, if that box is checked, Full Control will put these four Desktop settings into place seamlessly. However, if that box is not checked, updating Windows with the user's Desktop settings may require a re-logon by that user. This is because these four options change settings within Windows itself, and if they are not set into place early in the logon process they won't appear until the next logon. Checking the *Enhanced startup protection* box sets these options in place early, thus avoiding the re-logon.

For similar reasons, changing any of the three-choice checkboxes while in setup mode will cause Full Control to restart the computer when you resume security control so as to put the changed settings into place.

Wallpaper: Check the last 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. Changing this setting will not restart the computer.

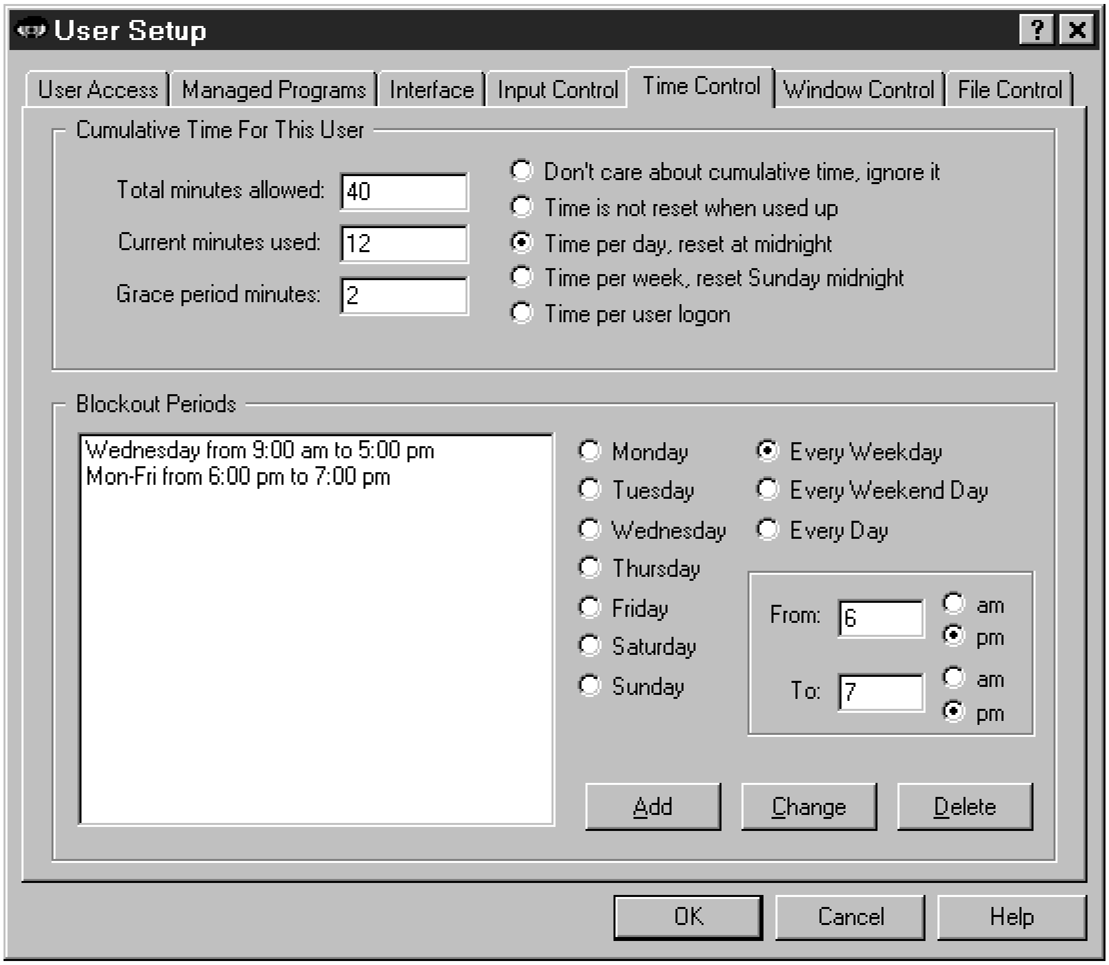
Drive/Network Access: These options control access to files, folders, and printers. Check the first box to hide the Entire Network icon in Explorer and Network Neighborhood; check the second box to hide workgroup members in Explorer and Network Neighborhood. If you don't want to allow users to modify 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. This is a 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. 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.

Configuration Restrictions: These options control the user's ability to reconfigure printers, the Registry, and certain parts of Control Panel.

Close Configuration Windows: Perhaps you want to leave My Computer, Network Neighborhood, and similar icons in place on the Desktop, but prevent the use of them. Or perhaps you don’t want users opening the Start button and related Taskbar menus. If so, use these boxes to tell Full Control to close such windows when they appear. If you'd like the screen look like it "should" but still be secure, consider using these options instead of the related *Desktop* and *Configuration Restrictions* checkboxes described above.

Time Control Tab



Cumulative Time For This User

Total minutes allowed: 40

Current minutes used: 12

Grace period minutes: 2

- ○ Don't care about cumulative time, ignore it
- ○ Time is not reset when used up
- ● Time per day, reset at midnight
- ○ Time per week, reset Sunday midnight
- ○ Time per user logon

Blockout Periods

Wednesday from 9:00 am to 5:00 pm
Mon-Fri from 6:00 pm to 7:00 pm

- ○ Monday
- ○ Tuesday
- ○ Wednesday
- ○ Thursday
- ○ Friday
- ○ Saturday
- ○ Sunday
- ● Every Weekday
- ○ Every Weekend Day
- ○ Every Day

From: 6 ○ am ● pm

To: 7 ○ am ● pm

This tab controls times during which programs can be run by this user.

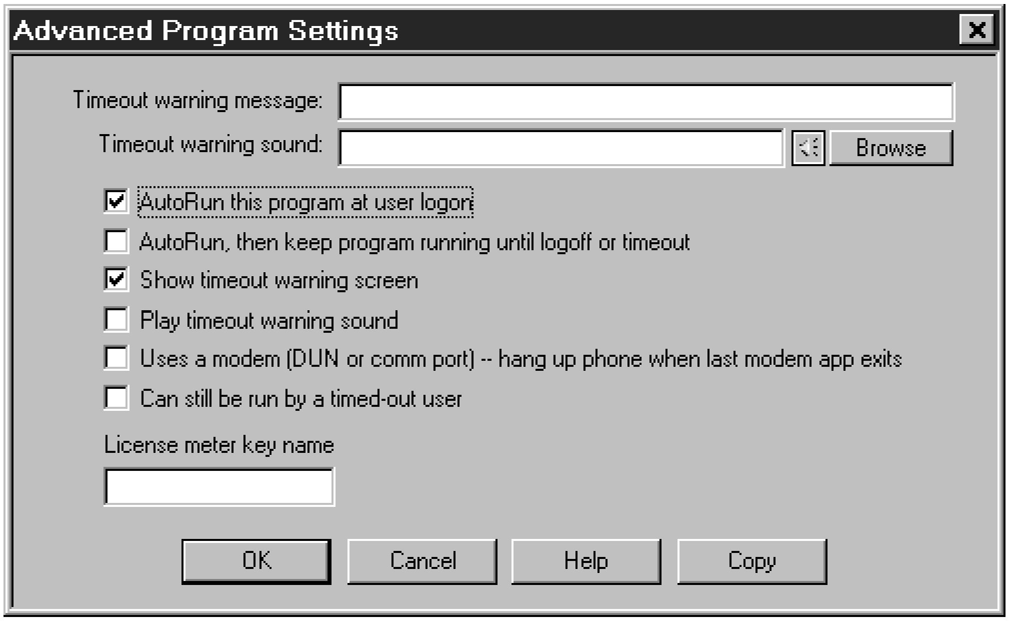
Cumulative Time: In addition to each program's individual time limit, the user can have a time limit. If desired, specify the maximum number of minutes allowed before forced termination. You can also change the number of minutes currently used. When the user time runs out, any active programs are terminated. 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 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.

Advanced Program Settings



☑ AutoRun this program at user logon
□ AutoRun, then keep program running until logoff or timeout
☑ Show timeout warning screen
□ Play timeout warning sound
□ Uses a modem (DUN or comm port) -- hang up phone when last modem app exits
□ Can still be run by a timed-out user

The Advanced Program Settings screen is reached by clicking the Advanced button on the Managed Programs tab of the User 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 username configuration.

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

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

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).

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 User 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. In that case, 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 look in the license meter monitor file to make sure there is a license "slot" available under the key name "Word 95". If a license is available, Full Control will update the license meter monitor file to add the new user, and allow the program to be run. When the user exits from the monitored program, Full Control releases the license "slot" making it available to other users.

Full Control looks for license metering information in the license meter monitor file. Give the name of this file on the Remote Management tab of the System Setup dialog. Then use the companion License Meter Manager program (metermgr.exe) to add this license meter key name, and the number of licenses it controls, to the license meter monitor file.

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

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 this user is logged on. However, the "hide drives" method is not as strong. Though the drives are not listed in Explorer, My Computer, and elsewhere, their files and folders are available by simply typing in the full path to them (for example in the Run screen or Open/Save dialogs). File Control is a much more reliable way to control sensitive areas.

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. On most computers you can also 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 User 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 User settings are used. Encourage users to log on under their own names by setting up the Default User to allow very little activity.

Full Control Order Form

After Printing
Click Here To Return

Send Orders To:
Bardon Data Systems
1164 Solano Ave. #415
Albany CA 94706 USA
(510) 526-8470 voice
(510) 526-1271 fax
orders@bardon.com

From:
Name:
Address:

Phone:
Fax:
Email:

Checks: We accept checks or money orders in US Dollars, drawn on a US bank and requiring no additional collection or currency-conversion fees. Make check or money order payable to **Bardon Data Systems.**

Credit Cards: We accept MasterCard, Visa, American Express, or Discover/Novus cards. Phone credit card orders to Bardon Data Systems or mail this order form:

1) Sign here to bill credit card for this purchase: ______________________________
2) Print Name As It Appears On Credit Card:
3) Credit Card Number:
4) Expiration Date: ___/___
5) Check if this is: MasterCard [ ] Visa [ ] AMEX [ ] Discover/Novus [ ]

Purchase Orders: Purchase orders are accepted from most organizations within North America. Terms are net 30 days unless arranged otherwise in advance. For orders under $100, please add an additional $10 processing fee if using a purchase order.

Multiple Copy Orders: Contact Bardon Data Systems for information on quantity discounts, educational pricing, and other special offers.

Maintenance Plan: Includes all Full Control upgrades for one year, plus other benefits. $24.95 per single copy, less in quantity.

Quantity			**Amount Enclosed**
	Full Control Security Access Control Software	$49.95	
	Maintenance Plan (per single copy)	$24.95	
	Shipping & Handling	$5.00	
	Purchase Order Surcharge Orders under $100 if using a purchase order	$10.00	
	California residents add 8.25% sales tax		
	Total Enclosed:		

Setup Mode

Setup Mode: In Setup Mode, security checks are temporarily suspended. The current user is by definition the system administrator, someone who already has access to the entire system. For such a user, further security testing serves no useful purpose. Therefore, in Setup Mode, passwords are not required or requested, and Full Control 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.

To exit from Setup Mode, choose *Resume Security 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 a number of built-in "emergency" passwords.   Each password can be used just once on a given Full Control computer.   After a password is used once, it is no longer valid.   For security reasons, the passwords are not listed here.   If you are in a situation where you need one, contact Bardon Data Systems and, after providing appropriate identification, one will be provided.

In addition, the "test-drive" version of Full Control has yet another built-in emergency password.   While evaluating, the setup password "FullCtl" always matches.   After purchase, this "back door" security hole is no longer active.

Logging To A Printer

Logging to printer is set up on the Event Log tab of the System Setup dialog. If this is enabled, Full Control will send logged events to a printer so they can be seen as they happen. For example, if you need to track usage on networked public-access computers, you can have all the computers print their log records to one printer, perhaps at your front counter. The computer name is included, making it easy to tell the source of such "merged" log records.

Normal log records can be wider than 80 characters, so you will need either a wide printer or a narrow print font (or both). For narrow printers, or when less detail is required, try the *Summary Logging* option. This provides just a few lines of information, including the amount of time and the number of pages printed by this user.

Reports

Full Control can generate a number of built-in usage tracking reports. These reports can be selected, viewed, and printed from the Reports tab of the System Setup dialog.

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

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

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

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

After a report and a view are selected, the output screen 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. Click the output screen's 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. If you need the printed report in computer-usable form, you can Print To File. (You can also use the logfile itself, which is designed to be easily parsed by database or spreadsheet programs.)

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 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. You will need to provide the search key in which you are interested. See the Log File Format section for more information on search keys. A Full Control companion program or other Full Control-aware application may add records to the Full Control logfile which use search keys not listed here. That program's documentation should have more information on these records.

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..

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.

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 ENDSES logfile records, which are written when the user exits a session voluntarily, or when Full Control terminates that user for timeout reasons.

Users that ran out of time: This report shows the ending time and amount of minutes where 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 user (voluntary) 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 user (voluntary) 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 by Full Control 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).

Pages printed by all users: This report tracks PAGECT records. At each user exit, one PAGECT record is generated for each printer being tracked. If the pagecount is being tracked, but not specifically by printer name, only a single PAGECT record is generated at user exit. It contains the number of pages printed by all printers.

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 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 it 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.

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 all files accessed by DOS programs is also listed as KERNEL32.

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

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).

Pages printed by the named user: This report tracks PAGECT records. At each user exit, one PAGECT record is generated for each printer being tracked. If the pagecount is being tracked, but not specifically by printer name, only a single PAGECT record is generated at user exit. It contains one count, the number of pages printed by all printers.

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.

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 Now* button on the Remote Management tab of the System Setup dialog. The clone file contains all the data that defines this computer's configuration, 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.

How to clone: To clone a computer, first set up one computer with your chosen users, managed programs, passwords, logfile, sounds, display restrictions, and whatever else you want to specify. Then click the *Export Clone File Now* button on the Remote Management tab of the master computer. 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 install the clone data onto the new machine. If you are installing from a floppy disk remember to leave some empty space on the disk for the installer to create some small temporary files during the installation process.

Updating manually: The second way is to 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.

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 Win95 logon) 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.

Another useful tool for cloning is Full Control's display restrictions feature. This lets you control the computers on which a user or managed program is monitored. When setting up your master computer, you can give information for each individual user and managed program. At runtime Full Control 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-user; 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.

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.

Tools especially geared towards system administration include:

Administrator Bypass
System Setup Dialog
User Setup Dialog
Emergency Passwords
How To Clone A Computer
Display Restrictions
Window Control
File System Access Control
License Meter Manager Program
Remote Administration Manager Program
Log To Printer
Reports

Log File Format

Full Control provides file-logging options that can be set in the System Setup screen. 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: ffffff, 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","a
pp","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
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
CMPLDF	S	Full Control component load failed: <name of component>
ENDAPT	M	Managed Program Terminated Due To Program/User Timeout
ENDAPU	M	Managed Program Terminated By User
ENDANM	M	Non-managed Program Terminated
ENDSES	S	End Of Full Control Session
FILACC	S	File access denied
MTRSBD	S	<metered-app startup bad, see its error message>
MTRSNS	N	Metered application startup denied: no more users are allowed
MTRSOK	N	Started metered application (now has N concurrent users)
MTRXBD	S	<metered-app exit bad, see its error message>
MTRXOK	N	Terminated metered application (now has N concurrent users)
PAGECT	P	N pages printed by <name of printer or All Printers>
STRAPP	Z	Managed Program Started
STRSES	Z	Start Of Full Control Session
TIMUSR	S	Users that ran out of time
WEBBRN	Z	A new Web browser window was opened
WEBBRX	W	Web Browser Exit: browser window closed (logs mins since its WEBBRN)
WEBPGC	W	Web Browser Page Change: title of page and mins on that page

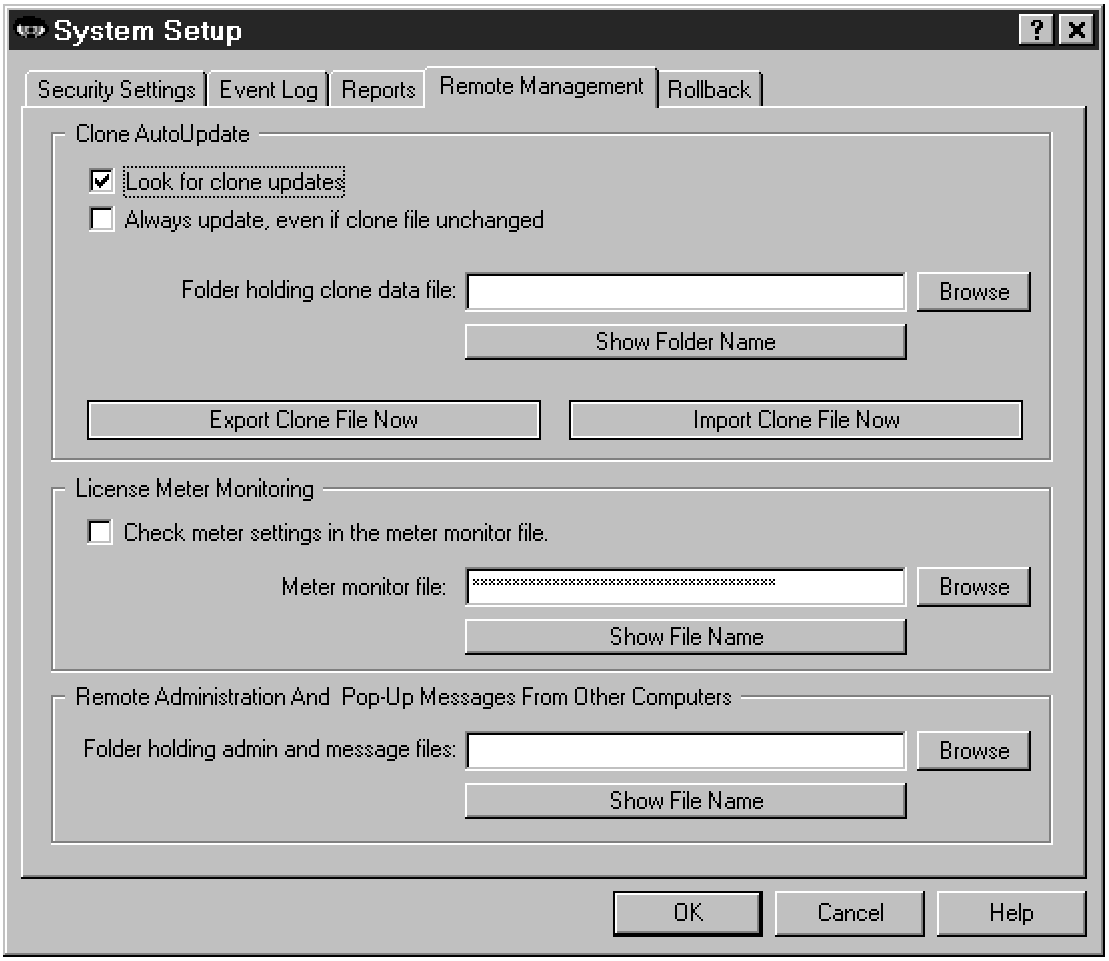
The "num" field generally, though not always, shows the number of minutes at the time this log record was generated.   The meaning of the "num" field is:

S: minutes in session
M: minutes in managed program
N: current number of users running metered application
P: number of pages printed by user
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.

Remote Management Tab



Clone AutoUpdate

☑ Look for clone updates

□ Always update, even if clone file unchanged

Folder holding clone data file:

License Meter Monitoring

□ Check meter settings in the meter monitor file.

Meter monitor file: **

Remote Administration And Pop-Up Messages From Other Computers

Folder holding admin and message files:

This tab lets you set up features which provide network-based remote configuration and application control. You can also set up a computer-to-computer communications channel, allowing Full Control users to send popup text messages to each other over the network.

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 if someone has defeated 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!

Export Clone File Now: Clicking this button sets up to create a clone data file. 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-user settings, or other features you have set up to control which managed programs or users are controlled on what computers. Cloning is further described in How To Clone A Computer.

Import Clone File Now: Clicking this button sets up to read a clone data file and immediately update the current computer's configuration. It's sometimes useful to be able to instantly update the current computer.

License Meter Monitoring: Full Control's built-in license meter management lets you control how many users can simultaneously run any program. 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. Full Control is designed to ensure that the number of simultaneous users never exceeds the number of licensed copies of the software.

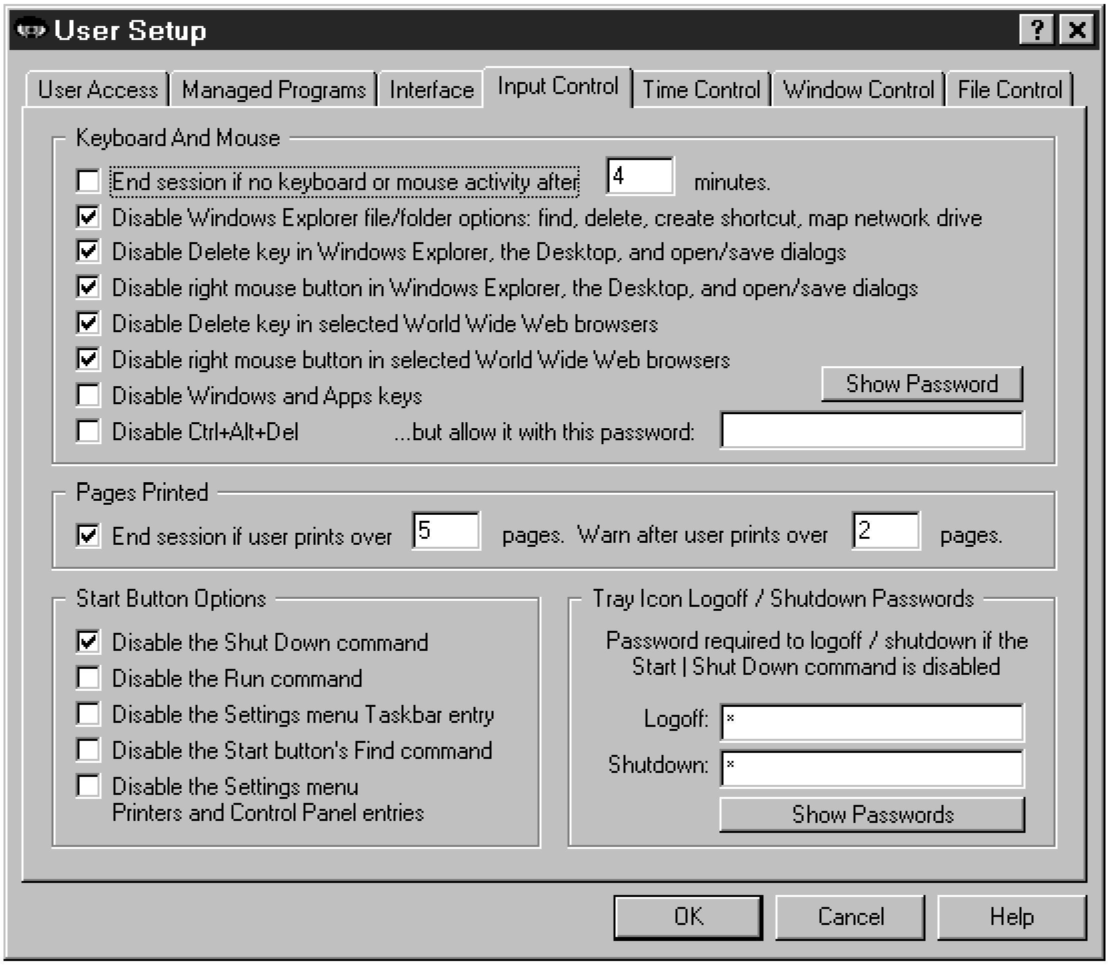
To set this up, you first install the program normally, making sure it can be run from each desired workstation. Set up the application as a managed program, and use the program's Advanced Settings screen to assign it a license key as set up in the License Meter Manager program. Then use this Remote Management tab to give the name of the meter monitor file in which Full Control can find that license key.

Remote Administration And Pop-Up Messages: Designate a directory here so you can use the Remote Administration Manager and the Message Manager to send virtually immediate messages from a remote network location to this computer. Remote Administration Manager messages can modify cumulative time limits and settings, log off the current user, hang up Dial-Up Networking, save a checkpoint, shut down or restart the computer, and cause popup text notes to appear on the target computer(s). Message Manager messages let users send short popup text notes to other Full Control computers on the network.

Full Control will look in the designated directory about once a minute for time and message files. This directory must be able to handle long filenames because both Remote Administration and message filenames exceed the now-defunct DOS 8.3 filename format.

To use the Remote Administration Manager or Message Manager, the user's computer must have read-write access to this directory, so Full Control can delete the message file after it is read.

Input Control Tab



Keyboard And Mouse

☐ End session if no keyboard or mouse activity after 4 minutes.

☑ Disable Windows Explorer file/folder options: find, delete, create shortcut, map network drive

☑ Disable Delete key in Windows Explorer, the Desktop, and open/save dialogs

☑ Disable right mouse button in Windows Explorer, the Desktop, and open/save dialogs

☑ Disable Delete key in selected World Wide Web browsers

☑ Disable right mouse button in selected World Wide Web browsers

☐ Disable Windows and Apps keys

☐ Disable Ctrl+Alt+Del ...but allow it with this password:

Pages Printed

☑ End session if user prints over 5 pages. Warn after user prints over 2 pages.

Start Button Options

☑ Disable the Shut Down command

☐ Disable the Run command

☐ Disable the Settings menu Taskbar entry

☐ Disable the Start button's Find command

☐ Disable the Settings menu Printers and Control Panel entries

Tray Icon Logoff / Shutdown Passwords

Password required to logoff / shutdown if the Start | Shut Down command is disabled

Logoff: *

Shutdown: *

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, and the mouse's right-button context menus. Full Control can also prevent the use of Explorer features such as Find File, Find Folder, Find Computer, Map Network Drive, and Go To. In addition, Full Control can disable the right mouse button and Delete key in the 32-bit Netscape (3 or 4) or Microsoft (3 or 4) web browsers. 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.

Disable Windows Explorer file/folder manipulation options: If checked, Full Control will look for certain Explorer-related window titles and cancel them when found, so as to disable their function. These window titles are: "Confirm File Delete", "Confirm Folder Delete", "Confirm Multiple File Delete", "Find", "Go To Folder", "Map Network Drive", and "Create Shortcut". Disabling these windows makes Explorer's menus safer.

Disable Delete key in Windows Explorer, the Desktop, and open/save dialogs: This prevents using the Delete key to delete files or folders on the Desktop, in Explorer, in the standard Windows Open/Save dialogs, and Microsoft Office applications.

Disable right mouse button in Windows Explorer, the Desktop, and open/save dialogs: This prevents using the right-mouse context menus on the Desktop, in Explorer, in the standard Windows Open/Save dialogs, and Microsoft Office applications. If uncontrolled, these menus can allow the user to run applications, delete and rename files, etc.

Disable Delete key in selected World Wide Web browsers: It's occasionally useful to disable this, for the same reason as with Explorer and Open/Save dialogs. Full Control can monitor the 32-bit Netscape (3 or 4) or Microsoft (3 or 4) web browsers.

Disable right mouse button in selected 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 the 32-bit Netscape (3 or 4) or Microsoft (3 or 4) web browsers.

Disable Windows and Apps keys: These keys, found on newer 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.

Pages Printed: Use this to set the maximum number of pages the user is allowed to print during the current session, and when to display the "close to limit" warning. If the limit is exceeded, the session will be ended using the forced-termination method you specified on the Security Settings tab. If this user has been given time control limits, time will be set to "all used up." This condition can be corrected by the administrator with the use of Full Control's Remote Administration Manager program.

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 the *Close Configuration Windows* and other options on the Interface tab, the *Keyboard And Mouse* options described above, Window Control options, and File Control options.

The *Start Button Options* change settings within Windows itself. Start button restrictions are set into place immediately, but on some computers restrictions won't be cleared until the next logon. If you need it, the companion Logoff Applet is a good way to logoff and reset your system.

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

Disable the 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.

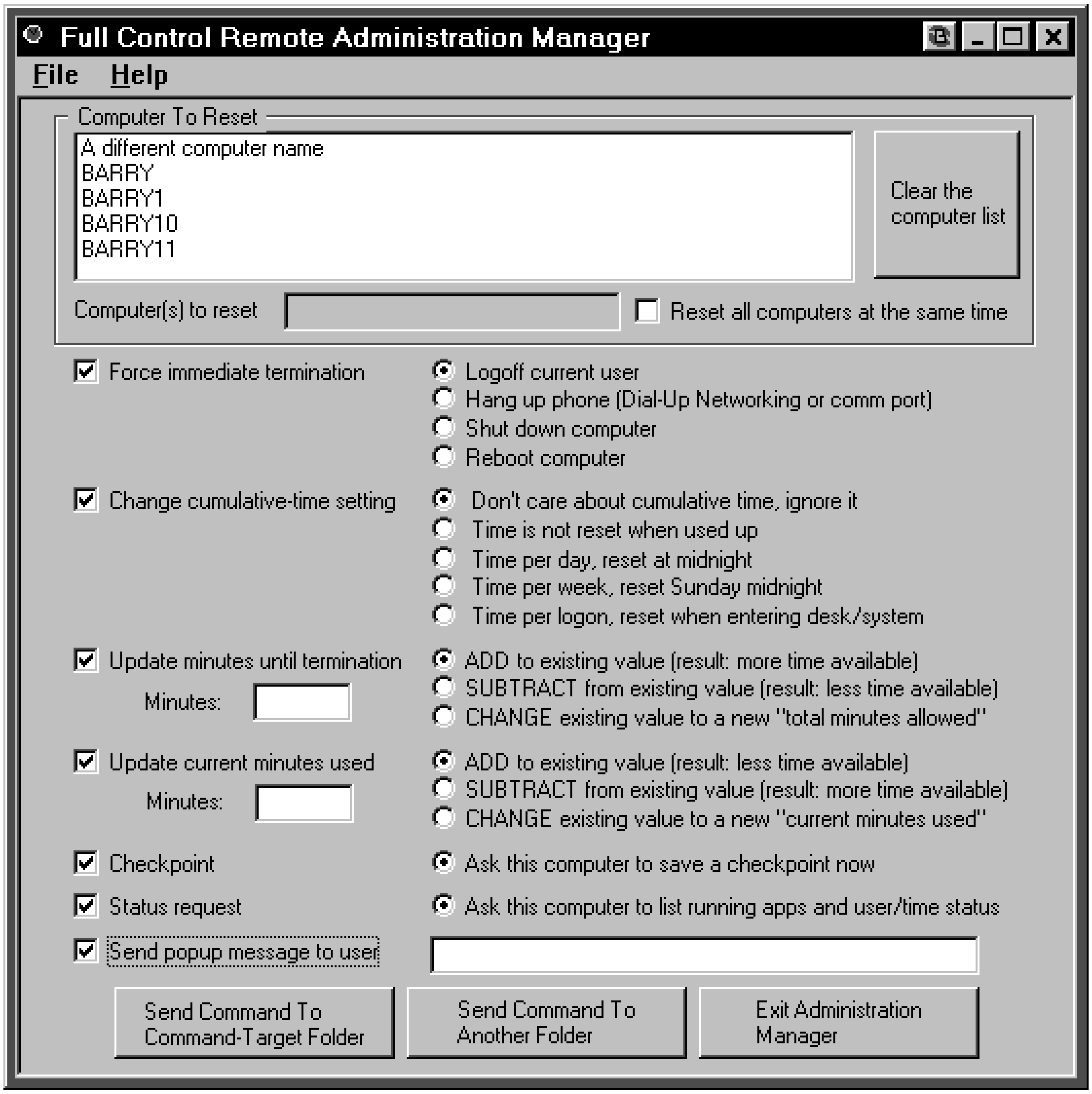
Disable the Start button's Find command: When checked, the user cannot use the Start button's *Find* command. However, the *Find* command can still be used through Explorer. To disable that route, check the *Disable Explorer file/folder options* box at the top of this tab.

Disable the Settings menu Printers and Control Panel entries: When checked, the user cannot use the Start button's *Settings* | *Control Panel* or *Settings* | *Printers* commands to access Printer or Control Panel options. However, they are still accessible through My Computer and Explorer.

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

When *Shut Down* is 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 the *Shut Down* command is not disabled, as a convenience the icon menu's logoff and shutdown functions do not require a password.

Remote Administration Manager



Full Control Remote Administration Manager

File Help

Computer To Reset

A different computer name
BARRY
BARRY1
BARRY10
BARRY11

Clear the computer list

Computer(s) to reset □ Reset all computers at the same time

☑ Force immediate termination
● Logoff current user
○ Hang up phone (Dial-Up Networking or comm port)
○ Shut down computer
○ Reboot computer

☑ Change cumulative-time setting
● Don't care about cumulative time, ignore it
○ Time is not reset when used up
○ Time per day, reset at midnight
○ Time per week, reset Sunday midnight
○ Time per logon, reset when entering desk/system

☑ Update minutes until termination
Minutes:
● ADD to existing value (result: more time available)
○ SUBTRACT from existing value (result: less time available)
○ CHANGE existing value to a new "total minutes allowed"

☑ Update current minutes used
Minutes:
● ADD to existing value (result: less time available)
○ SUBTRACT from existing value (result: more time available)
○ CHANGE existing value to a new "current minutes used"

☑ Checkpoint
● Ask this computer to save a checkpoint now

☑ Status request
● Ask this computer to list running apps and user/time status

☑ Send popup message to user

Send Command To Command-Target Folder | Send Command To Another Folder | Exit Administration Manager

The Remote Administration Manager lets the administrator, at another station on the network, create and send "messages" to Full Control stations elsewhere on the network. These messages can remotely logoff any user, reset the current time limits, shut down the remote computer, request the remote computer's status, initiate a checkpoint, or send a brief popup message to one or more Full Control computers on the network.

Setting Up The Local Computer: You set up the local computer to receive messages from the Remote Administration Manager by providing a target directory name on the Remote Management tab of the System Setup dialog. Typically this directory will be on a server, where it can be seen by both the Full Control computer and the administrator's station. The Full Control computer checks this directory for new messages about once a minute. If it finds a message addressed to this computer, the Full Control computer will read it and reset itself accordingly.

Using The Remote Administration Manager Program: The administrator can run the Remote Administration Manager from anywhere on the network that can access the target directory monitored by the Full Control computer. The network must be enabled for long file names. To set up the Remote Administration Manager, use the Data Extractor to create a set of data files, one for each Full Control computer. Copy these files into the Remote Administration Manager's own directory, or to either of the folders listed on this computer's Remote Management tab. All these locations will be checked for data files when the Administration Manager starts.

To build a command, first choose one or more computers to reset 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" box to reset every listed computer with this one command. Next, set up the command by checking one or more of the boxes on the left side and selecting from their options on the right side. Here are the checkbox choices and the options for each choice:

Force immediate termination: *Logoff* will immediately set the target computer to the default 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 Full Control computers at the end of the day to make sure all your phone lines are disconnected before closing up shop.

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

Note that if pages-printed limits are in effect for a user and excessive pages are printed, the user's current minutes value is set to the maximum ("all used up") to force immediate exit.   Therefore, decreasing the current minutes used will re-allow access for that user.

Checkpoint: Select this to ask the computer(s) to perform a checkpoint.   This assumes that the target computer(s) have been set up to do so, with a checkpoint folder specified and files in the checkpoint files list.

Status Request: Select this to ask the target computer(s) to tell you their status (what's running, user info, pages-printed status, etc).   The requested information appears in 15-40 seconds as a popup from the Remote Administration Manager.   To save this information, select the desired text with your mouse and press Ctrl+C to copy it to the clipboard.

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

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

One way to use the Administration Manager might be to set the public computer to "no time left" when Full Control 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*).   The user information window shows the time remaining, and Full Control will warn the customer in advance of expiration.   You then use the Administration Manager to send the machine more time.

An administration message file 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.   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.

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.

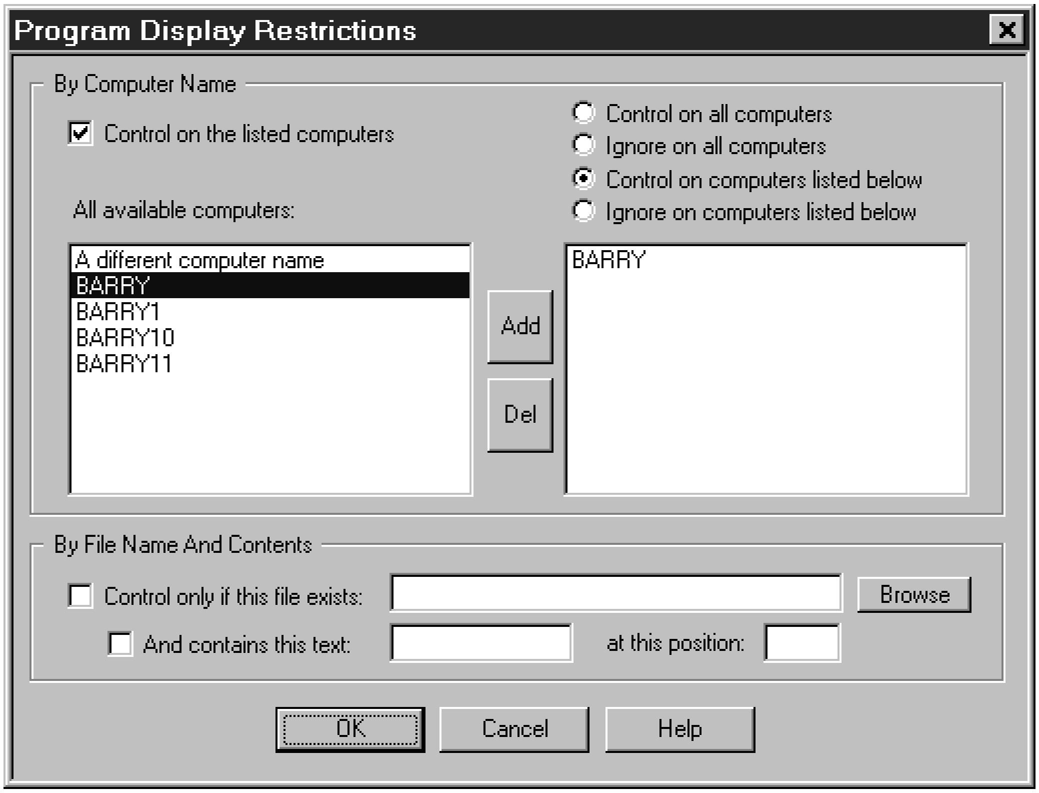
Let's say a customer arrives and sits at a computer. There is zero time available. From the administration station, you remotely send some time to that computer, perhaps 30 minutes. The customer uses the computer for the allotted 30 minutes as the counter ticks down.

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 and user information window 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.

Display Restrictions



Program Display Restrictions

By Computer Name

☑ Control on the listed computers

○ Control on all computers
○ Ignore on all computers
● Control on computers listed below
○ Ignore on computers listed below

All available computers:

A different computer name
BARRY
BARRY1
BARRY10
BARRY11

BARRY

By File Name And Contents

□ Control only if this file exists:

□ And contains this text: at this position:

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 User Setup tabbed dialog.   If you reach this screen from the Managed Programs tab, you can specify the computers on which that application will be treated as a managed program.   If you get here from the User Access tab, you can specify the computers on which a user's settings are considered at logon.   For example, if a user's Restrictions settings are such that the user is to be ignored on this computer, Full Control's logon validation can be set up to not accept that user.   If the user is allowed to log on under that name the Default User 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.

Full Control can look at the target computer's name to decide whether to monitor this managed program or user.   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 user. Then choose one of the radio buttons to decide which name-based test Full Control will perform. Should the program or user 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.

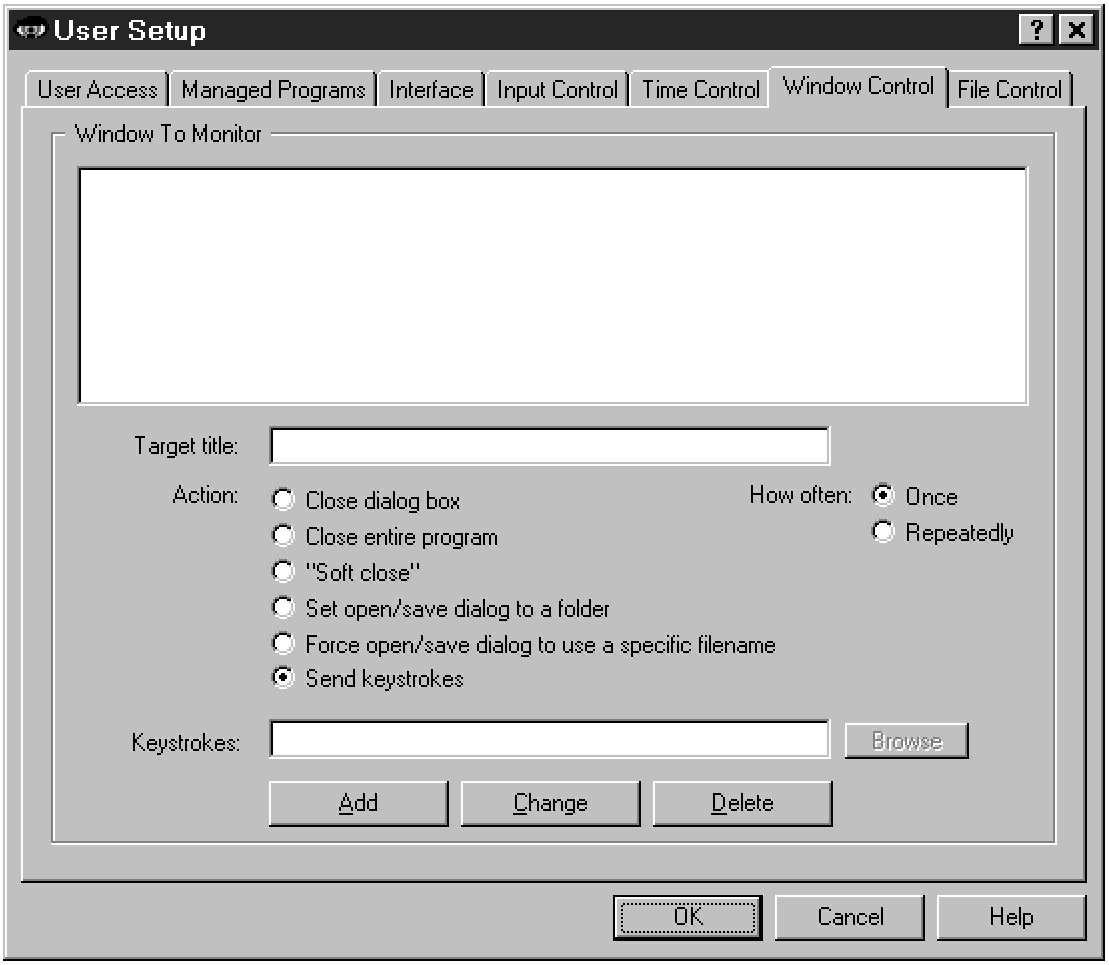
The names in the left-box list come from the "*.fcd" data files which are available to Full Control when you open this screen. These data files are generated by the Full Control Data Extractor program. Use the Data Extractor to create a set of data files, one for each Full Control computer. Copy these files into the Full Control directory, or to either of the folders listed on this computer's Remote Management tab. All these locations will be checked for data files.

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 user. If the file exists, the program or user will be monitored. You can also test the file's contents (see below).

And contains this text: Check this box if you want Full Control 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).

Window Control



Target title:

Action:
○ Close dialog box
○ Close entire program
○ "Soft close"
○ Set open/save dialog to a folder
○ Force open/save dialog to use a specific filename
● Send keystrokes

How often:
● Once
○ Repeatedly

Keystrokes:

Full Control's Window Control feature lets you control virtually any window or dialog when it appears.   Full Control looks at the title bar text of the current active window or dialog, and if the text matches any target title on the Window Control list, the appropriate action is taken.   The * and ? wildcards can be used freely in the target title specification.

What can you do to a matching 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. Among other things, this last option provides a good way to prevent web browser users from accessing the local hard disk.   See Using Internet Software for more information on this.

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 ways. First, the "allowed applications" feature only considers the main window of a program, but the Window Control options will work on any window, including dialogs and other "little" windows that are associated with a main program, which lets you allow a program yet disallow certain specific dialogs. Second, the Window Control feature offers three different ways to close different kinds of windows (see below).

The latter three options allow entry into the bottom edit line. 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 Win95 logon) 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.

For many of these features, you can perform the action just one time, or perform it repeatedly (about every three seconds) to make absolutely sure it is done the way you want. Let's look at each option in turn.

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

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

"Soft close": You won't need this often, but when you do it's very handy. Like the "close entire program" option, this is intended to close an entire application, not a dialog box. Use this to close those rare applications that *must* be given the opportunity to close in their own manner. Some programs leave themselves or the computer in a sub-optimal state when forced to terminate in the usual Full Control 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 to encourage users to open files from, or save files to, one particular folder. Give the proper directory in the bottom edit line (which will relabel itself to "Directory:" when using this option). You can drag-and-drop a folder from Explorer onto that line too, if you prefer. Of course the target title will generally be "Open" or "Save As." This works best with the standard Windows file-open and file-save dialogs, but can often be used with other non-standard dialogs as well. This does not force the dialog to stay in the directory to which it has been set. Think of it as a "strong suggestion" to use that directory. To use a mandatory name and location, use the next option. Note that other Full Control options allow you to hide drives, or make files or folders read-only or invisible, but these other options *keep the user away from* a location. Setting open/save screens to a folder actively *moves the user to* a location.

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 Win95 logon) 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 95 to do certain automated processing based on the file's extension.

Send keystrokes: This could be the single most powerful option in Full Control. With it you can send any keystrokes to any window the moment that window's target title appears. For example, let's say you want to prevent Netscape from accessing the local hard disk. Monitor for the title text *Directory listing of* (where * is a wildcard). When it appears, send keystrokes to switch to a non-local website instead. See Using Internet Software for more on this technique.

What keystrokes can you send to a window? You can give regular characters, of course, so to send "abc" simply type that into the bottom 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 ~.

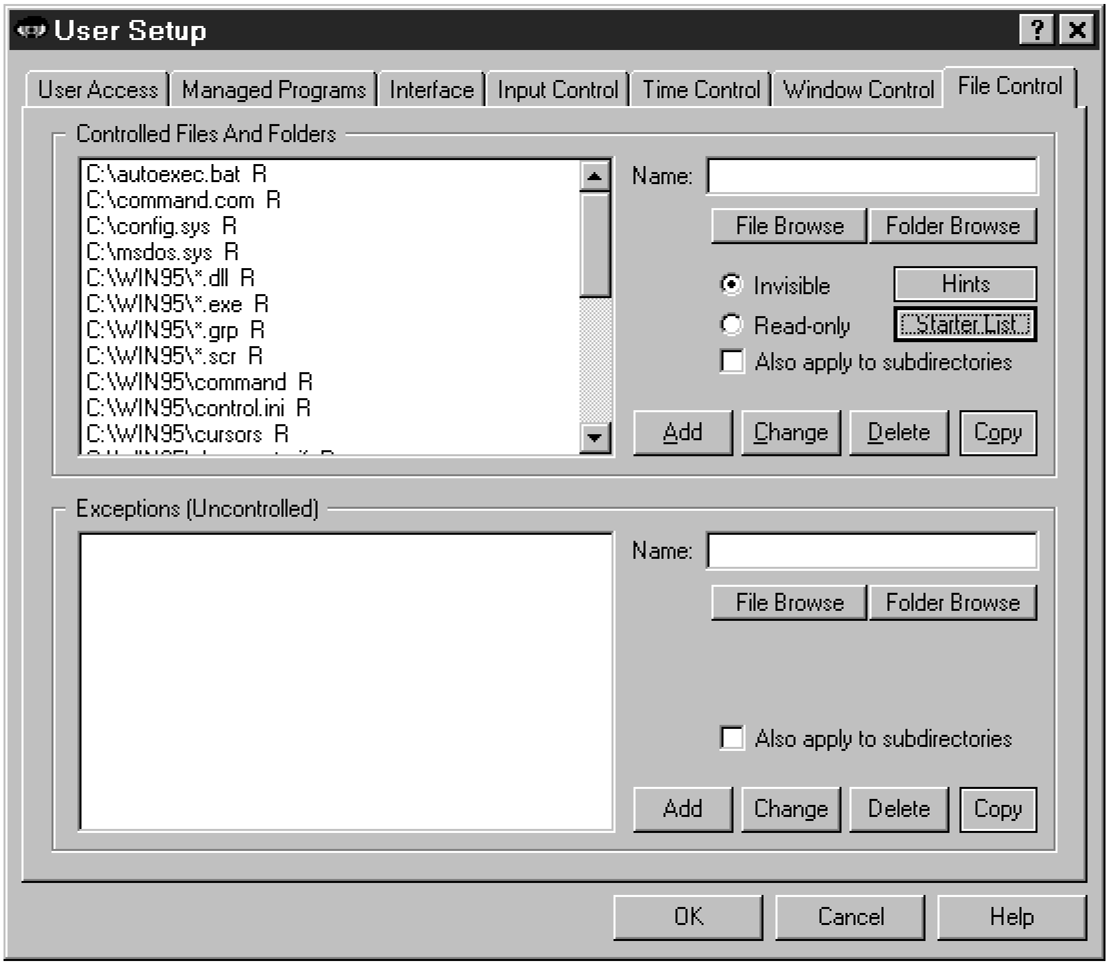
If you need to use a special character in its usual sense, enclose it in brackets. For example to send an actual plus character you'd type {+}. To send an open or close bracket, type {{} or {}} as required.

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



Controlled Files And Folders

C:\autoexec.bat R
C:\command.com R
C:\config.sys R
C:\msdos.sys R
C:\WIN95\*.dll R
C:\WIN95\*.exe R
C:\WIN95\*.grp R
C:\WIN95\*.scr R
C:\WIN95\command R
C:\WIN95\control.ini R
C:\WIN95\cursors R

Name:

● Invisible
○ Read-only
☐ Also apply to subdirectories

Exceptions (Uncontrolled)

Name:

☐ Also apply to subdirectories

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. Because controlled files and folders are locked to both the user and the operating system, certain files and folders should be controlled only with caution. See below for some cautions, hints, and suggestions.

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.

Use the *Exceptions* section when you want to protect the named *Controlled Files And Folders* in general, 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 user.   *Exceptions* are displayed only if there are *Controlled Files And Folders* listed.

The *Exceptions* section also provides a way to set up private work areas for each user. For example, you might have a subdirectory named User Folders, under which each user has a personal directory.   To ensure privacy, you might make all the User Folders subdirectories invisible to every user, but set a different Exception for the folder belonging to that particular user.

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.

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

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.   Be careful when controlling them!   Here are some examples:

Windows Directory: Previously, Microsoft told developers that the Windows directory was the only safe place for programs to automatically write new files.   This is no longer true, but older programs don't know this, and even some modern programs still assume this rule.   Additionally, most programs (and Windows itself) need to update some files that are already there, for example the Registry and certain initialization files in this folder.   Certain subdirectories underneath the Windows folder must remain available too, such as the Recent Documents and Spool folders.

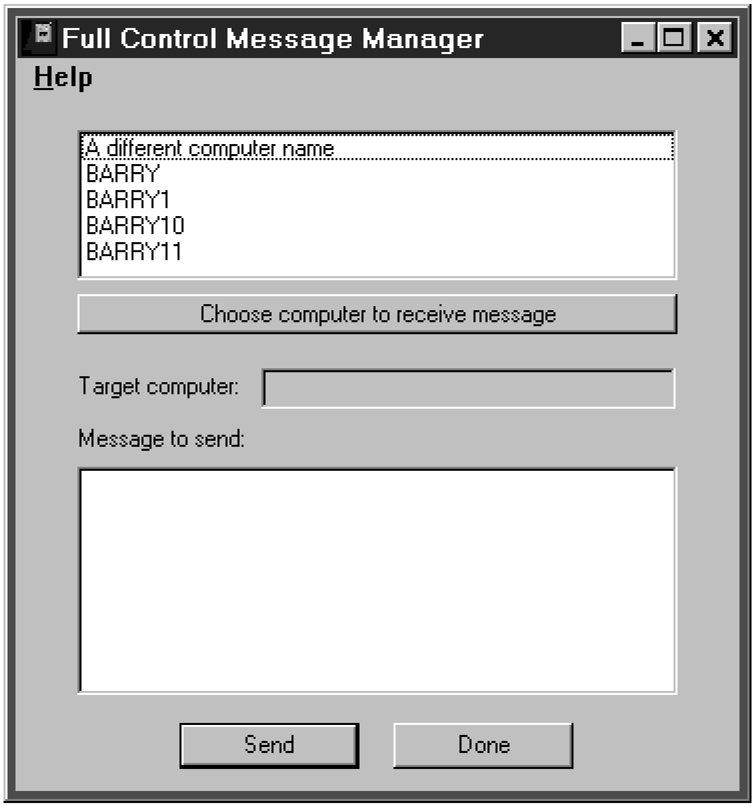
Entire Drive: If you protect the root directory of a drive, don't check the box to include all its subdirectories if those subdirectories include your Windows directory (the usual case for your boot drive), cache directories, or other locations which the system or key programs must have access to.

Directories Listed In Environment Variables: Most computers list certain folders under TEMP or TMP environment variables to tell programs that these directories are available for creating temporary files.   Certain programs also list their own necessary directories in environment variables.   Be very careful when controlling such 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.

Message Manager


Full Control Message Manager
Help
A different computer name
BARRY
BARRY1
BARRY10
BARRY11
Choose computer to receive message
Target computer:
Message to send:
Send
Done

The Full Control Message Manager lets users send brief text messages across the network from one Full Control computer to another. The message will pop up in a box on the target computer's screen. It works somewhat like the WinPopup applet supplied with Windows 95. However, the Message Manager makes it much easier for the administrator to control which users can send messages, and to whom.

To use it, set up the computer to run the Message Manager program (msgmgr.exe) in any way you like. When you run it, the Message Manager screen appears. Where do you want the message sent to? Pick a Full Control computer from the top box. What do you want to send? Type a brief message (up to 300 characters) in the bottom box.

Click the Send button to send the message. "Sending" a message means that it is saved to a file, and the file is placed in the "message" folder designated on the Remote Management tab of this Full Control computer's System Setup dialog. Presumably the other Full Control computers on the network have been set up to monitor this same directory for messages, and they will see this new message when it appears. To use the Message Manager, the network must be enabled for long file names, because message-file names can easily exceed the now-defunct DOS 8.3 filename standard. Full Control checks for messages about once a minute.

The message file is named for the computer to which it is addressed. For example a message file might be named "My Full Control Computer.fcm" and saved in the target directory. If there is already a file named "My Full Control Computer.fcm" then the new message will be named "My Full Control Computer.fcm1" and so forth. A given Full Control computer can have up to 10,000 pending messages. The message is deleted after it is read.

The list in the top box is generated from "*.fcd" data files created by the Full Control Data Extractor program. For each data file it finds, the Message Manager will display one computer name (the name found in that data file). The Message Manager looks for these data files in three places: 1) in its own directory, 2) in the same directory to which it will send its message file, and 3) in the "clone data" directory. The "message" directory and the "clone data" directory are designated on the Remote Management tab of Full Control's System Setup dialog. The data files can be in just one of these locations, or divided into more than one place.

Data Extractor

The Data Extractor creates data files needed by Full Control itself, and by its Remote Administration Manager and Message Manager programs.   To use one of these, you must run the Data Extractor (extract.exe) on each Full Control computer.   The Data Extractor will create one data file for each computer.   Each filename will be the corresponding Full Control system's computer name, so for example if the computer is named LIBRARY COMPUTER   the resulting data file will be LIBRARY COMPUTER.FCD.   Make sure all your computers have different names!

The easiest way to create all the data files is to copy the Data Extractor program to a floppy disk, then take the floppy disk around to all your Full Control computers.   On each computer, run the Data Extractor from the floppy disk.   This will create a new data file in the same directory as the Data Extractor program, that is, on the floppy disk. (Full Control does not have to be running when you do this.)   As you run the Data Extractor on all your Full Control computers, you will accumulate data files on the floppy disk.

When you have done all your Full Control computers, copy all the data files from the floppy disk into a directory from which they will be visible.   This can be the same directory as the Remote Administration Manager, and/or Message Manager program, or it can be the clone-data or message-data directory as defined on the Remote Management tab of the System Setup dialog.   All these places are checked for data files.

You will need to rerun the Data Extractor on any Full Control computer whenever you change the computer's name.   The file created by the Data Extractor is named after the computer name, so if you change the computer's name and copy the new file into the data file directory, remember to delete the computer's old file from that directory.   (It will have the previous computer name for the updated computer.)

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. It's useful if you accidentally create some security control which locks you out of the computer.

Reset Mode is also used to access Full Control's configuration options 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.

To start Full Control in Reset Mode, run the Full Control Reset program (fcreset.exe) from Explorer, or in any other convenient way. Remember that fcreset.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).

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.

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 this user; exit if a user's time has run out; process remote clone, message or remote-administration files; use license metering; monitor window titles; 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.

Also, 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.

Remote Administration Over 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, Remote Commander, and License Meter Manager are designed specifically to allow administrators to dynamically modify settings and control access and activity on networked computers.

Using 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.

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. Fortunately, the title bar of most web browsers will change to indicate that it is accessing a file or directory instead of a webpage. On the User Access tab you can set Full Control to close browser windows that are accessing local files. But you can also use Full Control's Window Control to take other action when this happens. Here is how to set this up for Netscape and Internet Explorer.

Netscape is easy to monitor, because its title bar always contains the phrase "Directory listing of" when accessing a file or directory instead of a webpage. With either Netscape 3 or Netscape 4, you can set up Window Control to look for the window title:

```
*Directory listing of*
```

(note the wildcards) and either immediately close the window, or send keystrokes to set the browser to a legitimate website. Here are two ways to do this. To set Netscape 3 or 4 to your designated homepage website, send the keystrokes:

```
%GH
```

This will send an Alt+G to open the Go menu and an H to run the Home command on that menu. This tells the browser to go to the website you have designated as the home page.

You can set Netscape to any other website by sending it that site's name. For example, this keystroke sequence sets Netscape 3 to the Bardon website:

```
%FLhttp://www.bardon.com/~
```

This sends an Alt+F to open the File menu, then an L to display Netscape's "open location" dialog, then the name of the target website, then a tilde ~ to send the Enter key which submits the command to Netscape.

The command to set Netscape 4 to a specific website is almost identical. Send %FOhttp://www.bardon.com/~ (note the O replaces the L in Netscape 4) instead.

Microsoft Internet Explorer takes a few more steps. First, use its Options menu to show the full path in its title bar. This allows you to monitor for titles of the form:

```
?:\*Microsoft Internet Explorer
```

(note the wildcards) and again, either immediately close the window, or send keystrokes to set the browser to a legitimate website. To set Internet Explorer 4 to your designated homepage website, send the keystrokes:

```
%GH
```

This will send an Alt+G to open the Go menu and an H to run the Home command on that menu. If you use Internet Explorer 3 you'll need to use %GS to go to the "start" page.

Either way, this tells the browser to go to the designated website. Unlike the Netscape browsers there does not seem to be a reliable menu-based method to set Internet Explorer to a specific site other than the "home" site. You might also want to set up a Window Control monitor to immediately close Internet Explorer's Options dialog when it appears so the "full path" setting can’t be changed.

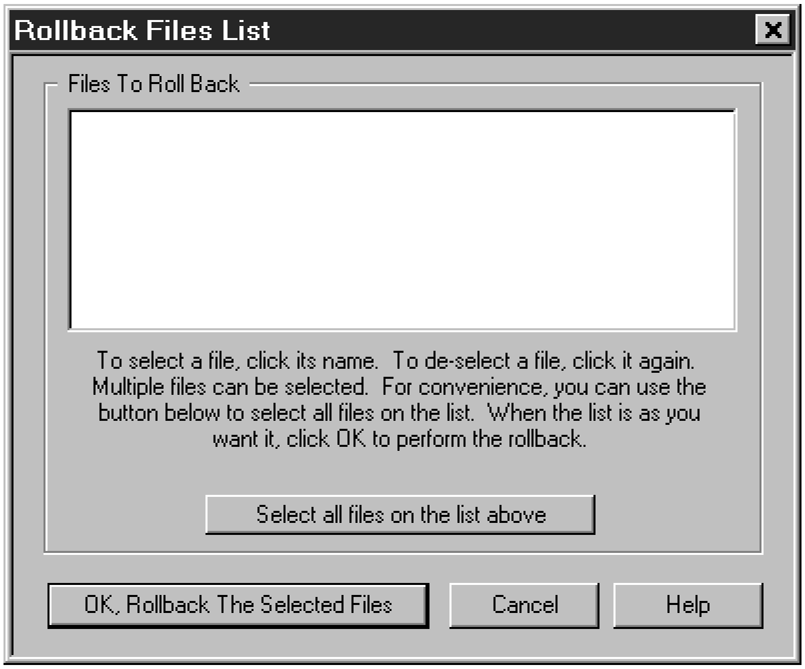
Web Browser Monitor

Full Control can monitor all the websites that are visited while Full Control is running. 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 (3 or 4) or Internet Explorer (3 or 4). This information can be viewed through Full Control's built-in reports.

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

Rollback Files List



Rollback Files List
Files To Roll Back

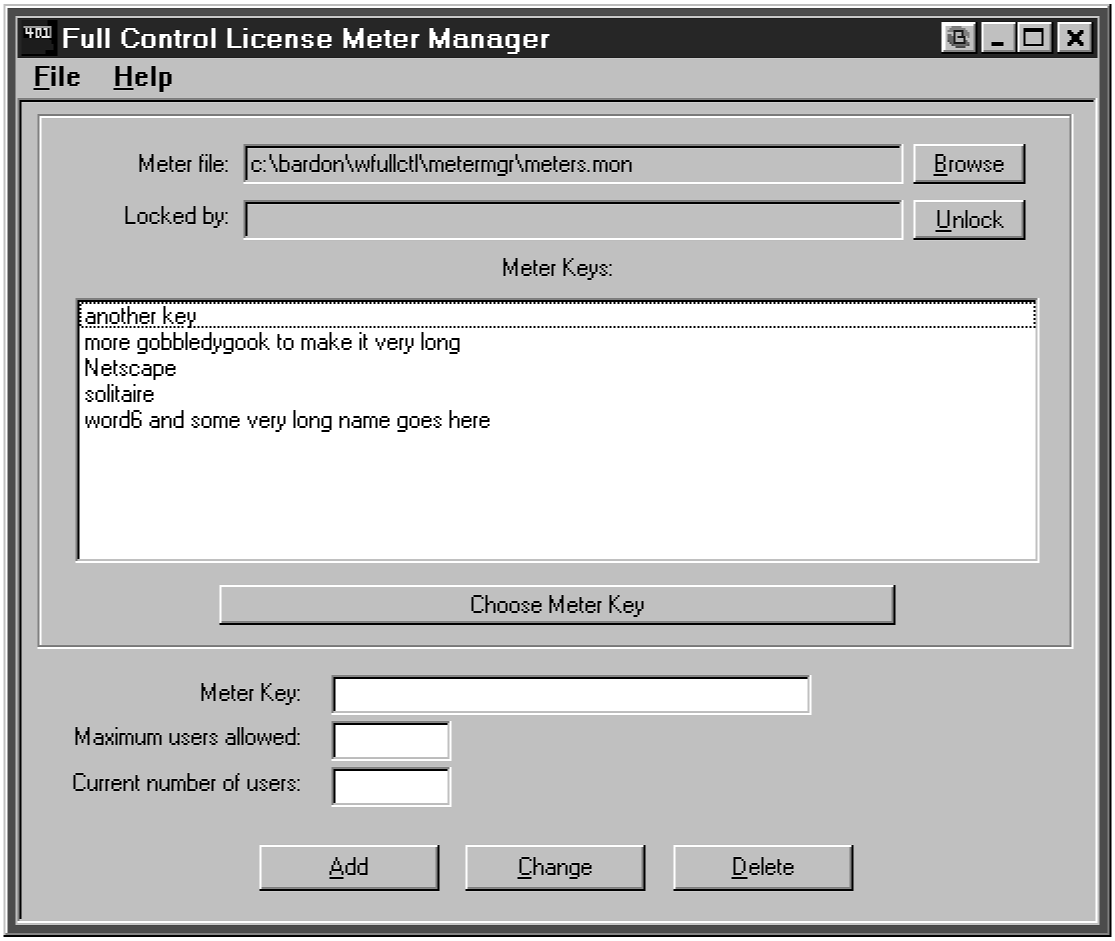
To select a file, click its name. To de-select a file, click it again. Multiple files can be selected. For convenience, you can use the button below to select all files on the list. When the list is as you want it, click OK to perform the rollback.

Select all files on the list above
OK, Rollback The Selected Files
Cancel
Help

This 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.

License Meter Manager



Meter file: c:\bardon\wfullctl\metermgr\meters.mon

Locked by:

Meter Keys:

another key
more gobbledygook to make it very long
Netscape
solitaire
word6 and some very long name goes here

Meter Key:

Maximum users allowed:

Current number of users:

Full Control's built-in network-based license meter management 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 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 managed program's Advanced Settings screen.   You must use the same key name with all managed programs that run the same associated application on all Full Control computers on your network.

When the user runs that program, Full Control will look 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, Full Control 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, Full Control releases the license "slot" making it available to other users.

Full Control looks for license metering information in the license meter monitor file. Give the name of this file on the Remote Management tab of the System Setup dialog. Each client computer must have read/write access to the directory holding the license meter monitor file.

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 Browse button or the File menu to tell the Meter Manager where the license meter file is located. You only have to do this once; the file's name and location will be saved. This is the same file listed in this Full Control computer's Remote Management tab entry and can be updated from there as well.

Selecting a file reads all its keys. To work with an existing key, choose it in the list and click the "Choose Meter Key" button, or just double-click the listed key. The key's data will appear in the Meter Manager fields. You can change the key's settings, or delete it altogether. To add a new key, give its name and settings and click Add.

Administrator Unlock: The meter file is locked by any process updating it. If it is locked, the Full Control computer which has the lock will be listed on the Meter Manager screen. Normally, the lock is held by a process for only a very brief time (less than a second) while it updates the file. If a process locked the meter file but did not unlock it, no users will be able to run any metered applications. In this case, you can use the "locked by" field to see which Full Control computer is behaving abnormally, then use the "unlock" button to correct the situation.

Installing Metered Software: Full Control’s 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, Full Control 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.)

Interfacing With Other License Metering Software: To do the actual locking, unlocking, and checking for available slots, Full Control uses the capabilities of the *validm.dll* file. The version of this file which comes with Full Control provides these services in the way described above. However, if you prefer to provide these services in some other way, you can create a customized *validm.dll* to perform license meter management in any way you like. Your customized license meter management mechanism will completely replace the built-in Full Control mechanism described above. If this is of interest, contact Bardon Data Systems for more information.

License Manager File Format

Full Control's built-in license meter management 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.

Full Control looks for license metering information in the meter monitor file.   Typically, this file would be on a server in a location visible to all Full Control client machines that need access to it.   Give the name and location of this file on the Remote Management tab of each client machine's System Setup dialog.

The license meter monitor file is in the standard Windows ini-file format.   As such, it is plain text, and can be edited by hand.   However, it is much easier to use Full Control's 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.

Consider this license file:

```
[Word 95]
maxAllowed=125
currInUse=62
Full Control computer name 1023452=1
Some other Full Control computer name=1

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

[Netscape]
maxAllowed=50
currInUse=50
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 Full Control computers that are currently using a license.   Blank lines between entries are acceptable.

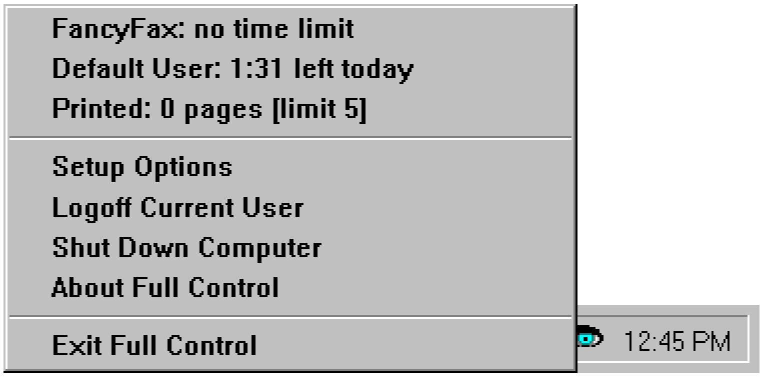
The text in brackets is the section header.   This is the license key name, the lookup key for this licensed application which is specified as the meter key in the monitored program's Advanced Settings screen.   Perhaps this is the name of the program, but it can be any text you choose.

The two entries *maxAllowed* and *currInUse* show the maximum and the current number of users.   The *maxAllowed* entry is a fixed number, set by you with Full Control's License Meter Manager program.   The *currInUse* entry is kept up-to-date by Full Control 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 a set of completely different executables under the same license key (for example an Office-type suite of applications).

Interfacing With Other License Metering Software: To do the actual locking, unlocking, and checking for available slots, Full Control uses the capabilities of the *validm.dll* file.   The version of this file which comes with Full Control provides these services in the way described above.   However, if you prefer to provide these services in some other way, you can create a customized *validm.dll* to perform license meter management in any way you like.   Your customized license meter management mechanism will completely replace the built-in Full Control mechanism described above. If this is of interest, contact Bardon Data Systems for more information.

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.

Clicking on the tray icon pops up a menu. The top few lines in the menu show the current program and user time limits, and the number of pages printed if printing is being tracked. Below that are four password-protected menu options, plus the inevitable About box. 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. This is the same information displayed on the top line of the User Information screen, if the User Information screen is enabled on the Security Settings tab of the System Setup screen. 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. This is the same information displayed on the second line of the User Information screen. Choosing this item closes the menu, but has no other effect.

Pages Printed: If you have set up Full Control to display the number of pages printed, the menu will show the printed pagecount's running total, and (if set) the maximum number of pages this user is allowed to print. This same information is displayed on the third line of the User Information screen. 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.

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.

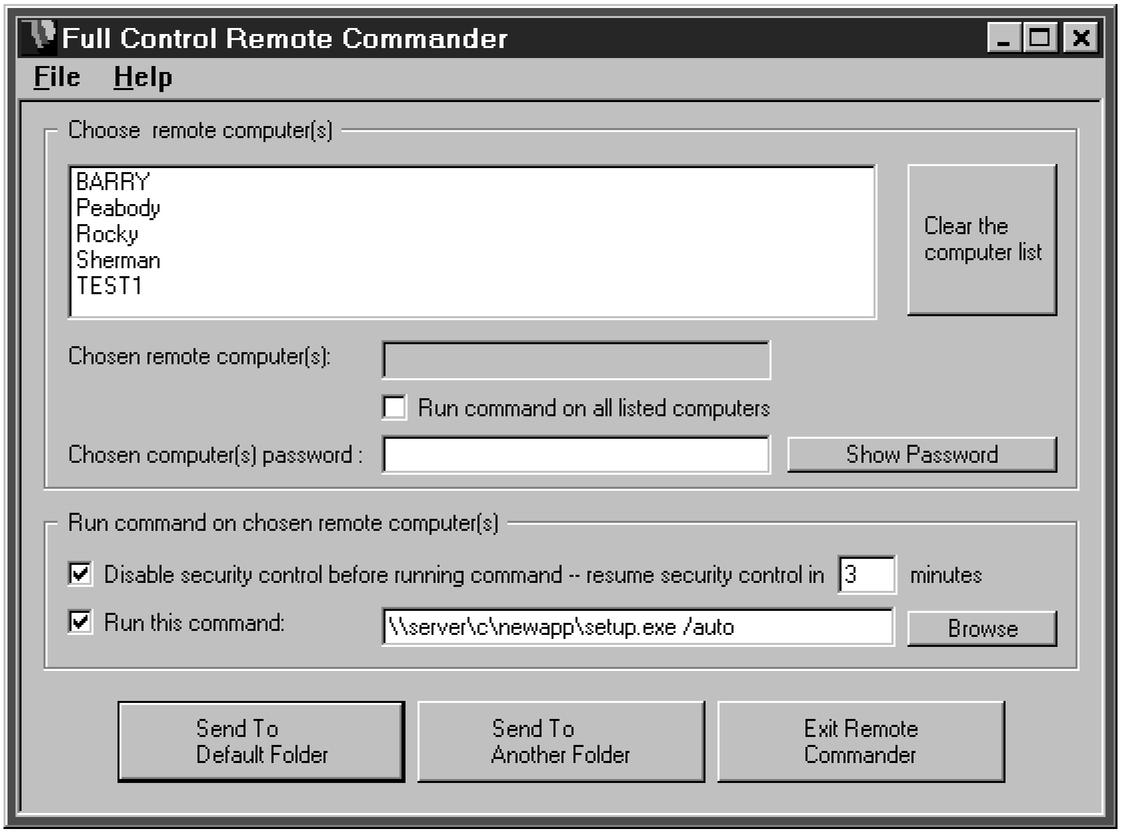
About Full Control: This displays the About box with version and contact information. This entry is not password-protected.

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

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) to log off and put everything right again. Don't worry, if you've disabled the Start button's Shut Down command, it won't log off while Full Control is active.

Remote Commander



Choose remote computer(s)

BARRY
Peabody
Rocky
Sherman
TEST1

Chosen remote computer(s):

□ Run command on all listed computers

Chosen computer(s) password :

Run command on chosen remote computer(s)

☑ Disable security control before running command -- resume security control in 3 minutes

☑ Run this command: \\server\c\newapp\setup.exe /auto

The Remote Commander is a free Full Control add-on utility available on the Bardon website (www.bardon.com). It allows administrators to run commands on any Full Control computer on the network. Like the Remote Administration Manager, the Remote Commander lets the administrator, at another station on the network, create and send "messages" (actually, files with the extension .fct) to Full Control stations elsewhere on the network. Remote Commander messages tell the Full Control computer to run a command on that computer. You can run installers, maintenance programs, batch files, or anything else, from your central administration location.

Setting Up The Remote Commander: It's best to install the Remote Commander to the same directory as Full Control itself, so the Remote Commander can use the regular Full Control helpfile. To do so, simply copy the program (remcmdr.exe) to the Full Control directory.

Setting Up The Local Computer: You set up the local computer to receive messages from the Remote Commander by providing a target directory name on the Remote Management tab of the System Setup dialog. Typically this directory will be on a server, where it can be seen by both the Full Control computer and the administrator's station. The Full Control computer checks this directory for new messages about once a minute. If it finds a message addressed to this computer, the Full Control computer will read it and act accordingly.

Using The Remote Commander: The administrator can run the Remote Commander from anywhere on the network that can access the target directory monitored by the Full Control computer. The network must be enabled for long file names. To set up the Remote Commander, use the Data Extractor to create a set of data files, one for each Full Control computer. Copy these files into the Remote Commander's own directory, or to either of the folders listed on this computer's Remote Management tab. All these locations will be checked for data files when the Remote Commander starts.

To send a command, first choose one or more computers fom the list at the top of the screen. To send the same command 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" box to run the same command on every listed computer. You must also provide the target computer's setup password, so that computer knows the command is valid. If you send one command to multiple computers, all the target computers must have the same setup password.

Next, set up the command by checking the appropriate boxes on the left side and selecting from their options on the right side. Here are the checkbox choices and the options for each choice:

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?

Run this command: This is the command to run on each remote computer. You can type it in, or drag-and-drop a file onto the Remote Commander screen, or use the Browse button to find the correct program. If necessary, you can add parameters on this line as well.

Send To Default Folder: Click this button to send the message to the "Administration and Message" folder listed on this computer's Remote Management tab. If Full Control isn't installed on this computer, or the name of the "Administration and Message" folder hasn't been set on its Remote Management tab, this button is not available.

Send To Another Folder: Click this button to send the message somewhere else.

Remote Commander messages are in the same format as Administration Manager messages. The actual message file 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. 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.

Time-delayed remote commands: Perhaps you want to run a command on a remote computer, but not right away. Here is how to do it. First, set up the Remote Commander's settings as usual: the target computer(s), password, command, and disable-security options. Click the "Send To Another Folder" button and save the ".fct" file to some handy location -- anywhere except the folder being monitored by the target computers, because you don't want them to see this message yet!

When you are ready to run the command, move the ".fct" file to the folder being monitored by the target computers. You can move it by copying it yourself, of course. You can also set up to move it with System Agent or any other timed-application utility. Create a batch file with the COPY command, and tell System Agent to run that batch file at your specified time.

In **ENGLAND**, Full Control is distributed by The Thompson Partnership. Price is £34.95 + £3.00 P&P + VAT (17.5%, EC customers only; or provide Non UK VAT Number if you are VAT-registered outside UK). Payment may be made by cheque, Eurocheque, money order, or credit card. VAT is applicable to orders from any European Union country.

The Thompson Partnership
Lion Buildings
Market Place
Uttoxeter
Staffordshire
ST14 8HP
ENGLAND

Voice: +44 (0)1889 564 601
Fax: +44 (0)1889 563 219
BBS: +44 (0)1889 568 625
Internet Orders: sales@ttp.co.uk
Internet Support: support@ttp.co.uk

You can print this form out by using the PRINT button at the top of this screen.

NAME____

COMPANY____

ADDRESS____

ADDRESS____

TOWN____

CITY____

COUNTRY______________________________ POSTAL CODE_________________

TELEPHONE____

FAX____

E-MAIL____

CREDIT CARD TYPE _____________CREDIT CARD EXPIRATION DATE __ __ / __ __

CREDIT CARD NUMBER __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

£______________ ______Copies of Full Control

£______________ VAT @ 17.5% EC customers only
Or provide Non UK VAT Number
if VAT-registered outside UK

£__3.00________ shipping

£______________ TOTAL

(Please make cheques payable to "The Thompson Partnership", and ensure your cheque card number is written on the reverse of the cheque.)

In **GERMANY**, Full Control is distributed by Vogel Datentechnik. Contact Vogel Datentechnik for current prices and payment methods accepted.

Vogel Datentechnik
Sharible Leserservice
Masurenweg 1
D-85521 Ottobrunn
GERMANY

Voice: (+49) 089 60 85 12 20
Fax: (+49) 089 60 85 12 20

Email: service@sharible.de
http://www.sharible.de/regis/

You can print this form out by using the PRINT button at the top of this screen.

NAME____

COMPANY____

ADDRESS____

ADDRESS____

TOWN____

CITY____

COUNTRY___________________________ POSTAL CODE_______________

TELEPHONE____

FAX____

E-MAIL____

CREDIT CARD TYPE ____________CREDIT CARD EXPIRATION DATE __ __ / __ __

CREDIT CARD NUMBER __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

In **NEW ZEALAND**, Full Control is distributed by PC Support Services. Please contact PC Support Services for information on latest prices and payment methods accepted.

PC Support Services Voice: +64 21 647 955
143 Tuhikaramea Road Fax: +64 78 473 955
Hamilton
New Zealand

Email: jkloeg@pcss.co.nz
http://www.pcss.co.nz

You can print this form out by using the PRINT button at the top of this screen.

NAME____

COMPANY____

ADDRESS____

ADDRESS____

TOWN____

CITY____

COUNTRY_____________________________ POSTAL CODE_________________

TELEPHONE____

FAX____

E-MAIL____

CREDIT CARD TYPE _____________CREDIT CARD EXPIRATION DATE __ __ / __ __

CREDIT CARD NUMBER __ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __

Full Control Bestelformulier voor Nederland en België

(Gebruik "Afdrukken"   uit bovenstaand menu, of markeer de tekst en kopieer hem naar het klembord)

De distributie en support van Full Control wordt in Nederland en België verzorgd door CopyCats Software & Services. De prijs van Full Control bedraagt fl 129,50 / 2395 BF incl. BTW en verzending.   Voor dit bedrag krijgt u de nieuwste complete versie met manual en recht op ondersteuning. Full Control wordt uit voorraad geleverd.

Om Full Control te bestellen stuurt u dit formulier volledig ingevuld aan:

CopyCats Software & Services
Postbus 1088
1700 BB   Heerhugowaard
Nederland
Tel. +31 (0)72 5745993,   Fax 5726559
E-mail: copycats@compuserve.com

KvK Alkmaar 37064222
Postbank (NL) 43.28.577
Postcheque (B) 000-1656064-80
BTW-Nr NL-185.152.119.B01

Ook voordelige multi-user licenties (5+ users) zijn leverbaar. Informeer naar de prijzen!

JA, Full Control bevalt mij! ik bestel hierbij:

```
Aantal:   Produkt:                 Prijs p.s.           Totaal:
-----------------------------------------------------------
....      Full Control single user á fl 129,50 / 2395 BF   .........

=========

Naam     : .........................................   M / V
Bedrijf : ................................................
Adres    : .................................................
Postcode: ............ Plaats: ........................
Land     : .......... E-mail: ...........................
Telefoon: .................. Fax: ....................

BTW-Nr   : (Belgische bedrijven)   |B|E|-|_|_|_|_|_|_|_|_|_|
Deel het ordertotaal door 1,175 als u een geldig BTW-Nr opgeeft!
```

Betaalwijze: *(ongeacht uw keuze ontvangt u een BTW-factuur)*

```
[ ] Bijgesloten cheque of betaalkaart.
[ ] (NL) Reeds overgemaakt op Postbank 43.28.577.
[ ] (B) Reeds overgemaakt op Postrekening 000-1656064-80.
[ ] Op rekening (grootbedrijf, overheid, onderwijs).


Datum: ...-...-...   Handtekening: ........................

Ik hoorde voor het eerst over Full Control via: ..................
Ik heb deze evaluatieversie gevonden op: ..................
```

Vriendelijk dank voor uw bestelling!

Genoemde prijzen zijn onder voorbehoud geldig t/m 31-08-1998. Bel na die datum eerst voor actuele prijzen.

In **AUSTRALIA** , Full Control is distributed by Comput-Soft. Price for Full Control is AU$99.00 plus postage. Contact Comput-Soft for more information on payment methods accepted.

Comput-Soft
P.O. Box 506
Welland, 5007
South Australia
comput@eisa.net.au
http://www.eisa.net.au/~comput

Voice: 08 83464614
Fax: 08 83464614
Mobile: 015 793311

Ring in regard to site licences etc.

You can print this form out by using the PRINT button at the top of this screen.

NAME____

COMPANY____

ADDRESS____

ADDRESS____

TOWN____

CITY____

COUNTRY______________________________ POSTAL CODE_________________

TELEPHONE____

FAX____

E-MAIL____

C.O.D __

Cheque __

Postal Order __