WinU 7

Security Access Control
For Windows

Installing, Using and Mastering

Bardon Data Systems

WinU 7

Security Access Control
For Windows

Installing, Using
and Mastering
WinU 7

Bardon Data Systems

WinU 7: Security Access Control For Windows
Installing, Using and Mastering

Contents

1. Getting Started

2. A Tour Of WinU

3. Setting Up Program Buttons

4. Security And Administration

5. Advanced Topics

6. Companion Software

Appendix A: File Formats

Appendix B: Miscellaneous

Chapter 1

Getting Started

Introduction

WinU: systems management, access control, event logging, web-browser tracking, remote administration ... and a simplified replacement user interface that makes computers accessible to even the most novice users.

WinU is a complete Windows 95/98/ME/NT/2000/XP/Vista/Win7 systems management solution. It includes security access control, malware/spyware oversight, time limits, logging, web-browser tracking, remote administration, and many flexible configuration options. In addition, WinU features a simplified replacement user interface that makes computers accessible to even the most novice users. With WinU, businesses can let employees use authorized applications, yet monitor all activities and prevent them from accessing or installing other programs ... stores, schools, and libraries can allow public access to their computers, yet safeguard computers against tampering ... and parents can control which programs and websites their children use.

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

System stabilization: After you finally get your systems the way you want them, what will keep them that way? What prevents the installation and use of unauthorized software, as soon as you turn your back? WinU can log all usage, prevent unauthorized installation, monitor and reconfigure settings remotely.

Stops malware, spyware, trojans, and more: WinU includes Intrusion Control that watches for programs that behave suspiciously. It can stop them silently and automatically, or ask what it should do. Naturally, the way it watches is completely customizable.

Web browser and application oversight: WinU monitors all World Wide Web browser activity by name, location, and time, providing a complete audit trail of all Web activity. It also logs all software usage, attempts to access locked files or folders, attempted password hacking, and more. Its built-in reports and graphs can analyze this information, or the data can be exported to any database or spreadsheet.

Configuration tracking and helpdesk support: When a computer acts oddly or crashes for no reason, wouldn't it be handy if support staff could call up a minute-by-minute list of all running programs? That's what Diagnostic Snapshot Logging is all about. It even lists hidden programs that won't show up on the Close Programs (Ctrl+Alt+Del) screen.

Simplified replacement user interface: WinU replaces the regular Windows interface (desktop icons, Start button, taskbar, etc.) with a full-screen simplified replacement user interface that's intuitively obvious and easy to use. This simplified replacement user interface makes computers accessible to even the most novice users. Staff with no training or instruction can understand how to run your designated software, so they can easily do what they are supposed to do. In addition, WinU's security features ensure that users don't do what they're not supposed to do. The time and cost of training staff to use computers is dramatically reduced.

Remote administration: WinU'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 WinU stations. Administrators can remotely manipulate the Registry, see and change the status of remote computers, and more, all from one central location. Administrators can also run commands remotely -- installers, uninstallers, maintenance programs, batch files, or any other software. These commands can even be broadcast to all stations at once, a handy way to automate software distributions across the network or do any other mass-manipulation chores. Administrators will also appreciate the built-in management tools and reports. They make it fast and easy to configure a WinU station to do whatever you require, even clone that station onto another computer without re-entering anything.

Logon validation: WinU can validate users at logon, even on laptops and other stand-alone Windows computers -- no network or NT/2000/XP/Vista/Win7 server is required. Unlike the standard-issue Windows logon screen, which is easily bypassed by pressing Escape or in other ways, WinU ensures that only valid users can log on. If you do have a network server, WinU can coordinate with it and ensure that no user can log on, even just onto the local computer, unless validated by your server.

What's included: WinU includes everything you need in one purchase: client-side monitoring software, central administration utilities, event logging, built-in reports, and other utilities.

Setup and configuration: Click the menu's Setup item to access the setup options. If the menu is hidden, click the WinU icon at the left edge of the title bar. These options are grouped by functional area onto two tabbed screens, Desk Setup and System Setup.

The Desk Setup screen controls per-desk options. Each desk can have different time limits, locked or hidden directories, allowed applications, look-and-feel options, and more. The user logs on at the regular Windows logon screen. If the logged-on user has a per-user Default Desk listed, that desk is shown for that user. If the Windows logon name is not listed, WinU uses its Default Desk. Or you can set up WinU so unknown users are not allowed to log on at all.

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

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

Installing And Uninstalling

To install WinU, run the program install.exe that comes with WinU. It will ask you the folder you would like to install into and what Start button group name you prefer. The installer will not put anything into any folder other than the one you specify, other than NT/2000/XP/Vista/Win7 drivers which are installed into the "drivers" folder. It will not change any system files, other than the Registry (per Microsoft standards). In NT/2000/XP/Vista/Win7, the logged-on user must have Administrator rights for the install to be successful.

WinU Extended Administration Kit: The WinU Extended Administration Kit includes the Logon Manager, Password Manager, and WinU Timer utilities. These optional tools extend WinU's capabilities. This add-on toolkit is available from from Bardon Data Systems.

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

Sample Desk: The first time you run WinU after installing, or anytime you start when there are no other desks, WinU creates a Sample Desk with a few buttons and sets it as the default desk. This lets you use WinU and get a feel for what it can do. In addition, some of the Sample Desk buttons illustrate handy WinU techniques.

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

Version Upgrade: If the computer has settings from a previous install of WinU, those settings will be read and used. If upgrading from 5.0 or later, the Remote Administration Manager can "broadcast" an upgrade to a later version.

Major-Upgrade Licensing: When doing a major-version upgrade (6.x to 7.x for example) and the old-version settings are automatically imported, it will be an unlicensed version even if the old version was licensed, because the old-version licensing won't apply to the upgrade. This is easily addressed by arranging for upgrade licensing, then distributing the new license key in a clonefile with the actual software upgrade. To do this, first install this new version on one computer. The old-version settings will be automatically imported into that computer. Or load in an old-version clonefile, that works too. Next, enter your new-version license number and create a clone file from that computer as described above. Include it with the install. This will bring in the new license data along with the settings.

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

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

WinU can't be uninstalled while it is running. In NT/2000/XP/Vista/Win7, the logged-on user must have Administrator rights for the uninstall to be successful. The uninstaller closes all active Explorer windows, a necessary step to deactivate some of the oversight components.

Automated Unattended Remote Install: The WinU 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	installer runs in automated mode
/addstart	icons will be added to the Start menu
/admin	also install administrator's tools
/targetdir=	folder into which files should be installed
/pausecmd=secs,cmd	run a command after install

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

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

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

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

The /targetdir item is also optional. If it is not given, WinU will be installed into the default directory, which is the \Program Files\WinU5 folder on the same drive as the computer's Windows directory.

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

Remote Install Options: Tools such as SMS can run parameterized commands remotely, or command-line parameters can be given by running the installer from a batch file, Shortcut, etc. This is easier than creating an SMS distribution. Simply place the WinU files in a network folder visible from your target computers (a read-only folder is fine) and distribute a command that points at the installer in that server's visible folder. You can even set up the batch file to delete itself after the install is complete. See below for more on this technique.

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

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

```
IF NOT EXIST c:\your path\yourdir\winu.exe \\server\c\masterdir\install.exe /auto
```

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

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

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

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

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

Quick Start

WinU In A Nutshell: WinU is a complete simplified replacement user interface with comprehensive security and system-management features. The WinU interface consists of buttons on a desktop. Use the keyboard or mouse to press any button and run its program. With the setup password, you can right-click on a button to change that button's settings, or right-click on the desk to modify desk settings, or use the Setup menu to change systemwide settings, or launch Explorer from within WinU.

WinU monitors every user logon and every running program, and can log all activity. If you have set up a particular application as a managed button program, WinU 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. WinU replaces the usual Windows screen with a complete simplified replacement user interface that makes computer usage easy, even for novices. At the same time, WinU enforces security and makes the computers easy for system administrators to manage remotely.

WinU 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.

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 WinU computers over a network.

Quick Start: WinU comes preconfigured with default settings so that you can get a feel for how it works. You will likely want to modify the default settings. Here's how:

- Decide if unknown users can log on, or if users must be "known" in order to use the computer. Then 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 a different WinU default desk, set up Windows to display its "log on by user name" screen when Windows starts. This step is optional, because even if you don't use the logon screen at all, WinU will work perfectly well by using its Default Desk as the initial desk for all users, providing them the permissions and restrictions you have listed as the default.

- Configure systemwide settings through the Setup menu items. Start with the System Setup screen. Modify the settings in the first three tabs (Security Settings, Event Log, and Screen Options) as needed. The fourth tab, Reports, displays usage reports and graphs. Use the fifth tab (Remote Management) to set up network-based WinU configuration updates, remote management and monitoring, and other communication and control options. The sixth tab (Intrusion Control) handles malware, spyware, trojans, browser hijacks, and similar nasties, as well as letting you lock down USB ports and drives.

- Set up your desks. WinU can control a thousand separate desktops per computer, each with its own buttons and settings. Create a new desk by clicking the Logon menu (or just left-click anywhere on the desk, or right-click the Apps Button). This displays the Choose Desk screen. Click the Add New Desk button. WinU will create a new desk and then display the Desk Setup screen in which you can add programs and configure the new desk to your liking. Other ways to display this screen are by right-clicking on the desk, or by choosing the Setup menu’s Desk Setup item, or from the System menu or Apps Button. The easiest way to add program buttons to a desk is to "drag and drop" files from Explorer onto the WinU desk. You can also add program buttons by entering them through the Buttons tab of the Desk Setup screen. Buttons can launch programs, Shortcuts, or any file with a known file extension. Buttons can also be set up to log off the current desk and go to another, exit WinU, shut down the computer, run the current screensaver, and do other system-like tasks.

You're Done: Now that 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, but a clone configuration can be replicated on other computers even if a network is not available. A clone file is also a good way of backing up your work.

If more than one person will be using this computer (or this replicated clone setup), think about which default desk each user should start on.

WinU Interface Elements

Dialogs: WinU has three main dialogs: System Setup, Desk Setup, and Choose Desk. The System Setup and Desk Setup tabbed dialogs are only available to those who know the setup password. The Choose Desk screen is available to all users through the menu bar's Logon item, by left-clicking anywhere on the desktop, or by right-clicking on the roving Apps Button. However, all of these methods can be disabled.

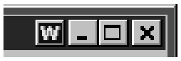
Title Bar: WinU's title bar displays the name of the current desk. It can also show the current user's logon name, and the computer name (set on the Screen Options tab). When WinU is in Setup mode, the title bar blinks as a reminder that this special mode is in effect.

Menu: The menu bar has three top-level items: Setup, Logon, and Logoff. The Setup menu items (aside from the About item) are only available by giving the setup password. Logon and Logoff are available to all users. Logon and Logoff are also available from the Choose Desk dialog, which can be displayed by left-clicking on the desktop. The menu bar can be hidden via a Kiosk Mode switch. (Desk-click dialogs can be disabled via Kiosk Mode as well.) Some of these menu items are also available from the System Menu, which can be displayed by clicking the icon at the left edge of WinU's title bar.

Status Bar: The Status Bar at the bottom of the screen has three segments. It shows a date/time clock, time limits (if any) for the current desk, and time limits (if any) for the current program, that is, the program launched from WinU which currently has the active focus. When WinU is in Setup mode, the clock area of the status bar bar blinks as a reminder that this special mode is in effect.

Scroll Bar: The scroll bar at the right side of the screen is displayed only if there is more than one screenful of buttons on the current desk. If all buttons are displayed, the scroll bar is not neded, so it is hidden. If it is showing, use it to move up or down the displayed buttons on this desk. You can also use the keyboard's arrow or tab keys to move to other buttons.

Apps Button: This button hops into the title bar of the current active application, so it's always accessible. The user can click it to list and launch all applications on the current WinU desktop. This is handy when the current active application blocks access to the WinU desktop buttons. If allowed, right-click the button to show another menu containing administration and navigation entries.

Here is how the Apps button appears in a title bar: 

It can be configured in a number of ways by using available apps button options.

Background: The background image can be any bitmap file of any size or color depth. It can be displayed either fullscreen or just in the top half of the screen. It can be tiled, or stretched to fill the entire available area, or displayed at its actual size. If you have chosen to retain its aspect ratio, it will be displayed without distorting its relative proportions. If the image is in the top half of the screen, the desk’s buttons and scroll bar are restricted to the bottom half. In this case, the button area’s background is a neutral gray color in normal mode. In Setup Mode, the button background changes to a bright turquoise color as a reminder. This is set up from the Appearance Tab of the Desk Setup dialog.

Program-Launch Buttons, Navigation Buttons, Function Buttons: WinU’s buttons are set up from the Buttons tab of the Desk Setup dialog. Buttons can launch programs directly, or run Shortcuts, or hold files for which there is a registered file extension. Buttons can also be set up to transfer the user to another WinU desk, or return to the previous desk. Like any other buttons, these DeskLink or PrevDesk buttons can have passwords, which will be tested before WinU changes desks. (Of course, the target desk can also have its own password.) Special buttons can also be set up to exit from WinU, shut down the computer, or perform system-level functions such as saving a Diagnostic Snapshot or launching the current screensaver; again, they can be password-protected.

Many button style options are available, including font, border, placement, and label options. You can choose any icon from a multiple-icon file, or use virtually any other image source on a button, not just icons. Images can be extracted from EXE, ICO, DLL, CUR, ANI, or BMP files, among others; the chosen graphic is resized to icon-size onto the button.

Companion Software: WinU also includes companion software used by the administrator to dynamically manage a remote system's configuration, passwords, time limits, rebooting, and license metering.

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 WinU won't interfere when programs such as Explorer or the Taskbar are accessed. This makes it easy for the system administrator to modify WinU settings, "drag and drop" programs onto the desk and create new buttons, or use other software tools that a normal user would not have access to.

To exit from Setup Mode, choose *Exit Setup Mode* from WinU's menu bar, or by right-clicking on the Apps Button, or from the System menu by clicking on the icon at the left edge of WinU's title bar. WinU will then reset to the previous security mode.

As a visible cue that Setup Mode is in effect, the WinU window shrinks. The title bar, status bar, and background color also change to indicate that this mode is in effect.

The Setup Password

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

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

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

The pre-purchase evaluation version of WinU 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."

Emergency Passwords

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

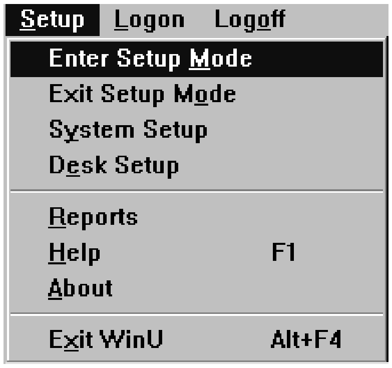
If you tried what you thought was the right password, and it didn't work, you still may not need an emergency password. Passwords are case-sensitive by default, so if your Caps Lock is on, the password might not match. Try hitting the Caps Lock key, then give the password again.

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

Chapter 2

A Tour Of WinU

Setup Menu



The Setup Menu is the main “control center” which you use when configuring WinU. To use any of its options you must first give the setup password when prompted. WinU 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 Exit Setup Mode.

Enter Setup Mode: This puts WinU into Setup Mode. You can then drag-and-drop programs onto the WinU desktop, or use any other system administration features.

Exit Setup Mode: This exits from Setup Mode into the regular user mode.

System Setup: This puts WinU into Setup Mode and displays the System Setup dialog. This dialog has six tabs: *Security Settings, Screen Options, Event Log, Reports, Remote Management* and *Intrusion Control*. For more information, see the detailed description of this dialog.

Desk Setup: This puts WinU into Setup Mode and displays the Desk Setup dialog. This dialog has seven tabs: *Access, Managed Buttons, Interface, Input Control, Time Control, Window Control,* and *File Control*.

Reports: This menu item provides a shortcut to the *Reports* tab of the System Setup dialog.

Help: The setup password is required to use Help, because this information is designed for administrators, not casual users. This password protection helps prevent casual users from learning the "inner workings" of WinU.

About: WinU version and other information. The About item is the only entry on the Setup menu that does not require the setup password in order to be used.

Exit WinU: The setup password is required to exit when using this menu item, or when exiting by pressing Alt+F4 or clicking on the titlebar's X button. The setup password is not required to exit when using an Exit or Shutdown button, created by you, on the desktop. However, like all other buttons, an Exit or Shutdown button can be password protected in the usual manner.

Logon and Logoff Menus

Clicking the Logon item shows no actual menu. Instead, it will display the Choose Desk dialog. With this dialog, users can log on to a new desk. By giving the setup password, administrators can add, delete, or copy a desk from this dialog as well.

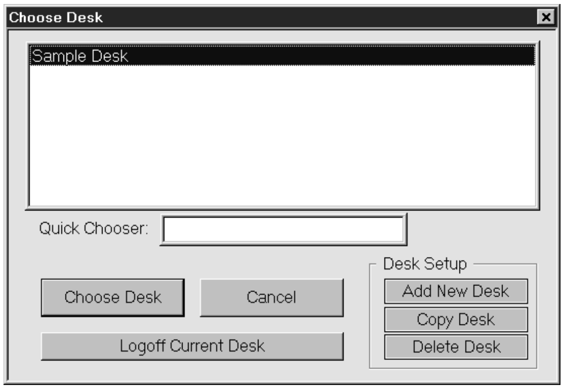
Another way to display the Choose Desk dialog is to left-click anywhere on the desk. If desk-click dialogs haven't been disabled with one of the Kiosk Mode options, the dialog will appear where you clicked your mouse. If allowed, right-clicking on the roving Apps Button provides another way to select the Logon menu item.

Like the Logon menu, clicking the Logoff item shows no actual menu. Instead, it simply exits from the current desk. If there is a default desk, it will be displayed. If there is none, the initial "No Desk" screen will be displayed. In general, exiting from a desk automatically terminates all applications launched from that desk.

You can also log off the current desk by left-clicking on the desk to bring up the Choose Desk dialog, then using its Logoff option. If allowed, right-clicking on the roving Apps Button provides another way to select the Logoff menu item.

The entire menu bar can be hidden with a Kiosk Mode option. If so, the Logon and Logoff Menus are unavailable.

Choose Desk Dialog



With this dialog, users can log on to a new desk, or log off the current desk. Scroll the list to the desired desk, select it, then click the Choose Desk button. Or just double-click the entry on the list.

If the list is very long, you'll appreciate the Quick Chooser. Type the first few letters of the desired desk into the Quick Chooser, and the list will scroll to bring the matching desk name(s) into view. When your desk is highlighted, press Enter or click the Choose Desk button to select it.

For convenience, the Choose Desk dialog can also be used to log off the current desk.

Administrators can add, delete, or copy a desk from here as well. The setup password is required to use these buttons.

In Setup Mode the Choose Desk dialog lists the desk *number* as well as the desk *name*. The desk number is used in conjunction with certain WinU companion programs and administration features.

Bring up the Choose Desk dialog by clicking the Logon menu item or left-clicking anywhere on the desktop. If allowed, you can also right-click WinU's roving title bar button and choose *Logon* from its popup menu. All these access methods can be disabled with Kiosk Mode settings.

System Setup Dialog

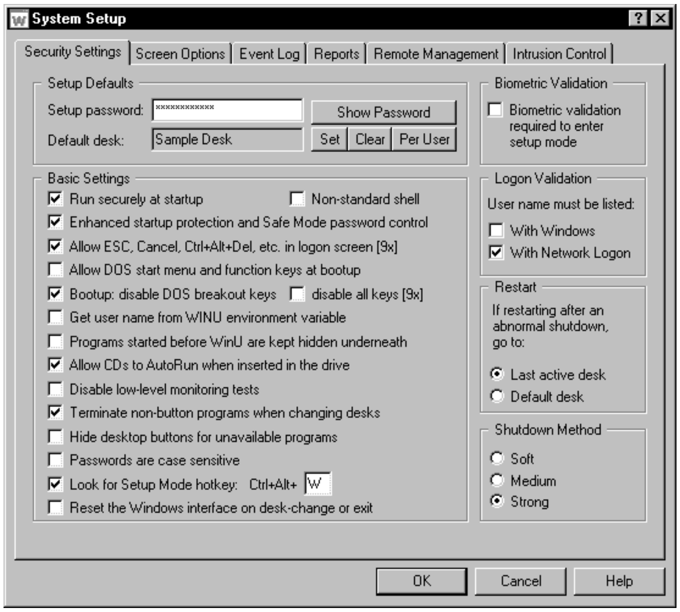
To set up systemwide options, use the System Setup tabbed dialog. Usually you'd launch this dialog through the menu bar's Setup menu. If allowed, you can also right-click WinU's roving Apps button and choose System Setup from its popup menu.

You can also get to the System Setup screen through the title bar's System menu. WinU adds this item to the System menu so that, when the WinU menu bar is hidden (via Kiosk Mode) the administrator can use the System menu to get out of Kiosk Mode. To open the System menu, click the icon at the left edge of WinU's title bar.

The System Setup dialog has six tabs:

Security Settings: systemwide security and preference options
Screen Options: password display time, Kiosk Mode, systemwide time limits, Apps Button
Event Log: logfile usage and tracking options
Reports: view and print usage reports and graphs
Remote Management: network-based remote management
Intrusion Control: control USB ports and drives,malware, adware, browser hijacks, trojans, etc.

Security Settings Tab



System Setup

Security Settings | Screen Options | Event Log | Reports | Remote Management | Intrusion Control

Setup Defaults

Setup password: ************ [Show Password]

Default desk: Sample Desk [Set] [Clear] [Per User]

Biometric Validation

□ Biometric validation required to enter setup mode

Basic Settings

☑ Run securely at startup □ Non-standard shell
☑ Enhanced startup protection and Safe Mode password control
☑ Allow ESC, Cancel, Ctrl+Alt+Del, etc. in logon screen [9x]
□ Allow DOS start menu and function keys at bootup
☑ Bootup: disable DOS breakout keys □ disable all keys [9x]
□ Get user name from WINU environment variable
□ Programs started before WinU are kept hidden underneath
☑ Allow CDs to AutoRun when inserted in the drive
□ Disable low-level monitoring tests
☑ Terminate non-button programs when changing desks
□ Hide desktop buttons for unavailable programs
□ Passwords are case sensitive
☑ Look for Setup Mode hotkey: Ctrl+Alt+ W
□ Reset the Windows interface on desk-change or exit

Logon Validation

User name must be listed:
□ With Windows
☑ With Network Logon

Restart

If restarting after an abnormal shutdown, go to:
● Last active desk
○ Default desk

Shutdown Method

○ Soft
○ Medium
● Strong

[OK] [Cancel] [Help]

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

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

Default Desk: The default WinU desktop is displayed at startup and when users log off other desks. It's an automated process. Even if the default desk is password-protected, the user won't be asked for that password when logging off another desk, or at startup when the system first sets to that desk. This section has three buttons labeled *Set, Clear,* and *Per User*. Click *Set* to choose a single desk as the default, or *Clear* to remove the existing default-desk setting.

Click *Per User* if you want the default desk to be dependent on the current multi-user or network logon. When you click this button the Per-User Default Desk screen is displayed. Windows and most networks let the user specify a name when logging on to Windows. WinU can look at this user name to see who is logged on, then display the appropriate default desk for that person. If a different user logs on to Windows a new default desk would be shown. Also, to accomodate older networking software which is not Windows-aware, you can optionally set up WinU to look for the current user name in an environment variable instead of the standard Windows registry-based location.

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

The other options let you further fine-tune WinU's behavior. They are:

<u>Run securely at startup</u>: This will set up the computer so WinU is run whenever Windows starts. Unlike a shortcut in the Startup folder, this method cannot be bypassed by pressing the Shift key when Windows comes up.

<u>Enhanced startup protection and Safe Mode password control:</u> Checking this box will set WinU to validate the user’s logon name immediately when they type it in, rather than after the WinU desktop appears. It will also password-protect Safe Mode, a special mode built in to Windows to allow for error recovery. In Safe Mode, many protections are disabled by Windows. If you check this box, WinU 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. In Windows 9x checking this box starts WinU before certain Windows shell components. If starting this early causes any problems, set a BDSWSHELL=1 environment variable. This tells WinU to start the Windows shell components first.

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

<u>Allow ESC, Cancel, Ctrl+Alt+Del, etc. in logon screen [9x]:</u> Unless this box is checked, WinU disables the Escape key and Cancel button in logon data-entry screens (it allows Escape and Cancel in simple message boxes). It also prevents any other bypass of the logon process, such as pressing Ctrl+Alt+Del to bring up the Close Programs box or Ctrl+Esc to bring up the Task Manager. If you are doing your logon validation through a Novell or NT/2000/XP/Vista/Win7 network, you should check the "With Network Logon" box, and you should probably check this box to allow the ESC key, Cancel button, etc. On stand-alone computers, or on peer-to-peer networks, you'll generally want to un-check this box, thus providing protection. Generally, you will want to un-check this box (to deny use of ESC, Cancel, etc.) if you are doing logon validation "With Windows", or if you haven't checked either of the logon validation boxes. This option is ignored under NT/2000/XP/Vista/Win7, which does not allow invalid logons.

Allow DOS start menu and function keys at bootup: This option is primarily for Windows 9x but also has a useful effect under NT/2000/XP/Vista/Win7. Under Windows 9x, it lets you control whether the keyboard and startup menu can be used when the computer starts. At boot time, pressing F4 starts the previous version of DOS, F8 brings up the startup menu providing methods to run bare DOS, "safe mode," etc. To enhance security, uncheck this option so WinU will disable access to these and the other boot-time keys. However, even when these keys are disabled, if Windows detects an abnormal bootup it will display the startup menu anyway. This could allow the user access to the "backdoor" methods described above. Therefore, using this option also sets a system flag which makes the startup menu more difficult to use: if the menu does indeed appear, its default choice is instantly chosen, then the menu immediately vanishes. Under NT/2000/XP/Vista/Win7, this option immediately closes the Boot Loader menu by automatically selecting the default choice Therefore, when using this option on dual-boot systems where you always want NT/2000/XP/Vista/Win7 to load, make sure you have set NT/2000/XP/Vista/Win7 as your default operating system in your boot.ini file. This setting is ignored under Windows ME because that operating system cannot boot to DOS.

Bootup: disable DOS breakout keys / disable all keys: In Windows 9x DOS programs that run from the autoexec.bat file can create a problem, because users can type Ctrl+C or Ctrl+Break to terminate those programs and gain access to the DOS prompt. While such programs are active, users can also type Ctrl+Alt+Del to restart the computer. To prevent the use of these keys, check the box labeled *disable DOS breakout keys.* Or, if you want to completely disable the keyboard until Windows loads, check the box labeled *disable all keys.* These options will add commands to your autoexec.bat to monitor the keyboard; if the computer has no autoexec.bat, no oversight is necessary so no commands are added.

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

These options are grayed-out if you have allowed the DOS start menu and function keys at bootup (the checkbox directly above this one). They are ignored in NT/2000/XP/Vista/Win7 because in NT/2000/XP/Vista/Win7, DOS does not load before Windows.

Get user name from WINU environment variable: At startup, WinU looks for the logon name of the current user. As described above, this name can be validated to control logon access. 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, WinU can get the user name from the WINU environment variable instead. Of course, you will need to modify your logon script to place the username into this environment variable at logon.

Programs started before WinU are kept hidden underneath: Check this box if you will be running programs before WinU launches and want to ensure that the user cannot access these programs, for example fax/modem management software or similar system-level utilities automatically run at startup. If this box is checked and the user tries to Alt+Tab to such programs, their windows will be pushed underneath WinU again. However, remember that these programs will not even be able to display a message dialog to the user! So, you should only check this box if you are sure that your programs will never need to interact with the user. If you do check this box, and you want to allow the user to access certain particular programs (which were run before WinU), list the filenames of such programs as Allowed Filenames on this desk's Access tab.

Allow CDs to automatically run when inserted in the drive: Standard Windows behavior is that when a CD-ROM is placed in the drive, its designated program runs automatically. Do you want to allow users to launch programs in this way? Any program launched in this way becomes a non-button program, so if you allow CDs to run automatically, be sure to either allow non-button programs (this is done per-desk), or list the CD's program as an Exception.

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

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

Terminate non-button programs when changing desks: Should non-button windows be closed when exiting the current desk? Also, remember to un-check this box if you have set up some of your programs to turn into non-button programs when exiting from the desk that launched them. It won't do much good to have WinU turn them into non-button windows at desk exit if you then immediately terminate them.

Hide desktop buttons for unavailable programs: If a program is not available at desk logon, should its button be displayed? You'd use this, for example, if a button launches a CD application and you want the button available for when the CD is put into the drive.

Passwords are case sensitive: Should passwords be case sensitive? This setting will affect all button passwords and the Setup password. It will also affect any desk passwords that are local to this computer. Desk passwords from a password file are not case-sensitive at any time.

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

Reset the Windows interface: If your computers use Windows 98 you may want to check this box. Windows 98 saves many settings in memory instead of re-reading them from disk as needed. Checking this box forces Windows to read the new settings instead of using the old (cached) settings.

This is usually not needed unless you have set up your WinU desks to allow the Start button or to use the Strict option (both are set on the Desk Access tab). If you don't need this, don't use it, because it takes a few seconds every time you start up, change desks, or exit.

Here is how to test to see if your computers can benefit from this setting. While not in Setup Mode, go to a desk which allows the taskbar and Start button to be used. Click on the Start button. A number of the usual items should be missing, for example Run, Find, and Logoff. (If they are still there, try to click on them -- even if these menu entries are visible they should be disabled.) Now go into Setup Mode and then click on the Start button again. Did the missing (or disabled) items come back when you entered Setup Mode? If they did not come back when you entered Setup Mode, check this box, click OK to save the settings, exit normally from WinU, restart your computer, and try the test again. If the Start menu items are now available when you enter Setup Mode, leave the box checked. Note: on some computers the tray icons may vanish when doing a reset. If this is an issue for you, don't use this feature.

Logon Validation: When WinU 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, WinU will logoff Windows. This is a useful feature if you don't have centralized network-based logon validation (through Netware, NT/2000/XP/Vista/Win7, etc) or if you prefer validation that will continue to work if your server or network goes down

If you have checked *Enhanced startup protection and Safe Mode password control*, the validation is tested immediately. If you haven't checked this box, the logon validation is tested after the desktop appears and WinU starts. There are two ways that WinU can validate this name:

With Windows: To log on, the user must give a name which is known to Windows as a valid logon name, that is, a name that has previously been set up through the Windows logon mechanism. If this is checked and the user name was set up less than 30 minutes ago, or if the user hits Escape or otherwise cancels the Windows logon process, WinU logs off Windows. In Windows 9x, all valid names are listed in the system.ini file under the [Password Lists] section. This section shows the password-list file associated with each valid logon name, so to make a name invalid remove the name's line from this section and delete its password file. This option is ignored under NT/2000/XP/Vista/Win7, which does not allow invalid logons.

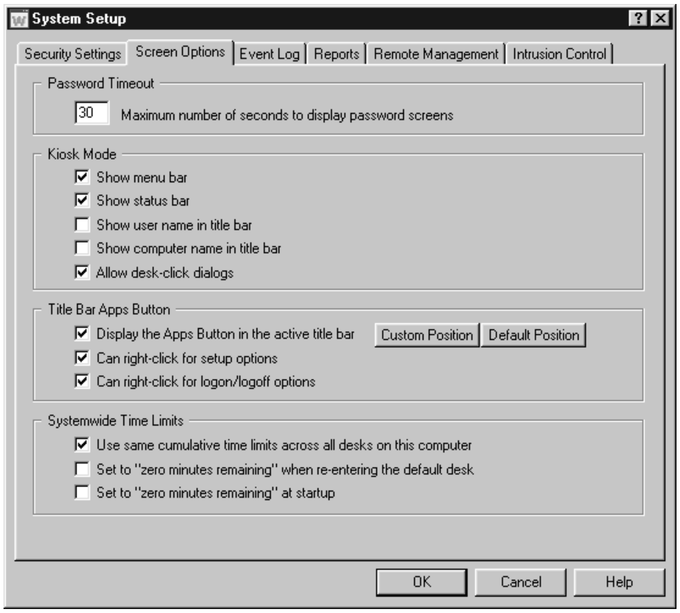
With Network Logon: If you have a network with a Netware or NT/2000/XP/Vista/Win7 server, check this box to ensure that users cannot ever get past the Windows logon unless they are validated by your server. This is especially useful on a Windows 9x computer, because on such machines even if the logon fails the network may not prevent access to the local computer. This option will work with NT/2000/XP/Vista/Win7 server validation, and many recent versions of Netware.

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

Restart After Abnormal Shutdown: By default, if WinU is shut down in a way it shouldn't (for example, turning off the computer's power switch), it goes to the last active desk at the next restart. That is, it picks up right where it left off. If you prefer, use this option so WinU goes to the default desk instead.

Shutdown Method: WinU can shut down the computer at various times, for example when the user clicks a Shutdown button. At that time, there are three ways that WinU can use to 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, WinU "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; WinU then steps back and waits for Windows to handle it all.

Screen Options Tab



Password Timeout

30 Maximum number of seconds to display password screens

Kiosk Mode

☑ Show menu bar
☑ Show status bar
☐ Show user name in title bar
☐ Show computer name in title bar
☑ Allow desk-click dialogs

Title Bar Apps Button

☑ Display the Apps Button in the active title bar
☑ Can right-click for setup options
☑ Can right-click for logon/logoff options

Systemwide Time Limits

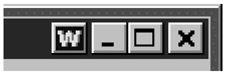
☑ Use same cumulative time limits across all desks on this computer
☐ Set to "zero minutes remaining" when re-entering the default desk
☐ Set to "zero minutes remaining" at startup

On this tab you can modify a number of options which control WinU's interface and behavior.

Password Timeout: Indicate how long you want a password screen to stay visible before it times out.

Kiosk Mode is a group of switches which control whether the menu bar and status bar are displayed, whether the user can bring up dialogs by clicking on the desktop surface, and whether the user name or computer name are shown in the title bar. The menu bar and desk-click dialog switches lets you tightly control desk-to-desk navigation. When there is no menu bar, and the user can't bring up the Choose Desk dialog by clicking on the desk surface, the only navigation elements are any DeskLink or PrevDesk buttons you have provided on the current desk. DeskLink buttons are like webpage links, they change to a specific desk. PrevDesk buttons let you go back to previously-visited desks, in reverse order. When combined with these Kiosk Mode options, DeskLink and PrevDesk buttons let you set up a distinct navigation sequence through your WinU desks. Of course if you provide no such buttons on the visible desk, the user can't go anywhere.

When these switches are used, the screen is much like a kiosk, or an ATM machine: what you see is what you get. Full use of them disables all the usual routes to the System Setup dialog, so to turn off Kiosk Mode, WinU adds a System Setup menu item to the standard System menu. (To open the System menu, click the small icon at the left edge of WinU's title bar.) Desk-click dialogs are always allowed in Setup mode, so the administrator can use this feature while configuring the system.



Title Bar Apps Button: Another access-control element you can set here is whether WinU's roving program-launch button is available. This button hops into the title bar of the current active application. The user can click it to list all programs available on the current WinU desktop. This is useful when the an application blocks the user's view of the WinU desktop buttons.

Right-clicking the button can optionally show a different menu. There are two components to this other menu, each of which can be allowed or denied with a separate checkbox. The first checkbox adds four entries: Enter Setup Mode, Exit Setup Mode, System Setup, and Desk Setup. These entries do exactly the same thing as their menu-based counterparts, and like them are password protected. The second checkbox adds two entries: Logon and Logoff. Again, these entries behave just like the WinU main menu items. If you allow access to those items, they are a handy way of navigating when the regular menu is inaccessible underneath an application window. If neither box is checked, the right-click menu is the same as the left-click menu.

Custom Position: By default the Apps Button places itself on the right side of the current window's title bar next to the standard buttons. You might prefer it elsewhere, for example if you have another program that also puts something in every active application's titlebar. When selecting a custom position, the cursor changes to the crosshairs style. Click the mouse in any app's main window. From then on, the title bar button will be displayed that distance from the right-side border in every window. If you change your mind while the crosshairs cursor is showing, press Escape to abort.

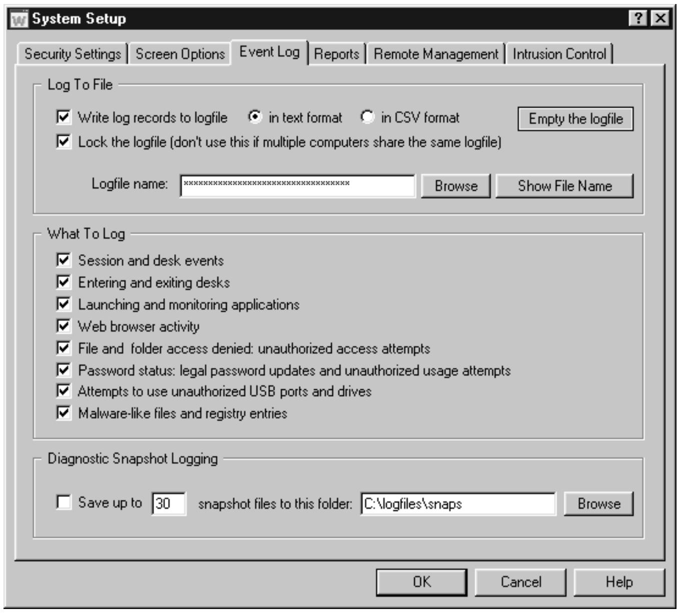
Default Position: Click this so the Apps button once again sets itself in the default title bar position on the right side next to the standard buttons.

Systemwide Time Limits: By default the cumulative time limits on each desk are entirely independent. Running out of time on one desk does not affect another desk. Sometimes, however, it's handy to have just one cumulative-time mode, and one global time limit. With this option in effect, the administrator need only set the cumulative time limits on one desk, and the settings will be carried over to all other desks. The user can switch from one desk to another, yet the time will count down uniformly. If you use cumulative time per day or per week, the maximum time is reset on all desks simultaneously whenever the time period restarts.

If you have set up to use cumulative time per logon, you can take advantage of another Systemwide Time Limits switch which tells WinU to set to "no time left" when re-entering the default desk. This can be very useful, especially in conjunction with the Remote Administration Manager program. With this switch, a patron can have full use of all desks, but immediately on return to the default desk, the time is all zeroed out. Recall that the inactivity monitor can force a logoff to the default desk, and that the administrator can remotely force any WinU computer to logoff its current desk by using the Remote Administration Manager. The Remote Administration Manager can also remotely change the current desk (or Systemwide) time limits, and logoff, shut down, or restart the computer.

The third box lets you set to "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 WinU from the outside, for example a bill acceptor or 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.

Event Log Tab



Log To File

☑ Write log records to logfile ● in text format ○ in CSV format

☑ Lock the logfile (don't use this if multiple computers share the same logfile)

Logfile name: **********************************

What To Log

☑ Session and desk events
☑ Entering and exiting desks
☑ Launching and monitoring applications
☑ Web browser activity
☑ File and folder access denied: unauthorized access attempts
☑ Password status: legal password updates and unauthorized usage attempts
☑ Attempts to use unauthorized USB ports and drives
☑ Malware-like files and registry entries

Diagnostic Snapshot Logging

☐ Save up to 30 snapshot files to this folder: C:\logfiles\snaps

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

Log To File: You can send logged events to any file on your computer or network. There are three ways to indicate the 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. By default the logfile is in the All Users\Applications Data\Bardon folder on the local computer.

<u>Lock The Logfile:</u> It's generally a good idea to lock the logfile because a locked logfile cannot be moved, changed, or deleted while WinU is running. However, don't lock the logfile if it is used by more than one computer. Different computers can share the same logfile, but in general this is not as useful as having separate logfiles for each computer. For one thing, you cannot lock the logfile if it is shared, because only one computer can access a locked logfile. For another thing, a shared logfile can provide only aggregate reports (on all your logged computers taken together), where separate logfiles can provide reports on individual computers, or they can be merged to provide aggregate reports.

<u>Per-Computer Logfile Names:</u> You can use the word %COMPUTERNAME% as part of the logfile name. If you do, WinU 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), %DESKNAME% (the current WinU desk), and %CURRTIME% (a unique number based on the current time) here. (All these are case sensitive.) For example, let's say you have named the logfile \\server\C\logs\%COMPUTERNAME%log.txt in this tab. Then let's say you clone this computer and distribute the clone setup over the network to dynamically update three computers named Moe, Larry, and Curly. Moe will then save its logfile data to \\server\C\logs\Moelog.txt, Larry will save to \\server\C\logs\Larrylog.txt, and Curly to \\server\C\logs\Curlylog.txt.

What To Log: Check the events you want logged. For basic logging, check *Start/End Session, Entering/Exiting Desks, Launching/Monitoring Applications, Password Status,* and perhaps *Web browser activity*. You only need to check the other boxes if you are using the WinU features they monitor. You can log these events:

<u>Session and desk events:</u> Each time WinU started or shut down, entered or exited Setup Mode, or encountered certain error conditions. Checking this box will also log the active (foreground) window, which logs the name, title, and time of every window the user actually worked in (including individual Web pages), so you can see where they actually spent their time.

<u>Entering and exiting desks:</u> Each time a user logged on or off a desk.

<u>Launching and monitoring applications:</u> Each time a button launched a program, each time such a program was terminated (voluntarily by the user or forcibly by WinU), and each time a World Wide Web browser accessed a webpage.

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

<u>File and folder access denied: unauthorized access attempts:</u> Check this box if you use WinU's File Control feature, or the Allowed Folders option of the Window Control feature. When using either of these features to limit file access, some programs (and users!) may still try to manipulate read-only files, write to invisible directories, etc. WinU 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: legal password updates and unauthorized usage attempts: Check this box to have WinU log each time a password was changed, and each time anyone attempted to use an invalid password.

Locked USB ports and drives: log attempts to access controlled ports and drives as set up on the USB section of the Intrusion tab.

Malware like activity: log events indicated on the Malware section of the Intrusion tab.

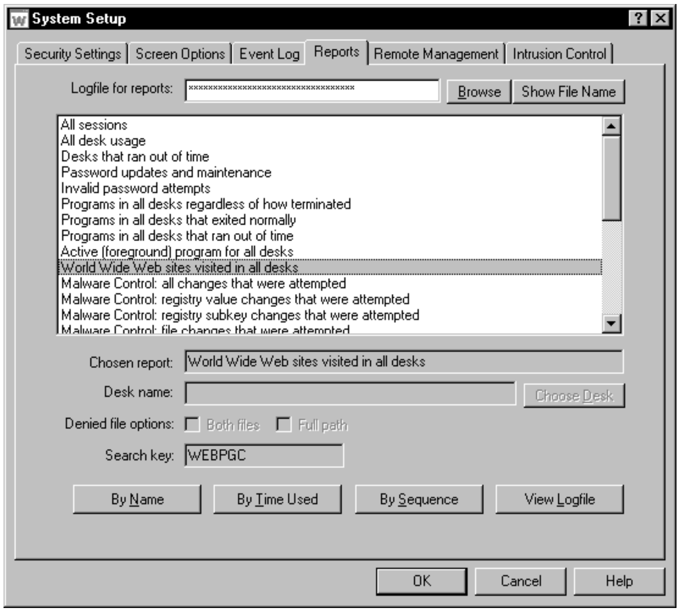
Diagnostic Snapshot Logging: WinU can take "snapshots" listing all running applications in great detail. For each running process, they show the windows opened, the primary file's date and size, the product name, version, company, copyright information, and description, the threads created, any other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

If checked, WinU 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. Snapshots are saved as plain-text files so they can be accessed even if Windows won't run.

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

Reports Tab



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

All sessions
All desk usage
Desks that ran out of time
Password updates and maintenance
Invalid password attempts
Programs in all desks regardless of how terminated
Programs in all desks that exited normally
Programs in all desks that ran out of time
Active (foreground) program for all desks
World Wide Web sites visited in all desks
Malware Control: all changes that were attempted
Malware Control: registry value changes that were attempted
Malware Control: registry subkey changes that were attempted
Malware Control: file changes that were attempted

Chosen report: World Wide Web sites visited in all desks
Desk name:
Denied file options: □ Both files □ Full path
Search key: WEBPGC

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

Choose a report, then click a button indicating how you want to view that report's data on the report output screen. For per-desk reports, indicate the desk 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, desk 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&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, WinU 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 WinU-aware program may add records to the logfile which use additional search keys. That program's documentation should have more information on those records.

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

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 differerent 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, WinU 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.

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

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

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

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

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

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

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

Logging DOS Programs: Windows runs DOS programs in a "DOS box" virtual environment. The actual running program for all DOS applications is the same. Therefore, to log meaningful information when a non-managed DOS program is running, WinU logs the titlebar text of the DOS box instead of the filename of the running program, which would otherwise be identical in every case.

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

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

<u>All sessions</u>: This report shows the ending time and amount of minutes used for all logged WinU sessions. It tracks ENDSES logfile records, which are written when the administrator exits from WinU. Since all sessions have the same

name, the *Name* button is disabled.

All desk usage: This report shows the ending time and amount of minutes used for all desk usage. It tracks CHGDSK logfile records, which are written when the user exits from a desk voluntarily, or when WinU terminates that desk for timeout reasons.

Desks that ran out of time: This report shows the ending time and amount of minutes used for desk usage where the desk ran out of time. It tracks TIMDSK logfile records, which are written when WinU forcibly terminates a desk session. This could be due to the internal cumulative time, time limits originating in the external password file, or the start of a blockout period. In all these cases the user is given an advance warning message. This report tracks instances in which this warning was ignored and the desk was forcibly terminated.

Password updates and maintenance: This report shows when button program passwords, desk passwords, and the setup password were changed. It also notes when the external password file name was changed, and shows any use of emergency passwords. It does this by tracking all CHPWD records (CHPWDP, CHPWDD, CHPWDS, CHPWDF, 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 by the user. It does this by tracking all BADPW records (BADPWA, BADPWD, BADPWE, BADPWH, BADPWI, BADPWJ, BADPWK, BADPWL, BADPWP, BADPWR, BADPWS, BADPWU, and BADPWX). Since such events take no time, the *Time Used* button is disabled.

Programs in all desks regardless of how terminated: This report shows all programs that were run in any desk, whether they were exited normally by the user or forcibly terminated by WinU. It tracks all ENDAP records (ENDAPT and ENDAPU). These show desk timeout, application timeout, and user (voluntary) exit.

Programs in all desks that exited normally: This report shows all programs, run in any desk, which were exited normally by the user. It tracks ENDAPU records, which show user (voluntary) exit.

Programs in all desks that ran out of time: This report shows all programs, run in any desk, which were forcibly terminated by WinU because the individual program ran out of time. It tracks ENDAPT records.

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

World Wide Web sites visited in all desks: 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. Note that if you check Session and desk events on the Event Log tab WinU logs information for the Active (foreground) program report. This report also includes Web Browser windows, though not with quite as much detail as the specific Web Browser Monitor report.

The "Malware Control" reports: These reports list all changes, registry value changes, registry subkey changes, or file changes. The items monitored are listed on the Malware Monitor page which is set up from the Intrusion Control tab.

Intrusion Control: locked USB port/drive access denied: This report lists locked USB port/drive access attempts, as set up on the Intrusion Control tab.

The "File Control access denied" reports: If you have given file/folder names on WinU'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 desk-by-desk 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 in all desks: by program: This report lists FILACC records generated in all desks, sorted by the program which requested the denied file.

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

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

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

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

This report is especially useful when your file-access restrictions cause a program to behave oddly. You know it needs access to a file you've restricted, but which file is it? This report will list all the files it tried to access, but couldn't. Look at the list, identify the problem file, then add it to the Allowed Folders for the restricted program on the Window Control tab.

When using this report, two filenames are involved: the name of the program which requested the file, and the name of the file requested. You can view the report sorted by either the filename of the program which requested the file, or the filename which it requested. In either case, the report's lines can include just the reported file, or both the reported file and the other file. If using just the reported file, the results will be aggregated as tightly as possible. If using both files, the additional level of detail may cause useful patterns to emerge. Additionally, you can include the full path of each listed filename, or just list the actual filename without its path. The first way is more detailed, the second easier to read.

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

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

Programs in the named desk that exited normally: This report shows all programs, run in the one named desk, which were exited normally by the user. It tracks ENDAPU records, which show user (voluntary) exit.

Programs in the named desk that ran out of time: This report shows all programs, run in the one named desk, which were forcibly terminated by WinU because the individual program ran out of time. It tracks ENDAPT records.

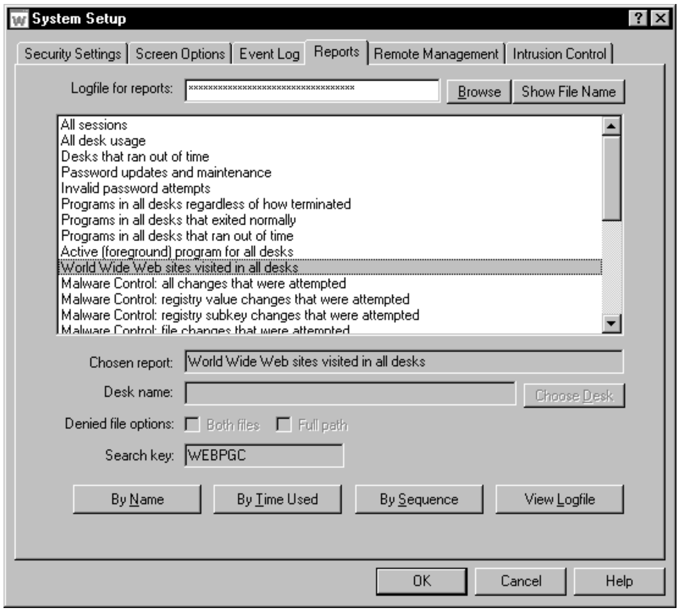
Active (foreground) program for the named desk: This report lists the active foreground program as it changed through the session. It is a good way to see exactly what windows the user accessed, in what order, and for how long. It includes the title bar text of the foreground window, so it will show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

World Wide Web sites visited in the named desk: 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. Note that if you check Session and desk events on the Event Log tab WinU logs information for the Active (foreground) program report. This report also includes Web Browser windows, though not with quite as much detail as the specific Web Browser Monitor report.

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

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

Remote Management Tab



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

All sessions
All desk usage
Desks that ran out of time
Password updates and maintenance
Invalid password attempts
Programs in all desks regardless of how terminated
Programs in all desks that exited normally
Programs in all desks that ran out of time
Active (foreground) program for all desks
World Wide Web sites visited in all desks
Malware Control: all changes that were attempted
Malware Control: registry value changes that were attempted
Malware Control: registry subkey changes that were attempted
Malware Control: file changes that were attempted

Chosen report: World Wide Web sites visited in all desks

Desk name:

Denied file options: □ Both files □ Full path

Search key: WEBPGC

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

Clone AutoUpdate: You can dynamically update the entire WinU configuration from a remote location. To use this feature, list a full-path clone data file or folder here and check the Look for clone updates box. You can drag-and-drop a file or folder onto this dialog from Explorer, and its name will appear as the AutoUpdate source. If it is a folder name, WinU will look in that directory for a clone data file named clone.bds. If it is a file name, WinU will look there for that specific file. Different managed computers can look for different files in the same folder, which can simplify AutoUpdate distribution when your computers are not identical.

A clone data file is generated by clicking the Export Clone File button. WinU looks for an AutoUpdate file at startup. If found, WinU will overwrite its current configuration with the new data.

If you are exporting a clone data file from a licensed copy of WinU, that license number will be transferred to any computer that reads this clone data file. But what if the target computer already has a license, and you want the target computer to keep its own license? To do this, export your clone file from an unlicensed copy of WinU. When you export it, you will be asked whether the target computer should keep its current license, or become unlicensed.

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

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

Export Clone File: Clicking this button sets up to create a clone data file. The file will be created when you click OK to exit from the System Setup screen. By default it is named clone.bds and is placed in the named AutoUpdate directory. Cloning is further described in How To Clone A Computer.

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

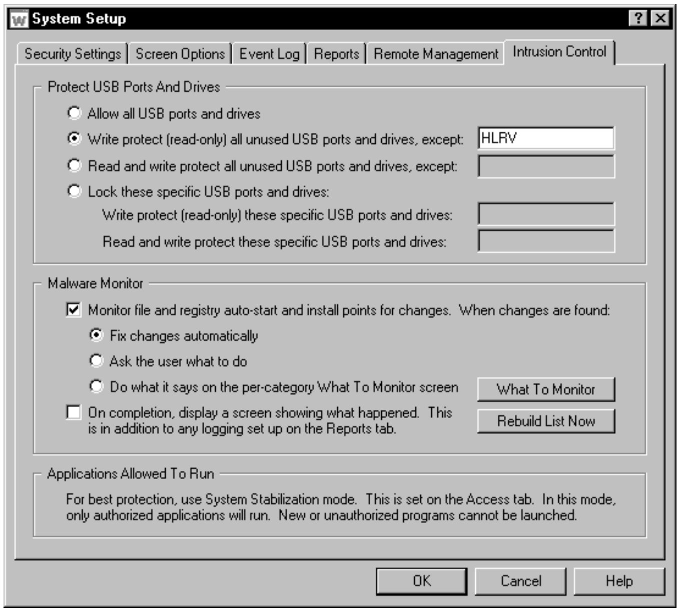
Export Plain-Text Settings File: Clicking this button sets up to create a plain-text settings file which contains listings for all the options that can be set in WinU. The file will be created when you click OK to exit from the System Setup screen. You can save this file as a record of your settings.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

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

Remote Administration Messages: If you like, you can pre-designate a directory here for messages from the Remote Administration Manager. However, it's rarely necessary to do so, because the Administration Manager broadcasts over the network the location of the Message Directory it wants to use. Virtually the only time it's necessary to pre-designate this location is when the WinU computer is in a different NT/2000/XP/Vista/Win7 domain than the computer running the Administration Manager program.

This folder must be able to handle long filenames because Remote Administration filenames can exceed the now-defunct DOS 8.3 filename format. If you are not using TCP/IP messaging (set from the Administration Manager) then all computers must have read/write access to this folder. If you are using TCP/IP messaging then the Administration Manager needs read/write access but the other computers just need read-only access to this folder.

Intrusion Control Tab



Protect USB Ports And Drives

○ Allow all USB ports and drives
● Write protect (read-only) all unused USB ports and drives, except: HLRV
○ Read and write protect all unused USB ports and drives, except:
○ Lock these specific USB ports and drives:
Write protect (read-only) these specific USB ports and drives:
Read and write protect these specific USB ports and drives:

Malware Monitor

☑ Monitor file and registry auto-start and install points for changes. When changes are found:
● Fix changes automatically
○ Ask the user what to do
○ Do what it says on the per-category What To Monitor screen
☐ On completion, display a screen showing what happened. This is in addition to any logging set up on the Reports tab.

Applications Allowed To Run

For best protection, use System Stabilization mode. This is set on the Access tab. In this mode, only authorized applications will run. New or unauthorized programs cannot be launched.

The Intrusion Control tab includes mechanisms to handle malware, spyware, trojans, data theft, and similar threats. There are two sections to this tab.

At the bottom of this tab there is also a reminder that for best protection, use the Applications Allowed To Run option on the Access tab. This prevents unauthorized programs from running. Use the Strict option there for the best protection.

Protect USB Ports And Drives

This section is fairly straightforward. With these settings, you can lock USB ports (and actually, any other local drives such as CD or DVD writers). The drives can be set as read-only or completely invisible and unusable. This can go a long way to preventing data theft. It can be set to scan at startup and lock all unused drives, or it can lock the specific list of drives you provide. "Lock" can mean read-only or read-write protection, as you prefer.

Logging: Incidents will be logged if you have turned on USB Ports And Drives logging on the Event Log tab.

Malware Monitor

Malware is anything you (the administrator) don't want run automatically. In Windows, programs can be auto-launched at startup, or 'piggyback' when a legitimate program is launched by the user. Check the box to monitor file and registry auto-start and install points for changes that do this. There are three options here:

- When changes are found, fix them automatically. This is the preferred option. The settings in place at startup will be restored automatically.

- Ask the user what to do. However most users will not know what to do, so this option is not preferred.

- A third option allows detailed customization, to do what you list on the What To Monitor screen for each type of incident. There are 18 types of incidents, and each type can have different options.

Logging: Incidents will be logged if you have turned on Malware logging on the Event Log tab.

Rebuild List Now: The button to Rebuild List Now will only be needed rarely, typically when you enter Setup Mode and change a monitored file or registry setting. It will re-scan all settings and rebuild the list of allowed files and registry settings, thus including your new change.

What To Monitor: This button brings up the What To Monitor screen, where you can customize how each type of incident is handled. Here, you can customize how each type of incident is handled. The options on the What To Monitor screen for each incident type are:

Log: Monitor for this type of incident and if found, log it (if you have checked the box to turn on Malware logging on the Event Log tab). This option must be checked to use any other option.

Ask: Ask the user what to do for this type of incident. However most users will not know what to do, so this option is not advised.

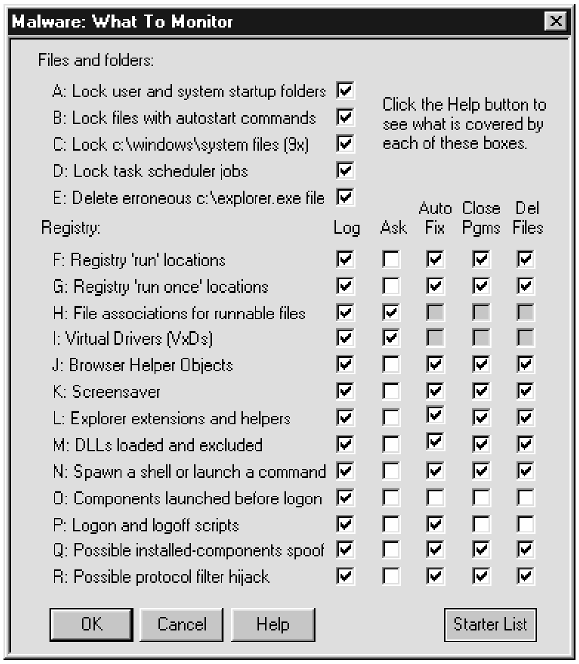
Auto Fix: Automatically fix the problem. For registry incidents this means the registry listing is put back as it was when our app began monitoring.

Close Pgms: This looks at the unauthorized entry which was added to the registry. It sees if a file by that name is running, and attempts to close that program.

Del Files: This also looks at the unauthorized entry which was added to the registry. It tries to delete the unauthorized filed found in that registry location.

Some of these options will gray-out and be unavailable unless other options are chosen. Their relationship ought to be fairly clear.

Here is a detailed list of monitored files and registry keys, by category, as listed on the What To Monitor screen. The response for each category can be customized.



Files and folders:

- A: Lock user and system startup folders ☑
- B: Lock files with autostart commands ☑
- C: Lock c:\windows\system files (9x) ☑
- D: Lock task scheduler jobs ☑
- E: Delete erroneous c:\explorer.exe file ☑

Click the Help button to see what is covered by each of these boxes.

Registry:	Log	Ask	Auto Fix	Close Pgms	Del Files
F: Registry 'run' locations	☑	□	☑	☑	☑
G: Registry 'run once' locations	☑	□	☑	☑	☑
H: File associations for runnable files	☑	☑	□	□	□
I: Virtual Drivers (VxDs)	☑	☑	□	□	□
J: Browser Helper Objects	☑	□	☑	☑	☑
K: Screensaver	☑	□	☑	☑	☑
L: Explorer extensions and helpers	☑	□	☑	☑	☑
M: DLLs loaded and excluded	☑	□	☑	☑	☑
N: Spawn a shell or launch a command	☑	□	☑	☑	☑
O: Components launched before logon	☑	□	□	□	□
P: Logon and logoff scripts	☑	□	☑	□	□
Q: Possible installed-components spoof	☑	□	☑	☑	☑
R: Possible protocol filter hijack	☑	□	☑	☑	☑

Files And Folders

A: *Lock user and system startup folders*

We ensure that unauthorized entries can't be added. These are what generate the Start button 'run at startup' entries. The locations vary by computer but typically the files that generate these are in:

C:\Documents and Settings\<user>\Start Menu\Programs\Startup
C:\Documents and Settings\All Users\Start Menu\Programs\Startup

... and in any similar per-user nonlocalized Startup program group and all-users nonlocalized Startup program group.

B: *Lock files with autostart commands*

These are files where programs can be listed to run in various ways at startup. In NT/2K/XP these are config.nt, autoexec.nt, and autoexnt.bat in the Windows\System folder. In 9x they are dosstart.bat, winstart.bat and wininit.ini in the root folder, and autoexec.bat and config.sys in the Windows folder.

C: *Lock c:\windows\system components (9x)*

These are 9x locations that could potentially be hijacked. Includes all files in Windows\system\iosubsys and Windows\system\vmm32.

D: *Lock task scheduler jobs*

Task scheduler launches programs listed in files saved in Windows\tasks folder. We lock this folder so unauthorized tasks can't be added.

E: *Delete erroneous c:\explorer.exe file*

The explorer shell program should never be found in the root of the boot drive. Unfortunately due to a bug in some versions of Windows, if a file named explorer.exe is found there, it supercedes the real explorer.exe, and some malware does exploit this vulnerability. For this reason we delete c:\explorer.exe (in root of C drive).

Registry Entries

F: *Registry 'run' locations*

Places in the registry where listed programs are run at every startup:

HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows [values: load, run]
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices [all values]
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run [all values]
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run [all values]
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run [all values]
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run [all values]

G: *Registry 'run once' locations*

Places in the registry where listed programs are run at the next startup:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce [all values]
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce [all values]
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce [all values]
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnceEx [all values]
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce\Setup [all values]

H: *File associations for runnable files*

Places where registry entries can be subverted to run unauthorized programs:

HKEY_CLASSES_ROOT\exefile\shell\open\command [value: "" (the default value)]
HKEY_CLASSES_ROOT\comfile\shell\open\command [value: "" (the default value)]
HKEY_CLASSES_ROOT\batfile\shell\open\command [value: "" (the default value)]
HKEY_CLASSES_ROOT\piffile\shell\open\command [value: "" (the default value)]
HKEY_CLASSES_ROOT\scrfile\shell\open\command [value: "" (the default value)]
HKEY_CLASSES_ROOT\htafile\Shell\Open\Command [value: "" (the default value)]
HKEY_CLASSES_ROOT\vbsfile\shell\open\command [value: "" (the default value)]

HKEY_CLASSES_ROOT\vbefile\shell\open\command [value: "" (the default value)]
HKEY_CLASSES_ROOT\jsfile\shell\open\command [value: "" (the default value)]
HKEY_CLASSES_ROOT\jsefile\shell\open\command [value: "" (the default value)]
HKEY_CLASSES_ROOT\wshfile\shell\open\command [value: "" (the default value)]
HKEY_CLASSES_ROOT\wsffile\shell\open\command [value: "" (the default value)]
HKEY_CLASSES_ROOT\txtfile\shell\open\command [value: "" (the default value)]
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts [all subkeys and values]

I: *Virtual drivers (VxDs)*

Virtual drivers can be set to run at startup so we make sure no new ones are added:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\VxD [all subkeys and values]

J: *Browser Helper Objects*

In the Microsoft Internet Explorer browser, a BHO is launched whenever the browser runs. Of course in many versions of Windows there is little difference between IE and the Windows file manager (Explorer). Sadly, this provides a very neat way of hijacking, not only a browser, but the entire computer, so we monitor this location for any unauthorized changes:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Browser Helper Objects [all subkeys and values]

K: *Screensaver*

A screensaver is of course a program. If it is changed, the other program might not do what you'd expect so we monitor:

HKEY_CURRENT_USER\Control Panel\Desktop [value: SCRNSAVE.EXE]

L: *Explorer extensions and helpers*

Various items that can be set to automatically run when Explorer or MSIE runs:

HKEY_CLASSES_ROOT\Folder [all subkeys and values]

M: *DLLs loaded and excluded*

These are DLLs that are loaded into every process when it is launched. Malware listed here will run in tandem with every program.

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Windows [value: AppInit_DLLs]
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\MPRServices [all subkeys and values] (note: this is in 9x only)

N: *Spawn a shell or launch a command*

These are locations that Windows looks at when a command shell is launched, or a command is run through an existing shell:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\WOW [values: cmdline, wowcmdline]
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor [value: AutoRun]
HKEY_CURRENT_USER\Software\Microsoft\Command Processor [value: AutoRun]
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify [all subkeys and values]
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ShellExecuteHooks [all values]
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options [all subkeys and values]

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Accessibility\Utility Manager [all subkeys and values]
HKEY_CLASSES_ROOT\Drive [all subkeys and values]

O: *Components launched before logon*

These places list programs to be run before the user logs in. You don't want malware to add itself here! This is one reason why you should always run the Bardon management application whenever any user is logged in:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon [values: shell, Userinit, GinaDLL, System, VmApplet]
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SessionManager [value: BootExecute]
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad [all values]
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskScheduler [all values]
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\\SafeBoot\Option [value: UseAlternateShell]

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\\SafeBoot [value: AlternateShell]
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager [values: BootExecute, PendingFileRenameOperations, ExcludeFromKnownDlls]

P: *Logon and logoff scripts*

Scripts run commands, so we monitor locations that can auto-launch scripts:

HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\System\Scripts [all subkeys and values]
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System\Scripts [all subkeys and values]

Q: *Possible installed-components spoof*

Some locations where malware can mimic legitimate components. When those components are called, the malware might be launched:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Winsock2 [all subkeys and values]
HKEY_LOCAL_MACHINE\Software\Microsoft\Code Store Database\Distribution Units [all subkeys and values]
HKEY_LOCAL_MACHINE\Software\Microsoft\Active Setup\Installed Components [all subkeys and values]

R: *Possible protocol filter hijack*

This is a registry location where malware could register a permanent filter that can be set up to launch programs automatically so we monitor for additions or changes to this list:

HKEY_CLASSES_ROOT\Protocols\Filter [all subkeys and values]

Desk Setup Dialog

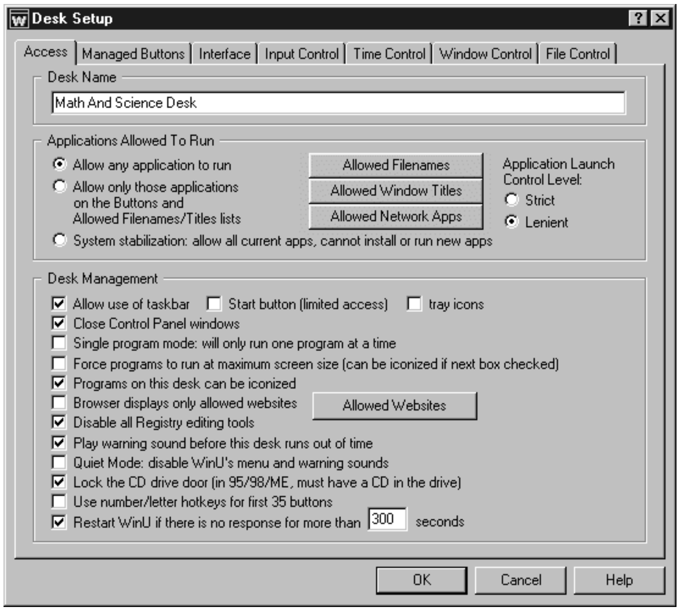
To set up options for the current desk, use the Desk Setup tabbed dialog. You can launch this dialog from the Setup menu, or by right-clicking anywhere on the desktop (if desk-click dialogs haven't been disabled via Kiosk Mode), through the roving Apps Button, or through the System menu. (To open the System menu, click the small icon at the left edge of WinU's title bar.)

The Desk Setup dialog has seven tabs:

Access: desk name, password, and program-management options
Managed Buttons: including program and special-function buttons
Interface: wallpaper, button, sound, and color options
Input Control: keyboard, mouse, and inactivity monitoring
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

These are described below. For information on modifying desktop buttons, also see Adding Or Changing Programs.

Desk Access Tab



Desk Name: Math And Science Desk

Applications Allowed To Run

- ● Allow any application to run
- ○ Allow only those applications on the Buttons and Allowed Filenames/Titles lists
- ○ System stabilization: allow all current apps, cannot install or run new apps

Application Launch Control Level:

- ○ Strict
- ● Lenient

Desk Management

- ☑ Allow use of taskbar ☐ Start button (limited access) ☐ tray icons
- ☑ Close Control Panel windows
- ☐ Single program mode: will only run one program at a time
- ☐ Force programs to run at maximum screen size (can be iconized if next box checked)
- ☑ Programs on this desk can be iconized
- ☐ Browser displays only allowed websites
- ☑ Disable all Registry editing tools
- ☑ Play warning sound before this desk runs out of time
- ☐ Quiet Mode: disable WinU's menu and warning sounds
- ☑ Lock the CD drive door (in 95/98/ME, must have a CD in the drive)
- ☐ Use number/letter hotkeys for first 35 buttons
- ☑ Restart WinU if there is no response for more than 300 seconds

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

Desk Name: This is the name by which the desk is identified. It is also used in the logfile and external password file, if used. Though WinU allows it to be identical to another desk's name, this is probably not a good idea. You can rename the desk at any time.

Applications Allowed To Run: Some programs can be launched, not by WinU from a button, but by other programs. For example, let's say users can run Explorer from a button. Should they be allowed to use Explorer to launch programs? Indicate here how you want such non-button programs to be treated.

• If you *Allow any application to run* there are no restrictions on non-button programs. They are allowed to run, and no time limits are enforced against them.

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

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

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

Strict: This is the tightest possible control. The only programs that can be run while in this desk are WinU managed-button programs and those listed under *Allowed Filenames* or *Allowed Network Apps*. WinU sets certain low-level Windows options when entering this desk, and clears them when WinU exits the desk.

Abnormal-exit in Strict mode: If for any reason WinU exits abnormally, the Strict low-level "don't run" settings will still be in place, and almost nothing on your computer will run. If it happens, WinU provides a number of recovery options, which are listed here in the recommended order.

• First, try to run WinU again; you can exit immediately if you like, because when WinU exits normally it will clear any leftover control settings.

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

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

Lenient: This option isn't as strong as the Strict method, but it does not create any low-level restrictions. Instead, WinU itself looks at all new top-level windows. A window owned by another window is ignored (for example a Save As dialog). If the window's title doesn't match any 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. WinU will also allow any window from a program on the *Allowed Filenames* list. If you use the System Stabilization option all programs run from UNC network shared folders are allowed.

Other considerations: If you are using the Strict option, and you set up a button on the Advanced screen to launch immediately as a non-button program, you should list that program as an exception so it is not immediately terminated. List such a program exception by window title or by filename. Different programs will work better with one or the other listing methods. You may want to put a program on both lists. It is generally just fine to list an exception by both its filename and its window title.

Have you checked the box on the Security Settings tab of the System Setup screen which hides programs started before WinU? As a convenient way to allow access to such a program, list its window title or filename as an exception. The user will then be able to Alt+Tab to such a program, or view popup windows from it, without having WinU immediately hide that program. To get you started, a few popular antivirus and similar tools have been pre-entered on this list.

Desk Management: These settings let you customize the way in which WinU runs programs.

Allow use of Taskbar / allow Start button / allow tray icons: With these boxes you can allow this desk's users to access the standard Windows taskbar, Start button (in a limited way), or tray and Quick Launch icons. If the taskbar is not allowed, neither the taskbar nor any of its components are visible or accessible. (If you allow the taskbar, don't set its Properties to use AutoHide, because this will force both WinU and the taskbar to constantly resize itself.) If you allow the taskbar, you can also allow the Start button and/or tray and Quick Launch icons. If the Start button is not allowed, clicking on the Start button does nothing. Similarly, if the tray and Quick Launch icons are not allowed, clicking on one of them has no effect. If allowed, Start button access is limited; if the Start button is allowed, certain items are removed (Run, Find, Logoff, Shut Down, Windows Update, Folder Options, Favorites, and Taskbar Settings), and the Recent Documents list is cleared at desk logon. Tray icons are next to the clock on the Taskbar; Quick Launch icons are next to the Start button.

Close Control Panel Windows: Control Panel's system settings are usually not appropriate for WinU users, so you will probably want WinU to close Control Panel and its individual applets. To allow access to Control Panel, un-check this box. Of course, you will then want to create a WinU button for Control Panel or whichever individual applets you will allow. Remember to set up Window Controls to close any applets you do not want to allow.

Single program mode: If checked, when the user clicks a button to launch a program, any other currently-running button program (which was launched by WinU) will be forcibly terminated.

Maximum screen size: Check this box to ask button 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, assuming you've allowed this. Of course, when running a program fullscreen, WinU's main screen is not visible. In this case you may want to let patrons use WinU's roving Apps Button to get around.

Can be iconized: Check this box to allow WinU-launched programs to be minimized. A minimized program has no visible window or icon, but you can tell that a program is still running because its button is yellow. To bring back a running, minimized program, click its yellow button again. Or you can use the Apps Button menu to bring it back, or just Alt+Tab to that program in the usual Windows way.

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

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

Disable all Registry editing tools: With this box checked, the user cannot run regedit.exe, regedt32.exe, and similar registry editing tools. It is only really necessary if non-button programs are allowed, because it's unlikely that you're putting a registry editing tool on a user button!

Warning sound: Do you want WinU to play a warning sound before this desk runs out of time? The sound is played at the same time the desk-time warning screen pops up. Choose any WAV sound as the warning (on the Interface tab) or let WinU use its built-in default sound. If no program is running at the warning time, no warning sound is played.

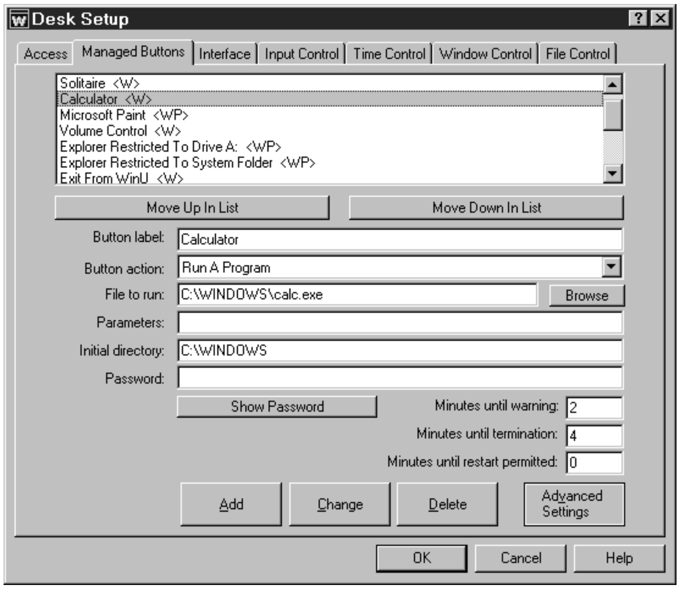
Quiet Mode: Check this box to disable the "click" menu and button sound, and all other sounds generated by WinU.

Lock CD drive door: Check this box to help prevent valuable CDs from walking away from the computer while on this WinU desktop. In Windows 9x if you enter this desk with no CD in the drive, the door will remain unlocked until a CD is put into the drive.

Number/letter hotkeys: Checking this box allows the user to launch the first 35 programs by pressing a single key on the keyboard. WinU will automatically add numbers and letters to your button text for each of the buttons that can be controlled in this way.

Restart WinU if no response: WinU includes components that make sure in various ways that the program continues to run normally. One of these components can provide "program is hung" protection. If you check this box, this component listens for messages from WinU to ensure that everything is still running normally. If you want to use this component, indicate here how many seconds it should wait before concluding that WinU is not responding. We recommend setting this to at least 180 seconds to allow for certain kinds of applications which occasionally monopolize the computer briefly. While the computer is monopolized in this way, WinU can't send these "I'm OK" messages, so be sure the time is long enough to bridge any such periods.

Managed Buttons Tab



Solitaire <W>
Calculator <W>
Microsoft Paint <WP>
Volume Control <W>
Explorer Restricted To Drive A: <WP>
Explorer Restricted To System Folder <WP>
Exit From WinU <W>

Button label: Calculator
Button action: Run A Program
File to run: C:\WINDOWS\calc.exe
Parameters:
Initial directory: C:\WINDOWS
Password:
Minutes until warning: 2
Minutes until termination: 4
Minutes until restart permitted: 0

WinU's simplified replacement user interface consists of buttons on a desktop. These are referred to as Managed Buttons. They can run programs, switch to another desk, exit from WinU, shut down the computer, and more (see below). This tab lets you create, change, delete, or copy buttons. You can also give restrictions to control on which computers this button is displayed.

The *button action* defines what this button can do, for example run a program, link to another desk, or perform a special action such as launching the current screensaver. For Program or DeskLink buttons, adding a button requires just two pieces of information: the button's label, and the filename (or deskname). Give these, then click Add and you're done. Most of the special-action buttons such as PrevDesk, Exit and Shutdown buttons (see below) are even easier, since they require only a button label. The button label is used for logging and internal tracking, so it must be given even if you have set up this desk so its buttons display only the program icon with no label.

There are a wide range of ways to customize the appearance and behavior of buttons. See Adding Or Changing Buttons for more on this. Further customization options are described under Display Restrictions and Advanced Program Button Settings.

Button Action: You can create many kinds of buttons. The button action is chosen from a dropdown list. Each type is described below:

<u>Run A Program:</u> A button which launches a program, file, or Shortcut. The minimum setup here is to give the button text and the program / Shortcut / file to run (WinU will find the correct program for a Shortcut or a file having a registered file extension). There are three ways to indicate the program filename to use. You can type in its name, use the Browse button, or "drag and drop" any file from Explorer onto this dialog.

<u>DeskLink:</u> A DeskLink button switches to another desk when clicked. When you choose DeskLink from the list, the *File To Run* label changes to *Switch Desk*. Enter the name of the target desk, or use the *Choose* (changed from *Browse*) button to select the target desk to which this button should go when clicked. Some options will become disabled to indicate that they don't apply to DeskLink buttons.

<u>Exit WinU:</u> A button which exits from WinU when clicked. Exiting from WinU returns to the usual Windows interface. Some options will become disabled to indicate that they don't apply to Exit buttons. The Setup password is not required when exiting from WinU with an Exit button. If you want password protection for this function, give the button its own password in the usual way.

<u>Shut Down Computer:</u> A button which shuts down the computer when clicked, using the shutdown method selected on the Security Settings tab of the System Setup dialog. Some options will become disabled to indicate that they don't apply to Shutdown buttons. The Setup password is not required when shutting down the computer with a Shutdown button, so if you want password protection for this function, give the button its own password in the usual way.

<u>PrevDesk:</u> A PrevDesk button takes you to the desk you were on before this one. The last 100 visited desks are saved, so you can back out in exactly the order that got you to a particular desk in the first place. Some options will become disabled to indicate that they don't apply to PrevDesk buttons.

<u>Logoff Computer</u>: A button which closes WinU and logs off the current Windows session. Some options will become disabled to indicate that they don't apply to Logoff buttons. The Setup password is not required when using a Logoff button, so if you want password protection for this function, give the button its own password in the usual way.

<u>Restart Computer</u>: Sometimes you might want to shut down and immediately restart your computer, all in one step. The Restart button does just that, and it works with WinU so the shutdown and restart stay in sync with WinU's security

protection. It uses the shutdown method selected on the Security Settings tab of the System Setup dialog. Some options will become disabled to indicate that they don't apply to Restart buttons. The Setup password is not required when shutting down the computer with a Restart button. If you want password protection for this function, give the button its own password in the usual way.

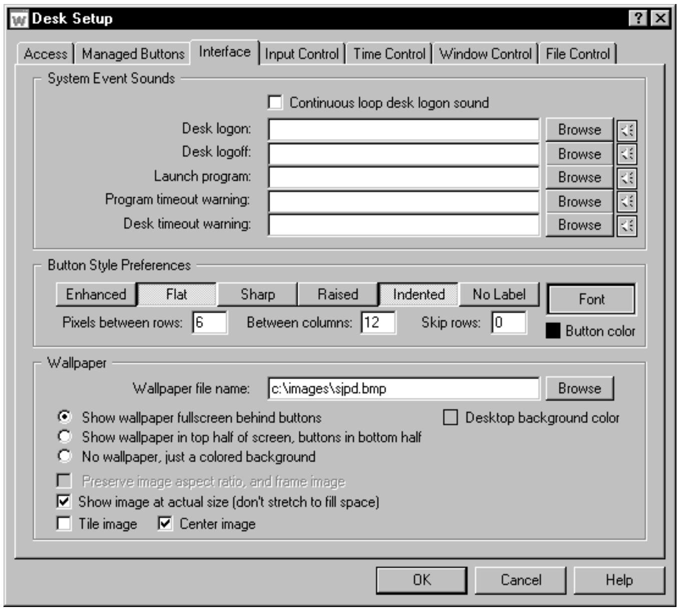
Diagnostic Snapshot: The user can click on this button to generate and display a Diagnostic Snapshot. This can be a very useful tool for remote troubleshooting.

Run Screensaver: A button which launches the currently-set screensaver when clicked. Some options will become disabled to indicate that they don't apply to Screensaver buttons.

Close Dial-Up Networking: A button which shuts down any and all open Dial-Up Networking connections. Some options will become disabled to indicate that they don't apply to Close DUN buttons.

Spacer/AutoRun Button: This special button is an invisible button that takes up a space on the screen. In addition to providing a blank space as a layout tool when setting up your desk's display, it can also provide a way to AutoRun a program at desk logon without having a visible button on the desk. If using this as a simple Spacer button you only need to provide a button label.   If using this to AutoRun a program you must provide the same information as is required of a regular Program button (see above). Hint: if you want to use this as an AutoRun button but don't want it taking up an obvious space, put it at the end of the list for this desk. Nobody will know it's there.

Interface Tab



System Event Sounds

☐ Continuous loop desk logon sound

Desk logon:

Desk logoff:

Launch program:

Program timeout warning:

Desk timeout warning:

Button Style Preferences

Pixels between rows: 6 Between columns: 12 Skip rows: 0

■ Button color

Wallpaper

Wallpaper file name: c:\images\sjpd.bmp

● Show wallpaper fullscreen behind buttons

○ Show wallpaper in top half of screen, buttons in bottom half

○ No wallpaper, just a colored background

☐ Desktop background color

☐ Preserve image aspect ratio, and frame image

☑ Show image at actual size (don't stretch to fill space)

☐ Tile image ☑ Center image

This tab is used to customize the desk's audio and visual interface.

System Event Sounds: If you haven't checked the Quiet Mode box on the Access tab, WinU will play the sound (.wav) files you list here when entering a desk, leaving a desk, launching a program, or when the desk or a program is almost out of time. For each event, you can type the soundfile name or use the Browse button to select a soundfile. The yellow "speaker" buttons let you preview the chosen sound. If sounds are enabled but no file is specified for an event, WinU uses its built-in sound for that event.

The Desk Logon sound can be made to *loop*, that is, to play continuously. A looping sound will be repeated while no program is running from this desk.

Note: WinU can also associate sounds with an individual button (set on the Buttons tab). If there is both a individual-button Launch Program sound and a desk-level Launch Program sound, or an individual-button Program Timeout Warning sound and a desk-level Program Timeout Warning sound, the button sound is played, not the desk sound.

Button Style Preferences: You can choose the font and color to be used for the button text by clicking on the Font button, and you can choose the button background color by clicking the "button color" box. When choosing a button background color, remember that WinU uses button color to show when certain events happen. WinU's colors are white (button has the focus), yellow (program is running), light yellow (focus button's program is running), and red (wait, program is launching). Preferably, don't use those colors for your customized button background.

The appearance of a desk's buttons can also be customized by choosing one or more of the six listed border-style attributes. Different combinations of attributes generate different-looking buttons. The first five include all available Windows button border style attributes. Though they can all be manipulated, some have a more noticable effect than others. The sixth button-style attribute determines whether label text is displayed for buttons on this desk. If no label text is displayed, the buttons on this desk are just icons in a border. As you change the button-style options, the Font button is modified to show that style.

By default, the buttons are displayed starting at the top of the available space. If you'd like to leave empty rows, and start the buttons lower down, indicate here how many rows to skip. You can also control the amount of space between buttons, both horizontally and vertically. The default spacing is 6 pixels between rows and 12 between columns. Remember, too, that you can create spaces between buttons, or empty rows between groups of buttons, by including Spacer buttons on this desk. Like all buttons, these are set on the Managed Buttons tab.

Wallpaper: WinU has its own "built-in" wallpaper, or you can set this desk to display any other Windows bitmap as the background image by giving its file name here. You can type in the bitmap filename, or use the Browse button, or "drag and drop" the image file from Explorer onto this dialog. It will appear as the bitmap file name. If you leave this blank, WinU's built-in background image will be used.

Fullscreen / top half: Whether you use an external bitmap image or WinU's built-in wallpaper, the picture can be displayed fullscreen behind this desk's buttons, or unobstructed in the top half of the WinU screen.

No wallpaper: If you prefer, you can display no wallpaper at all, just a plain colored background.

Desktop background color: To choose the background color, click the color box. This color box also controls the color of the bottom half of the screen if you use the setting to "Show wallpaper in top half of the screen, buttons in bottom half."

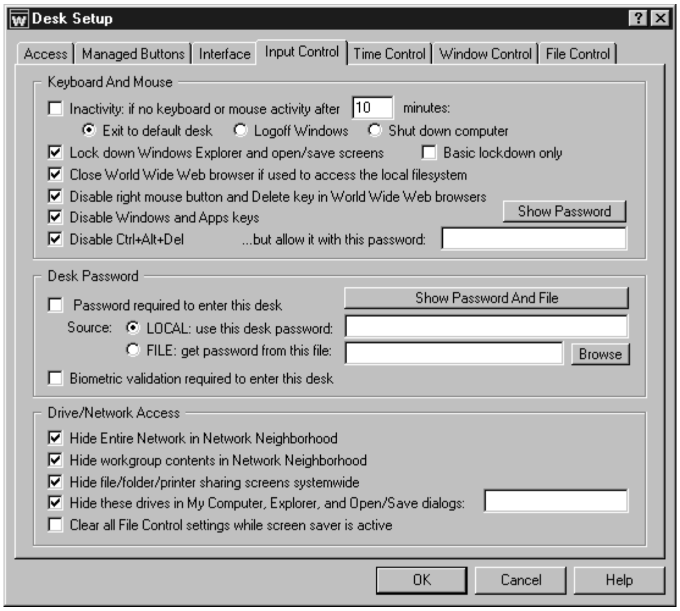
Aspect ratio: There's a box to check if you don't want the bitmap's aspect ratio changed. If checked, the background image will be displayed as large as it can go while still keeping the proportions of the original. A frame will be drawn around the image.

Actual size: You can display an external bitmap at its actual size (not stretched to fit the available space). This is a good way to display text or other finely detailed images. If using this option, it's best to choose a bitmap bigger than the space it needs to cover in your chosen screen resolution; any excess will be truncated. If it is smaller than the space, and you aren't tiling the image, the excess space will be filled with your chosen desktop background color.

Tile image: This will copy the bitmap as many times as required to fill the space. Tiled images must be displayed at their actual size.

Center image: This will display the image once, centered in the space. Centered images must be displayed at their actual size.

Input Control Tab



Keyboard And Mouse

☐ Inactivity: if no keyboard or mouse activity after 10 minutes:

● Exit to default desk ○ Logoff Windows ○ Shut down computer

☑ Lock down Windows Explorer and open/save screens ☐ Basic lockdown only

☑ Close World Wide Web browser if used to access the local filesystem

☑ Disable right mouse button and Delete key in World Wide Web browsers

☑ Disable Windows and Apps keys

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

Desk Password

☐ Password required to enter this desk

Source: ● LOCAL: use this desk password:

○ FILE: get password from this file:

☐ Biometric validation required to enter this desk

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:

☐ Clear all File Control settings while screen saver is active

Use these options to indicate how WinU should treat certain kinds of user input.

Keyboard And Mouse: WinU 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. WinU can also prevent the use of Explorer features such as Find File, Find Folder, Find Computer, Map Network Drive, and Go To. In addition, WinU can disable the right mouse button and Delete key in Netscape, Mozilla, or Internet Explorer. All these features can provide "back door" access methods to your computer.

Inactivity: if no keyboard or mouse activity: WinU can test for periods of inactivity, like a screensaver. If there has been no activity for a specified time, it can logoff, shut down, or exit from the current desk. If you choose to exit it will switch to the current systemwide or per-user default desk if one has been specified, or to the "No Desk" startup screen otherwise.

Lock down Windows Explorer, the desktop, and open/save screens: If checked, WinU will disable Delete and Cut from Explorer's menu or toolbar, or from the keyboard. It will also look for certain Explorer-related window titles and cancel them when found, so as to disable their function (Confirm File Delete, Confirm Folder Delete, Folder Options, Internet Options, Customize, Run Application, Confirm Multiple File Delete, Find, Map Network Drive, Go To Folder and Create Shortcut, however if there is a Window Control for any of these, the Window Control takes precedence). It will also disable right-mouse-button context menus which, if uncontrolled, can allow the user to run applications, delete and rename files, etc. In NT/2000/XP/Vista/Win7, checking this box will also close the Task Manager. Disabling these makes Explorer safer. This also prevents using the Delete key and right mouse button in standard Windows Open/Save dialogs and most Microsoft Office applications.

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

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

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

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 features like the Close Programs box. If no password is listed, pressing Ctrl+Alt+Del has no effect at all.

Desk Password: The desk password can come from this local setup, in which case it is supplied here. Or it can come from an external password file, perhaps on a server where the same file can be accessed by many WinU computers simultaneously. This file can be centrally managed by WinU's Password Manager program.

The password or filename can be blank if no password is required to access this desk. It is perfectly okay to have a desk which does not require a password.

Biometric validation required: WinU supports Identix biometric fingerprint validation. If this box is checked, an enrolled fingerprint must be provided to log on to this desk. If Identix fingerprint validation is not installed, checking this box has no effect.

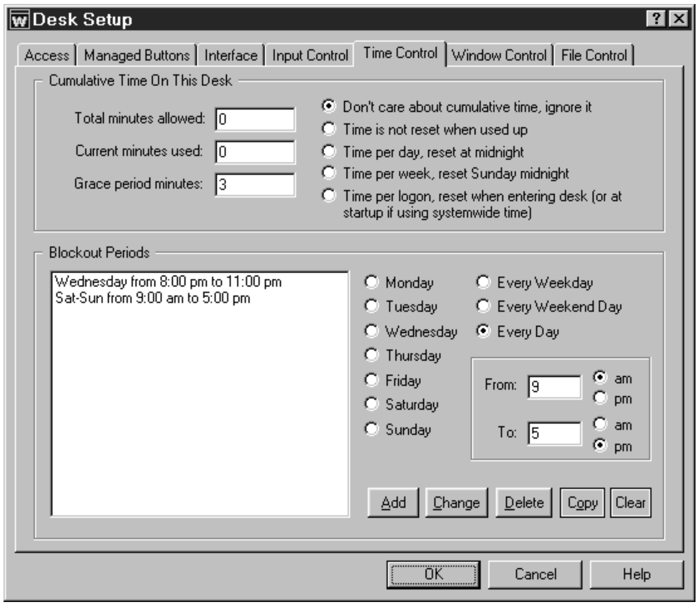
Drive/Network Access: Windows Open and Save screens act like little Explorer windows. They can provide access to My Computer, Network Neighborhood, and more. To control this, use these options to hide local drives or network access folders in the dropdown lists of Open and Save screens, and in Explorer.

Check the first box to hide the Entire Network icon in Explorer and the Open/Save screen's Network Neighborhood; check the second box to hide workgroup members in Explorer and in the Open/Save screen's 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. It's like an unlisted phone -- the number isn't in the book, but it will still ring if you call it. This is a fairly good way to remove obvious sources of temptation, and sometimes that's all you need. However, even if (for example) the C drive is controlled through this option, a user can still save a file to c:\somedir\myfile.txt by simply typing the full path into the Save dialog. And if Explorer is explicitly told to open on to a hidden drive, that drive will be displayed. For a much stronger "invisible files" mechanism, consider the File Control feature of WinU, which makes files and folders so totally invisible that not even Windows itself can see them. You can give systemwide restrictions on the File Control tab, or per-program file control restrictions from the Advanced screen of the Managed Programs tab.

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

Time Control Tab


Desk Setup
Access | Managed Buttons | Interface | Input Control | Time Control | Window Control | File Control
Add
Change
Delete
Copy
Clear
OK
Cancel
Help

Cumulative Time On This Desk

Total minutes allowed: 0
Current minutes used: 0
Grace period minutes: 3

● 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 (or at startup if using systemwide time)

Blockout Periods

Wednesday from 8:00 pm to 11:00 pm
Sat-Sun from 9:00 am to 5:00 pm

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

From: 9 ● am ○ pm
To: 5 ○ am ● pm

This controls times during which programs are allowed to run.

Cumulative Time: In addition to each program's individual time limit, the desk itself 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 desk 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 WinU to give no warning before desk 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. In these modes, when time expires the desk remains visible but deactivated. However, you can use the Advanced Screen to set any button so it continues to work in a timed-out desk.

You can also set this as time per logon, in which case the maximum time is available whenever logging onto the desk. This setting can be useful when setting up a public kiosk because, unlike the other time settings, when the "time per logon" runs out WinU closes all running programs and completely logs off that desk. This can be helpful in encouraging those "enthusiastic" users to yield the computer to other patrons. When this setting forces a logoff, WinU switches to the default desk if there is one, or to the initial "No Desk" screen if there isn't. WinU will close all running programs and reset the time even if there is only one desk, and that desk is the default, and you're already on that desk. Therefore, when the default desk has a "time per logon" setting, you can use this as a way to restart without actually changing desks.

If you use "time per logon" and have set up WinU to use Systemwide Time Limits, you can optionally tell WinU to reset the systemwide time to zero (no time left) when returning to the default desk. Another Systemwide Time Limits option can initially start the computer with no time available on any desk. Nothing will run until time is sent to this computer externally, perhaps by using the Remote Administration Manager.

The desk time limit can also be set in the password file, if you have set up this desk to look for its logon password in an external file. The password file can specify the desk's maximum amount of time (time per logon) when accessed with that password, or time per day or per week. You can also set an expiration date/time after which that password is no longer valid. Like cumulative time testing, password-file timeouts count the amount of time that the user spends logged on to the desk, whether a program is running or not. If using "time per logon," WinU completely exits from that desk when time expires. In the other time modes, the desk remains visible but deactivated.

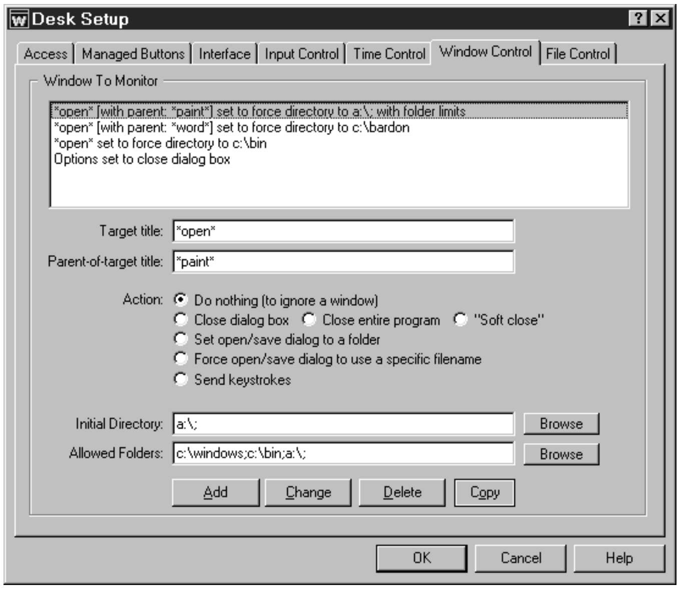
Remember that there are two independent time-control mechanisms: the cumulative time mechanism and the password file mechanism. If using both a password-file time limit and a local-computer cumulative time limit, the smaller (sooner) time limit will prevail. WinU's Administration Manager modifies the cumulative time mechanism but not the password-file time mechanism. So, if the user is running out on the password-supplied time, the cumulative time won't override.

Blockout Periods: These are days and times during which no programs on this desk will run (except those buttons which were set so as to continue to work in a timed-out desk), 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. Navigation buttons can be set so they will still work during a blockout period, allowing the user to exit from a blocked desk.

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

Clear: This will delete all entries.

Window Control Tab



open [with parent: *paint*] set to force directory to a:\; with folder limits
open [with parent: *word*] set to force directory to c:\bardon
open set to force directory to c:\bin
Options set to close dialog box

Target title: *open*
Parent-of-target title: *paint*

Action:
● Do nothing (to ignore a window)
○ 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

Initial Directory: a:\;
Allowed Folders: c:\windows;c:\bin;a:\;

Window Control lets you control virtually any window or dialog when it appears. What can you do to a window? You can close it (in one of three ways); you can set Open or Save As dialogs to a particular folder, from which the user provides the actual filename; you can provide the complete folder-and-filename yourself, forcing the dialog to open or save only that one specific file; and most powerful of all, you can send any keystrokes to any window the moment it appears. You can also "do nothing" to a window, which lets you ignore it, a good way to provide an "exception" (see below).

You might wonder how these "close window" options differ from WinU's "close non-button window" feature. There are two ways. First, the non-button window 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. This 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, with three different radio buttons on this screen. See below for details.

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

Let's look at each option in turn.

Target title: WinU looks at the title bar text of the current active window or dialog, and if the text matches a target title on the Window Control list, the corresponding action is taken. The * and ? wildcards can be used freely in the target title specification. The title is not case sensitive.

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

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

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

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

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

Do nothing: This is a way of providing an "exception" for a specific dialog. For example, you might have a Window Control set up to close all Options dialogs from any program. But maybe you want to allow the Options dialog from one specific program. To do this, list a target title of Options, and a parent-of-target title of the program you want to allow. That program's Options dialog will be allowed, yet all other program's Options dialog will be closed.

Close dialog box: Many programs provide menu items which pop up dialog boxes. Perhaps you don't want a particular dialog box available to the user. If so, give that dialog's title text as the target title. 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 title bar text here. It will be terminated in the usual WinU fashion as soon as it comes up. Of course, another way to disallow such programs is by making sure non-button windows are not allowed on this desk. But then you have to list as Exceptions every non-button program which is allowed to run. That can get tedious. Use the "close entire program" when you are willing to allow most non-button windows, but want to deny access to one specific program.

"Soft close": Like the "close entire program" option, this is intended to close an entire application, not a dialog box. Use this to close 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. However, such programs might tolerate this "soft close" method, which attempts to use the program's own termination procedure to get it to exit gracefully. This method won't always work; in particular, it might trigger an "are you sure you want to exit" message from the program you are trying to terminate, which could allow the user to continue. But if the program does not have this sort of "are you sure" message (or if you can disable that message), the "soft close" can provide a useful alternative method of terminating fussy programs. "Soft close" is especially handy when trying to persuade a recalcitrant game to restore the normal Windows screen colors at exit.

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

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

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

Force open/save dialog to use a specific filename: This is similar to setting a file-open or file-save dialog to a folder, but this option sets it to the complete 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 %DESKNAME% (current desk name), %USERNAME% (user name given through current network or Windows logon) and %COMPUTERNAME% (the designated name of this current WinU computer). All these are case sensitive.   And here's a hint: when constructing the forced filename, don't give a file extension. Instead, let the Save As dialog add its default extension to your generated name. This allows Windows to do certain automated processing based on the file's extension.

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

What keystrokes can you send to a window? You can give regular characters, of course, so to send "abc" simply type that into the 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 pause before the keystrokes are sent, start the keystroke sequence with {Wait N} where N is the approximate number of seconds to wait before sending the keystrokes. For example {Wait 15} will wait about 15 seconds before sending the keystrokes. The {Wait N} item must be the first element on the line.

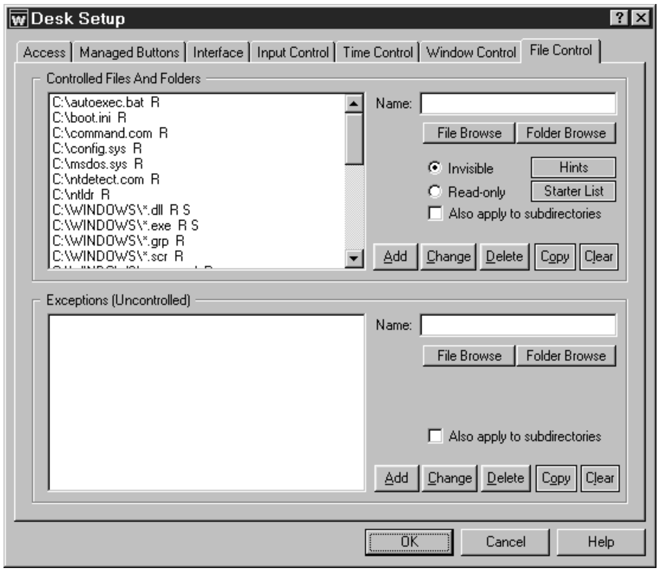
To give a regular key combined with Shift, Control, or Alt, precede the key with one or more of the +^% special characters. To indicate that more than one of these are held down while pressing a key, enclose the entire set in brackets, for example {^%J}. Parentheses can be used to group keystrokes. For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

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

Clear: This will delete all entries.

File Control Tab



Controlled Files And Folders

```
C:\autoexec.bat  R
C:\boot.ini  R
C:\command.com  R
C:\config.sys  R
C:\msdos.sys  R
C:\ntdetect.com  R
C:\ntldr  R
C:\WINDOWS\*.dll  R S
C:\WINDOWS\*.exe  R S
C:\WINDOWS\*.grp  R
C:\WINDOWS\*.scr  R
```

● Invisible
○ Read-only
□ Also apply to subdirectories

Exceptions (Uncontrolled)

□ Also apply to subdirectories

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

In addition to these systemwide restrictions, you can also give per-program file control restrictions that are in effect only when a particular managed-button program is active. This is done from the Advanced screen of the Managed Buttons tab. If per-program restrictions are given, and that program happens to be the active window, the per-program restrictions will override these systemwide settings on the File Control tab.

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

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

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

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

Clear: This will delete all entries.

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

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

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

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

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

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

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

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

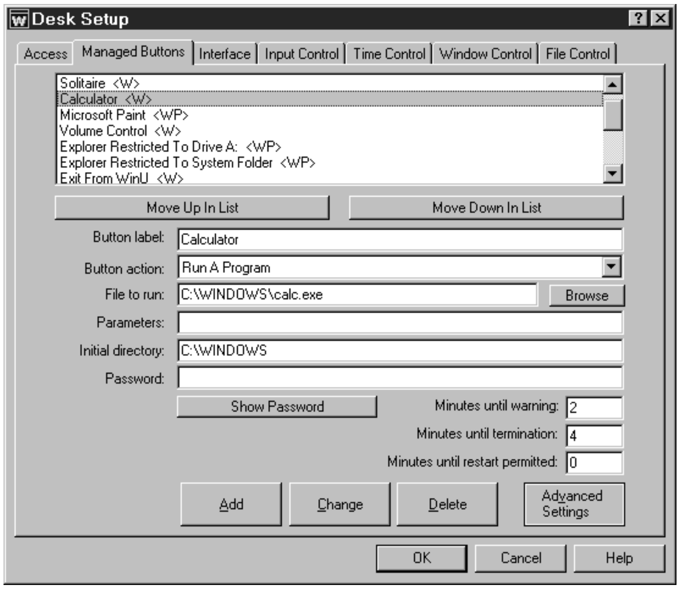
Access-Denied Reports: If any of your programs don't work correctly under WinU's file protection, use WinU's access-denied reports to see which required files were unavailable, and what programs requested them. Then list those files or folders as Exceptions.

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

Chapter 3

Setting Up Program Buttons

Basic Button Settings



Solitaire <W>
Calculator <W>
Microsoft Paint <WP>
Volume Control <W>
Explorer Restricted To Drive A: <WP>
Explorer Restricted To System Folder <WP>
Exit From WinU <W>

Button label: Calculator
Button action: Run A Program
File to run: C:\WINDOWS\calc.exe
Parameters:
Initial directory: C:\WINDOWS
Password:
Minutes until warning: 2
Minutes until termination: 4
Minutes until restart permitted: 0

WinU displays each application on a button. These are set up on the Managed Buttons tab. To run that program, click the button with the mouse or keyboard. Desktop buttons can be set up to launch programs, files, or Shortcuts. DeskLink and PrevDesk buttons can change to another desk, Exit and Shutdown buttons terminate WinU or the entire Windows session, and other button actions can perform specialized tasks.

WinU buttons are easy to set up. Just drag-and-drop any Shortcut, program, or file with a registered filetype onto the WinU desktop, and a new button will appear. WinU asks if you want to configure the new button when you create it. To reconfigure the button later, right-click on it.

Or you can use the Buttons tab to add, change, or delete a button. Most button settings are optional. The required information depends on the *button action*, which is chosen from a dropdown list. For Program or DeskLink buttons, you need give only the File To Run (or desk to switch to) and the button label text, then click *Add* to create the button. PrevDesk, Exit, Shutdown, and similar 'special purpose' buttons require only a button label.

You can get to the Managed Buttons tab through the Setup menu, or by right-clicking on the Apps Button or on the desktop (if not disabled via Kiosk Mode), or by right-clicking on the button itself. All methods bring up the same screen.

After providing the information, click the *Add* button to create a new button. 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.

Applications List: The list at the top of the dialog shows all buttons on this desk. If you got here by right-clicking on a button, the screen starts with that button’s settings displayed. You can at any time select any listed application, to see and change its properties. Following each application's name is a set of letters, enclosed in angle brackets. These letters indicate the settings of the Restrictions and Advanced dialogs for that button. 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:

A: AutoRun this program at desk logon
B: Start as a non-button program
C: Don't terminate program at desk logoff ("continue to run")
F: Custom file control while this program is the active window
H: Hang up the phone on exit
I: Ask program to start minimized as an icon
K: AutoRun, then keep it running until desk logoff
L: Launches Dial-Up Networking
N: No File Control for this program
P: Launch tracking pause is given
S: Use "soft close" on forced termination

T: Can still be run in a timed-out desk
U: Uses Dial-Up Networking
W: Show warning screen for timeout warning
X: Identix biometric validation required to use this button
Y: Play warning sound for timeout warning

Move Up or **Move Down:** Use these buttons to change the order of the applications in the list. This is also the order on the desk and in the Apps Button menu.

Button Label: The text to be displayed on this button. All buttons on this desk are the same width, determined by the text of the longest button label on the desk. Button label text cannot be blank, even if you are using the No Label button style, because the label is also needed for logging and other internal recordkeeping and tracking purposes.

Button Action: Does this button run a program, switch to another desk, go back to the previous desk, exit from WinU, shut down the computer, etc? The action is chosen from a dropdown list. (Actions are described on the Managed Buttons Tab page.) If this is a program button, the label says *File To Run*, and displays the full path and filename of the file, program, or Shortcut which will be launched when this button is chosen (for example C:\BARDON\FANCYFAX.EXE). You can type it in, or use the *Browse* button, or "drag and drop" any filename from Explorer onto this dialog. If this is a DeskLink button, the label changes to *Switch Desk*; WinU will switch to the named desk when this button is clicked.

File To Run/Switch Desk: This is the full path and filename of the program launched by this button, or the name of the desk to switch to if this is a DeskLink button. If this is a PrevDesk, Exit, Shutdown, etc. button, this field is disabled.

Command parameters: Command-line parameters or switches needed by the File To Run. Some button types take no parameters, such as DeskLink, PrevDesk, or Exit buttons.

Initial Directory: The starting directory for a program. If you leave this blank, the program file's directory is used as the initial directory (C:\BARDON in our example).

Password: Will a password be required to run this button? 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 application 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 Warning Screen* box in the Advanced Settings dialog. Un-checking that box will also stop any Desk Timeout warning screen from popping up while this program is active. This is 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 Desk Timeout warning screen.

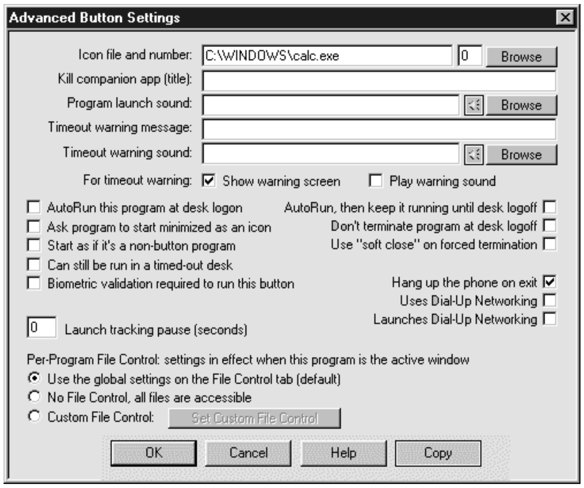
Minutes Until Termination: The number of minutes from the start of the application until the program is terminated. It must be a larger number than the Minutes Until Warning. For example, you might set 10 Minutes Until Warning, and 14 Minutes Until Termination. Set this to zero if you don't want any 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 change the button's icon image, provide a customized warning message, play a sound when this button is selected, and change a number of options which modify the way this application launches and terminates. You can also copy this button to other desks.

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

Advanced Button Settings



Icon file and number: C:\WINDOWS\calc.exe 0
Kill companion app (title):
Program launch sound:
Timeout warning message:
Timeout warning sound:
For timeout warning: ☑ Show warning screen □ Play warning sound

□ AutoRun this program at desk logon
□ Ask program to start minimized as an icon
□ Start as if it's a non-button program
□ Can still be run in a timed-out desk
□ Biometric validation required to run this button

AutoRun, then keep it running until desk logoff □
Don't terminate program at desk logoff □
Use "soft close" on forced termination □
Hang up the phone on exit ☑
Uses Dial-Up Networking □
Launches Dial-Up Networking □

0 Launch tracking pause (seconds)

Per-Program File Control: settings in effect when this program is the active window
● Use the global settings on the File Control tab (default)
○ No File Control, all files are accessible
○ Custom File Control:

The Advanced Button Settings screen is reached by clicking the Advanced button on the Managed Buttons tab of the Desk Setup dialog. The options on this screen let you further customize the way a program runs. You can also copy a button to another desk.

Icon file and number: Perhaps you'd prefer a button image other than the usual icon. You can type a filename, use the Browse button, or "drag and drop" an image file from Explorer onto this dialog. You can use many types of images on a button, not just icons. Try EXE, ICO, DLL, CUR, ANI, or BMP files. The chosen graphic can be of any size; WinU will draw it at icon-size on the button. Use the Browse button to choose any icon from a multiple-icon file, for example a Windows program or DLL.

Kill companion app: Does this program launch another application? Do you want WinU to also terminate the companion application when this program runs out of time? If you do, list the title of that "other" application here. The title match is not case sensitive, and wildcards (* and ?) can be used freely.

Program launch sound: If you've enabled System Event sounds for this desk, you can play a sound when this button is clicked. You can type the sound file name, "drag and drop" a sound file from Explorer onto this dialog, or use the Browse button to select a sound file. The yellow "speaker" button lets you preview the chosen sound. If sounds are enabled but no file is specified for an event, WinU uses its built-in sound for that event.

A desk-level Program Launch sound can also be specified. If there is both a button Program Launch sound and a desk-level Launch Program sound, the button sound is played, not the desk sound.

Timeout warning message: This is your customized warning message to be displayed for this program. 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, WinU plays its built-in warning sound.

A desk-level Timeout Warning Sound can also be specified. If there is both an individual-button Timeout Warning Sound and a desk-level Timeout Warning Sound, the button sound is played, not the desk sound.

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

Play 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, WinU plays its built-in warning sound.

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

Ask program to start minimized as an icon: Check this box if you want WinU to ask the program to start minimized. Most programs will comply with such a request.

Start as a non-button program: Non-button programs are those that were launched after WinU started, but not by WinU; they are not time-limited or tracked. Occasionally you may want to launch program from a WinU button, but not track or control it. To do this, start it as a non-button program by checking this box.

Can still be run in a timed-out desk: In general, when a desk runs out of time you don't want its buttons to work. However this is not always the case. For example, you may want to allow DeskLink buttons to work in a timed-out desk so a user can exit that desk. Or you might want to allow WinU's companion logon program to work because you have set up the logon program to send time to WinU if the logon is successful. To accommodate such situations, check this box to allow the button to work in an otherwise disabled desk.

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

AutoRun, then keep it running until desk logoff: If this box is checked, the program will not only run automatically when the user logs on to this desk, but will be restarted as necessary to ensure that it is always running while in that desk.

Don't terminate program at desk logoff: You usually want all programs launched from a desk to be forcibly terminated when the user logs off that desk. However, by checking this box you can allow a program to remain running even after logging off its desk. Checking this box tells WinU to turn the program into a "non-button" window when logging off its desk, instead of killing it. Because it will then be a "non-button" window, you will also need to make sure that "non-button" windows are allowed on the follow-on desk, and that "non-button" windows are not terminated when changing desks.

"Non-button" programs are not logged and no time limits are enforced against them so, if this box is checked, the program will be logged and tracked only until desk logoff. After desk logoff it is on its own.

Use "soft close" on forced termination: Some programs leave themselves or the computer in a sub-optimal state when forced to terminate. 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 target program doesn't display 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.

Hang up the phone on exit: If you tell it to, WinU will disconnect modem-using apps and hang up the phone. Check this box if this program uses a modem, and you want WinU to hang up the phone and reset the modem when this program must be forcibly terminated. If this app uses or launches Dial-Up Networking, also check the appropriate box below. If this modem-using program uses the old-style DOS "direct to the COM port" communications method, you need only check this one box.

Unlike DOS "direct to the COM port" modem apps, WinU will allow any number of DUN-using apps to run simultaneously. WinU will disconnect Dial-Up Networking after the last of these programs closes.

Uses Dial-Up Networking: Check this box if this button runs a Web browser, email program, or similar application that uses Dial-Up Networking.

Launches Dial-Up Networking: Check this box to indicate that this button directly runs a Dial-Up Networking shortcut. To create such a shortcut, open My Computer, then open Dial-Up Networking, then right-click on any existing DUN shortcut and select Create Shortcut. It will be created on your Windows desktop (you can then move it somewhere else if you like). Next, create a WinU button to run the new shortcut. The easiest way is to drag-and-drop the new shortcut onto the WinU desktop. Finally, go to the new button's Advanced screen and check the Launches Dial-Up Networking box.

This kind of direct shortcut to a Dial-Up Networking connection is the *only* thing for which this box should be checked. If the button runs a Web browser, email program, or another application that simply *uses* Dial-Up Networking, check "Uses Dial-Up Networking" instead. So, for example, the fact that Netscape automatically calls the DUN dialer after you invoke Netscape does not qualify Netscape as a "launching" application.

Launch Tracking Pause: There are some programs that start by launching a "helper" app, not the real program. The "helper" app simply sets things up, then in turn it launches the "real" program before itself exiting. For example, batch files and Shortcuts work this way. *Launch Tracking Pause* is a powerful option that lets you launch these "piggyback" programs in a way that allows WinU to track them. If you find that one of your programs doesn’t launch correctly, or launches for a few seconds and then vanishes, try giving it a two-second *Launch Tracking Pause*. This creates a brief security hole, but realistically it'd be hard for a user to do much damage in just a few seconds.

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

Copy Button: To copy this button to another desk, click the Copy button. You can copy a button to one specific desk, or to "Every Desk" on this computer.

Chapter 4

Security And Administration

System Administration With WinU

The concept of WinU 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 WinU-enabled computer, perhaps on a network.

WinU provides many ways for you to manage computers remotely. While a client computer is active you can use WinU'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, start programs, stop programs, change settings, and even logoff or shut down the computer remotely. WinU's Remote Administration Manager, License Meter Manager, Password Manager, and Logon Manager are designed specifically to allow administrators to dynamically modify settings and control access and activity on networked computers.

Another way to manage computers remotely is by broadcasting your changes using the clonefile mechanism. In addition, you can set up your master clone configuration with per-computer options which let you specify which managed programs and desks 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.

Security Considerations

WinU provides very thorough security control for your computer. Here are some things you can do to help WinU, 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 WinU's File Control to make your important files and folders read-only or invisible. Another option is to use the Input Control tab to hide drives when this desk is active. 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.

Close unnecessary programs: WinU doesn't mind when other programs run at the same time it is active, but before you start WinU you should still exit from all unnecessary programs. WinU can be set to keep hidden any programs running before it started. However, the most secure situation is to not run them in the first place.

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

Disable booting from floppy disk: If your computer is booted from a floppy instead of from your hard disk, WinU won't run, so it can't protect your system. Fortunately, it's easy to guard against this on most computers. 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.

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

Change passwords regularly: An easy way to enhance security is to change the setup, desk, and application passwords on a regular basis. Change them to something that isn't obvious, so as to make it difficult to guess. If you have set up your system to get its logon passwords from an external password file, it's easy to use WinU's Password Manager program to change the logon passwords for all the WinU computers on your network from one central location.

Kiosk Mode

Kiosk Mode is a group of switches which control whether the menu bar and status bar are displayed, whether the user can bring up dialogs by clicking on the desktop surface, and whether the user name or computer name are shown in the title bar. The menu bar and desk-click dialog switches lets you tightly control desk-to-desk navigation. When there is no menu bar, and the user can't bring up the Choose Desk dialog by clicking on the desk surface, the only navigation elements are any DeskLink or PrevDesk buttons you have provided on the current desk. DeskLink buttons are like webpage links, they change to a specific desk. PrevDesk buttons let you go back to previously-visited desks, in reverse order. When combined with these Kiosk Mode options, DeskLink and PrevDesk buttons let you set up a distinct navigation sequence through your WinU desks. Of course if you provide no such buttons on the visible desk, the user can't go anywhere.

When these switches are used, the screen is much like a kiosk, or an ATM machine: what you see is what you get. Full use of them disables all the usual routes to the System Setup dialog, so to turn off Kiosk Mode, WinU adds a System Setup menu item to the standard System menu. (To open the System menu, click the small icon at the left edge of WinU's title bar.) Desk-click dialogs are always allowed in Setup mode, so the administrator can use this feature while configuring the system.

Finally, the kiosk mode group includes a switch which controls whether WinU includes the computer name in the WinU title bar. Displaying this name provides a handy way to quickly identify a particular WinU computer.

Chapter 5

Advanced Topics

How To Clone A Computer

WinU's cloning feature takes a "snapshot" of the WinU setup on one computer, so it can be copied to another computer or saved as a backup. The data is saved in a clone file when you click the *Export Clone File* button on the Remote Management tab of the System Setup dialog. The clone file contains all the data in this computer's configuration.

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

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

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

<u>Update when installing:</u> To include clone data as part of the installation process, copy a clone data file named *clone.bds* to the same directory as the WinU installer (floppy disk or network install directory), with the other WinU files. Run the WinU installer in the usual way. When the installer sees the data file, it will offer to copy the clone data onto the new machine.

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

<u>Updating manually:</u> To update manually, enter WinU'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 WinU computer will immediately update itself. In this case, the clone file does not need to be named clone.bds because you are explicitly pointing WinU to the file you want it to use. You can also update manually using a plain-text "settings" file.

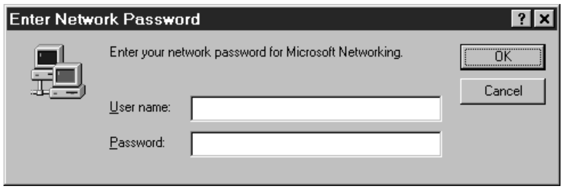
<u>AutoUpdate:</u> To dynamically update an already-installed remote client computer, copy a clone file to the directory in which that client computer looks for clone data files. This was specified in that computer's System Setup dialog on the Remote Management tab. On the next restart, the computer will see the new data file in that directory, read it, and replace the old data with the new data. For security reasons, you might want to just give the client machine read-only permission in that directory through the usual network facilities.

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

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

When setting up your master computer, you might also want to assign per-user default desks to have WinU look at the network logon name so as to determine which desk will be the default for this session. Since WinU's desk-to-desk navigation can be tightly controlled, you can use this method to ensure that different users of the same WinU computer have access to only those WinU desks they are allowed to use.

Using the Windows Logon Screen



Enter Network Password

Enter your network password for Microsoft Networking.

WinU can use the Windows logon name to provide per-user validation and customization.

Windows NT/2000/XP/Vista/Win7 already requires that users log on with a name and password, so there is nothing extra to set up. Here is how to set up your Windows 95/98/ME computers so users must give a logon name at startup.

When you boot your 9x computer, do you see a logon screen similar to the one in the picture, which asks for your user name and password? If so, you are all set. The name given by the user in that screen will be seen by WinU when it starts. If that name matches a per-user default desk listed in WinU, that desk's settings will be used.

You can set WinU to validate the logon. If you set this up, and the name is not valid, WinU 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 WinU, the Default Desk restrictions and controls will be put into place for this logon. So if you don't mind that all users start on the same desk, 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.

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

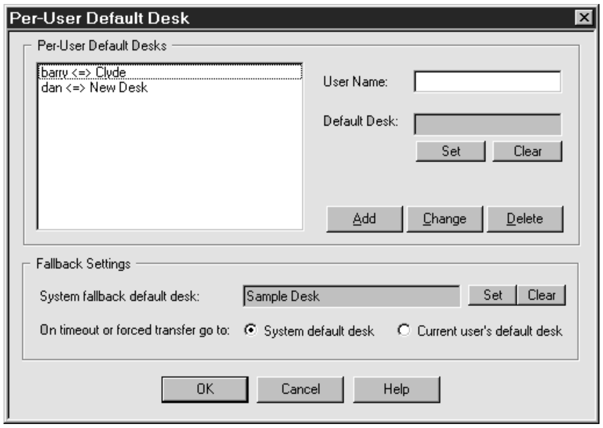
However, saving separate configuration files for each user can eat up quite a bit of disk space. For this reason, WinU does not require that Windows save each user's individual configuration separately. All that is needed is to have Windows display the logon-name screen itself.

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 WinU with a per-user default desk 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.

Per-User Default Desks


Per-User Default Desk

Per-User Default Desks

barry <=> Clyde
dan <=> New Desk

User Name:

Default Desk:

Fallback Settings

System fallback default desk: Sample Desk

On timeout or forced transfer go to: ● System default desk ○ Current user's default desk

The default desk is the first screen the user sees at logon. This is set up from the Security Settings tab of the System Setup dialog. If you use the Kiosk Mode switches to restrict navigation, the user cannot go to other desks unless you make them available through DeskLink buttons.

To give each user a different default desk, tell WinU that the default desk is dependent on the current multi-user or network logon. Windows and most networks let users specify a name when logging on. WinU can look at this user name to see who is logged on, then display the appropriate default desk for that person. If a different user logs on, a different default desk will be shown.

To accommodate older networks which are not Windows-aware, you can optionally set this up to look for the current user name in an environment variable instead of the standard Windows registry-based location.

User Name: Give the user name as it will be typed into your network logon screen. This is not case sensitive.

Default Desk: Use the *Set* button to choose the default desk to which WinU should switch when this user logs on, or use the *Clear* button if this user should be sent to the system fallback default desk.

Add: Add this user/desk entry to the list.

Change: Replace the selected list entry with new information.

Delete: Remove the selected entry from the list.

System fallback default desk: This is the desk that WinU should switch to if the per-user default desk is not available for any reason. It can also be used as the target desk when the current user runs out of time or is otherwise forced to exit. The system fallback default desk can be an actual desk, or it can be WinU's "No Desk" screen.

On timeout or forced transfer go to: If you have set to a per-user default desk based on the current logon name, you probably want to send the user to the system fallback default desk on timeout or other forced termination. The system fallback default desk won't have their personal set of programs available, but might have a Logoff button to allow someone else to log on to the network. You can even AutoRun the Logoff button so it logs off the current user immediately on entering the system fallback default desk.

Reset Mode

Reset Mode is a fail-safe mechanism built into WinU. It lets you start WinU 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 handy if your computer happens to go down at a time when WinU is set to not allow non-button windows by filename. If this happens, the "don't run" settings will still be in place on reboot, and almost nothing on your computer will run. Fortunately, things have been set up so that in this situation, WinU itself will still run. Most of the time you can simply start WinU (perhaps in Safe Mode), then immediately exit normally to remove the leftover security control settings from your computer.

If this doesn't work, though, start WinU in Reset Mode. The easiest way to do this is to run the WinU Reset program (reset.exe) from Explorer, or in any other convenient way (like WinU itself, this program will always run). Remember that reset.exe must be in the same directory as the WinU program itself. Another way is to start WinU from a command prompt with the /reset parameter (c:\somedir\otherdir\winu.exe /reset).

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

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

Using While WinU Is Running: Though this is rarely needed, Reset Mode can also be used to access WinU's configuration options while WinU is running. If WinU is already running when you run reset.exe, WinU will ask for its setup password, then go into setup mode. When using Reset Mode in this way, after leaving setup mode the disabled security settings listed below will be re-enabled and WinU will function normally.

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

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

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

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

How To Use: When in Reset Mode, you should simply make the necessary setup changes and then exit, because most of WinU's strongest security settings are not in effect. In this mode, WinU does not perform the following security checks: ensure that this is the only copy running; exit if this is an expired beta copy; test its components for tampering; validate user names at logon; enforce kiosk mode desk-click dialog restrictions; enforce the inactivity timer; run AutoRun buttons on this desk; exit a desk if using "time per logon" and the time has run out; process remote clonefiles or messages; use license metering; monitor for Window Control; do logging; control non-button windows; hide drives; 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.

Using Internet Software

Here is how to set up WinU to run your Web browser, email program, or other software that accesses the Internet. Special attention is paid to managing Dial-Up Networking, but this information will also be useful if you are using the Internet through a LAN connection.

Adding Internet Software: A browser, email program, or other Internet application is added to a WinU desktop in any of the usual ways. You can drag-and-drop the exe or shortcut onto the WinU desktop, or give its information through the Buttons tab of the Desk Setup dialog. There is only one difference: if you are connecting through Dial-Up Networking, you must go to that program's Advanced screen and check the two boxes labeled *Hang Up The Phone* and *Uses Dial Up Networking*. This tells WinU to monitor for Dial-Up Networking connections while this and other DUN-using programs are active, and close such connections when the last DUN-using program is closed.

Most Windows computers are set up to connect automatically to the Internet as needed. That is, Windows automatically makes the connection for you when an Internet application first tries to access a website, check your email, etc. However, if you need it, WinU does allow you to create a button which directly runs a Dial-Up Networking connection. You might want to have such direct-connection buttons if this computer isn't set up to connect automatically. Or perhaps you have more than one Internet Service Provider and want to be able to choose which connection to use.

If you create such a button, you must check its Advanced screen box labeled *Launches Dial-Up Networking*. This kind of direct shortcut to a Dial-Up Networking connection is the only thing for which the *Launches* box should be checked. If the button runs a Web browser, email program, or another application that simply uses Dial-Up Networking, check *Uses Dial-Up Networking* instead. So, for example, the fact that Netscape automatically calls the DUN dialer after you invoke Netscape does not qualify Netscape as a "launching" application.

To create such a shortcut, open My Computer, then open Dial-Up Networking, then right-click on any existing DUN conncetion icon. A popup menu will appear. On that menu, select *Create Shortcut*. The shortcut will be created on your Windows desktop. You can then move it somewhere else if you like.

Next, create a WinU button to run the new shortcut. The easiest way is to drag-and-drop the new shortcut onto the WinU desktop.

Finally, go to the new button's Advanced screen and check the *Launches Dial-Up Networking* box.

Whether Dial-Up Networking is started automatically from a program that *Uses Dial-Up Networking*, or explicitly from a button that *Launches Dial-Up Networking*, the connection will be terminated when the last DUN-using program is closed, or when logging off this desk. The administrator can also use the Remote Administration Manager to send this WinU computer a command to hang up the phone and close its currently-open Dial-Up Networking connection.

Web Browser Monitor: The WinU Web Browser Monitor lets you log all the websites that are visited while WinU 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. On the Input Control tab you can set WinU to prevent browser windows from accessing local files.

Controlling what websites users can visit: On the Access tab you can list the websites which users are allowed to visit. These can be listed by URL or title, and can be on the Internet or on your company's intranet.

Setting Up CD Based Software

Two problems sometimes arise when running software from a CD. Both are easily solved. by using options found on the Advanced screen, which can be accessed from the Buttons tab of the Desk Setup dialog.

CD drive lag time: Some CD software installs its executable program on the hard disk, but reads the data from the CD. The CD must be in the drive whenever the program is run. If the CD drive is slow, the program could start but might need to wait a relatively long time for the data on the CD to become available. During this wait, the program is inactive. If it is inactive long enough, WinU could decide that it is not running, and stop tracking the program. Or it might decide that the program is hung, and terminate it. The solution to this problem is to give that program's button a brief Launch Tracking Pause.

Look at the WinU button when the program launches. When you click the button, it turns red and says "please wait." Does it ever turn yellow? Yellow means that WinU has locked on to that program. If it never turns yellow, WinU couldn't find the program. A Launch Tracking Pause will give the program time to launch before WinU tries to track it. Here is how to set one up. In regular Windows (not through WinU), start your application and count how many seconds it takes for the final window to appear ... not a splash screen but the actual user window. Close the application. Start WinU and log on to the desk that contains the application's button. Right-click on the program button for that application. The password dialog will appear. Enter your Setup Password. The Buttons tab will appear with that program's information displayed. Click on Advanced. The Advanced screen appears. In the box marked Launch Pause enter the number of seconds you counted. You may want to add a few more seconds to ensure that the pause is long enough. Click OK to exit from the Advanced screen, and OK again to close the Desk Setup dialog. Exit from Setup Mode. Start the application from its WinU button. Its WinU desktop button should turn yellow, and the application's screen should remain visible.

Multimedia reconfiguration: Some multimedia programs (which are usually CD-based) insist on using a particular screen resolution, color palette, or sound configuration, to the exclusion of all other programs. These programs change your system to accommodate their own needs without regard to the fact that some other program might need to pop up a dialog box or play a sound while the multimedia program is running. Also, such programs are sometimes fussy about how they are closed when they run out of time. WinU provides a number of options to allow such programs to run under WinU's monitoring. Depending on the CD program's behavior, you may need to use one or more of these options.

While running your multimedia program under WinU, you'll know you have this problem if WinU's popup time-limit warning box makes the screen colors go funny, or if WinU's warning sound makes the audio behave oddly, or if, when the program runs out of time and WinU terminates it, the computer is left in any kind of sub-optimal state.

WinU provides options to not display warning popup messages or play warning sounds while a particular program is active. To terminate such programs in a way they will tolerate, WinU provides a "soft close" option that mimics the way a user might close the program from the keyboard. All of these are set from the Advanced screen for this program, which can be accessed from the Buttons tab of the Desk Setup dialog.

In extreme cases, you may need to start certain programs as non-button windows. Doing this means that WinU will not track the individual program. You can't have per-program time limits. However you can have desk time limits and unless you explicitly arrange otherwise the desk will close all non-button windows when it times out. Sometimes this is enough control, so this method can be used to solve these extreme cases, which fortunately are not common. As with the other options, starting an application as an "instant non-button" program is set up from the Advanced screen for this program, which can be accessed from the Buttons tab of the Desk Setup dialog.

WinU Web Browser Monitor

WinU is designed to provide reliable management oversight to Internet software.

WinU can monitor all the websites that are visited while WinU is running. To activate this feature, use the Event Log tab to set up WinU for logging, and check the box on that tab labeled *Web browser monitor*. WinU will log the website URL, title, and the number of minutes at each site, for all websites visited through Netscape, Mozilla, or Internet Explorer. This information can be viewed through WinU's built-in reports. It can also be viewed remotely through the Administration Manager.

On the Access tab you can list the websites which users are allowed to visit. With this option, if a browser displays a webpage that isn't on the list, the browser will be closed. Valid sites can be specified by title or URL.

On the Input Control tab you can set WinU to prevent web browsers from showing files or directories on the local hard disk or network.

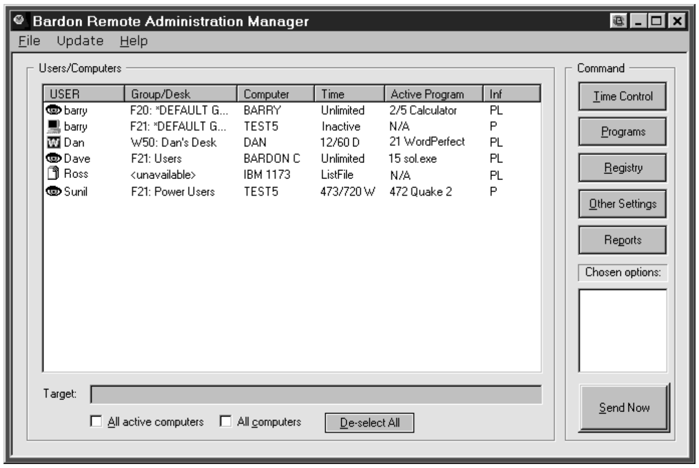
Browsers can have multiple windows open at the same time. WinU can track up to 500 open browser windows simultaneously. Pages which are visited for just a few seconds are ignored.

Note that if you check *Session and desk events* on the Event Log tab WinU logs all active (foreground) window usage. This includes Web Browser windows, though not with quite as much detail as the specific Web Browser Monitor report.

Chapter 6

Companion Software

Remote Administration Manager



USER	Group/Desk	Computer	Time	Active Program	Inf
barry	F20: *DEFAULT G...	BARRY	Unlimited	2/5 Calculator	PL
barry	F21: *DEFAULT G...	TEST5	Inactive	N/A	P
Dan	W50: Dan's Desk	DAN	12/60 D	21 WordPerfect	PL
Dave	F21: Users	BARDON C	Unlimited	15 sol.exe	PL
Ross	<unavailable>	IBM 1173	ListFile	N/A	PL
Sunil	F21: Power Users	TEST5	473/720 W	472 Quake 2	P

Target:

□ All active computers □ All computers

The Administration Manager lets the administrator, at another station on the network, reset the current time limits, list running programs, close programs, start new programs, modify the Registry, change clone-update settings, remotely logoff any user, shut down the remote computer, initiate a checkpoint, send a brief popup message, or generate various activity reports on the target remote computers.

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

The Administration Manager can have Full Control update itself using the Version Update menu item.

The remote stations can be running Full Control 2 or 3, or WinU 5 or 6. The Administration Manager can be resized and its columns adjusted. It remembers its columns, size and position from session to session.

Password Protection: A copy of WinU or Full Control must be installed on the administration computer, and its password must be given in order to use the Administration Manager. The password is requested when the Administration Manager starts.

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

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

The Message Command Folder: The "Message Command Folder" allows the exchange of data files and other large messages between the Administration Manager and the remote computers. If WinU or Full Control has been installed on this computer, and if a "Remote Administration Messages" folder has been named on the Remote Management tab, that folder is used. If not, you will be prompted for a folder at startup. Typically this directory will be on a server, where it can be seen by both the WinU and Full Control computers, and the Administration Manager station. This folder must be able to handle long filenames because Remote Administration filenames can exceed the now-defunct DOS 8.3 filename format. If you are using TCP/IP messaging the Administration Manager needs read/write access but the other computers just need read-only access to this folder. If you are not using TCP/IP messaging all computers must have read/write access to this folder. If you are using TCP/IP or Network Generic messaging when you change the folder here, the new folder location will be immediately broadcast to all listed computers, but if you are using the File-Based messaging method you must change this folder name on each of the remote computers in some other way.

Using The Remote Administration Manager Program: The administrator can run the Remote Administration Manager from anywhere on the network that can access the "Message Command Folder". The network must be enabled for long file names. A copy of WinU or Full Control must be installed on this computer, and its setup password is required in order to run the Administration Manager.

The "Users/Computers" list shows information about who is and isn't logged on, and the current state of those computers. The columns list the current logged-on user's name, the currently active WinU desktop or Full Control group, the name of the computer, time settings, whether this computer is currently active, and whether a password is available for this computer. Click any column header to sort the list by that column; click it again to reverse-sort. To change the width of these columns, place your cursor on the line between two columns. When the cursor changes to the "move" shape you can adjust the column widths to your liking. To reset the columns to default widths, press Ctrl-KeypadPlus, that is, the Control key and the big gray Plus key on the numeric keypad. The columns are:

User: This is the current logged-on user's name, as given at the Windows logon screen. The displayed icon shows whether the user is inactive, active in WinU, or active in Full Control. There is also a ListFile icon which is displayed if this user's line was read in from a ListFile (see below) and has not yet ever become active.

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

Computer: The Windows-defined name for the computer.

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

Active Program: If this user/computer is currently logged on, this column shows the current active application (foreground window) and the current number of minutes since that application was started. If that program has a time limit, it is shown after the current minutes, separated with a slash. If it is a Full Control managed application or a program launched from a WinU button, the name shown here is the same name you gave it when you set up that program, otherwise it is listed here by its actual executable filename. If you have allowed your users to launch multiple instances of Full Control managed applications, remember that these are all considered together for time-control purposes, so the current minutes shown are the number of minutes since the first instance was launched. Also, if that computer isn't running, its Active Program is listed as "N/A" (not available).

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

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

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

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

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

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

You can also schedule a message to be sent at a later time. To do this, choose the "Send Later" option from the File menu. If you are not using TCP/IP messaging (set from the File menu) then the target computer must have read/write access to this folder so it can delete the message file after reading it. If you are using TCP/IP messaging then the message is not sent by file, so the Administration Manager needs read/write access but the other computers just need read-only access to this folder.

Also on the File menu is an option to "Send Command To Another Folder." This saves the command as a file, and puts it in your chosen folder. At some future time, you could then manually copy that file to the "Message Command Folder" where it can be seen by the target computer. The target computer must have read/write access to the Message Command Folder so it can delete the message file after reading it.

A message that is sent by 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. WinU or Full Control will delete the file immediately after it is read. To transmit files, your network must support long file names so as to accommodate a computer name that might exceed the now-defunct DOS 8.3 filename standard. The target computer must have read/write access to the Message Command Folder so it can delete the message file after reading it.

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

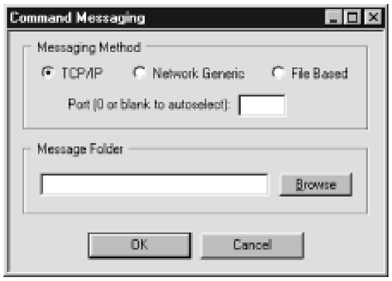
Delete Selected Chosen Options: As you build a command, entries are added to the Chosen Options list to remind you of what you have set up. If you change your mind, these options can be deleted by selecting one or more in the Chosen Options box and using this item from the File menu. It's just like un-checking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

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

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

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

Show Inactive Users: After a user logs off, a computer is displayed as Inactive during the current session. Sometimes it's useful to see these Inactive entries when starting the next session, too. Use this menu item to do so. If a user was logged on to more than one computer, you'll see the most recent of those logons.



Command Messaging

Messaging Method: ● TCP/IP ○ Network Generic ○ File Based

Port (0 or blank to autoselect):

Message Folder

Messaging Method and Message Command Folder: These two menu items were separate in previous versions. In this release, they display a single dialog box in which to supply the requested information. Briefly, the Administration Manager can communicate by any of three methods: TCP/IP, Network Generic, and File-Based. To communicate, you must also give a Message Command Folder, which is usually a shared folder on a server.

TCP/IP Messaging Method: This is the most reliable and robust option. With it, you can communicate to any computer within your LAN, even across NT/2000/XP/Vista/Win7 domains. If using personal firewalls on each computer, you will need to explicitly select a port so you can open that port in your firewalls. Otherwise you can let the Administration Manager autoselect the port. Most computers come with the TCP/IP protocol already installed, and so are able to use this right off the bat. If it's not there, the TCP/IP protocol can be installed from the Network applet of Control Panel.

Network Generic Messaging Method: The advantage of this is that it will run on any network, with any protocol you've installed. However it is sometimes slower and less reliable than TCP/IP, it generates more network traffic, and it cannot communicate between NT/2000/XP/Vista/Win7 domains.

File-Based Messaging Method: This is intended only as a fallback for those unusual situations where neither of the other methods work. It puts its messages in little files and copies these files to the designated "Message Command Folder" where they can be seen by the target computer.

Message Command Folder: This folder allows the exchange of data between the Administration Manager and the remote computers. If WinU or Full Control has been installed on this computer, and if a "Remote Administration Messages" folder has been named on the Remote Management tab, that folder is used. If not, you will be prompted for a folder at startup. Typically this folder will be on a server, where it can be seen by both the WinU and Full Control computers, and by the Administration Manager station. This folder must be able to handle long filenames because Remote Administration filenames can exceed the now-defunct DOS 8.3 filename format. If you are using TCP/IP messaging the Administration Manager needs read/write access but the other computers just need read-only access to this folder. If you are not using TCP/IP messaging all computers must have read/write access to this folder. If you are using TCP/IP or Network Generic messaging when you change the folder here, the new folder location will be immediately broadcast to all listed computers, but if you are using the File-Based messaging method you must change this folder name on each of the remote computers in some other way.

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

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

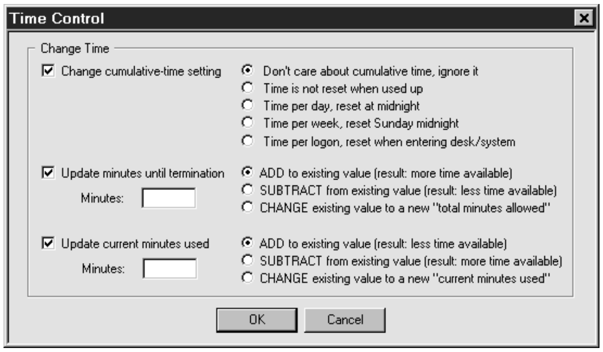
Let's say a customer arrives and sits at a computer. There is zero time available. From the administration station, you remotely send some time to that computer, perhaps 30 minutes. The customer uses the computer for the allotted 30 minutes as the counter ticks down.

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

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

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

Administration Manager Time Control



Time Control

Change Time

☑ 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"

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

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

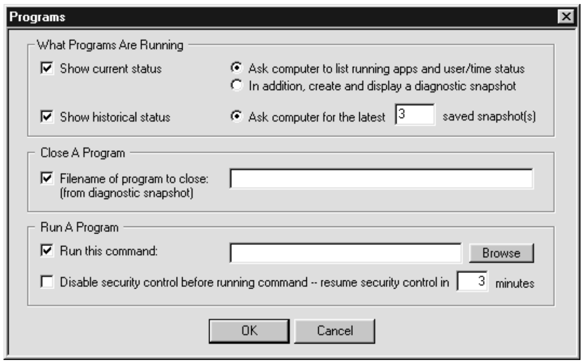
Update minutes until termination: If you increase the minutes until termination, there will be more time available; if you decrease this, there will be less time available. This change is permanent. It sets the cumulative time Minutes Allowed value, which is saved from session to session. You can *add* minutes to the current value, *subtract* minutes from it, or *change* it to a new value entirely. It can be set from zero (meaning: no time is available) to 9999999 minutes (approximately 19 years).

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

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

One way to use the Administration Manager might be to set the public computer to "no time left" when WinU or 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*). WinU or Full Control will warn the customer in advance of expiration. You then use the Administration Manager to send the machine more time.

Administration Manager Programs Control


Programs

What Programs Are Running

☑ Show current status
● Ask computer to list running apps and user/time status
○ In addition, create and display a diagnostic snapshot

☑ Show historical status
● Ask computer for the latest 3 saved snapshot(s)

Close A Program

☑ Filename of program to close: (from diagnostic snapshot)

Run A Program

☑ Run this command:

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

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

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

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

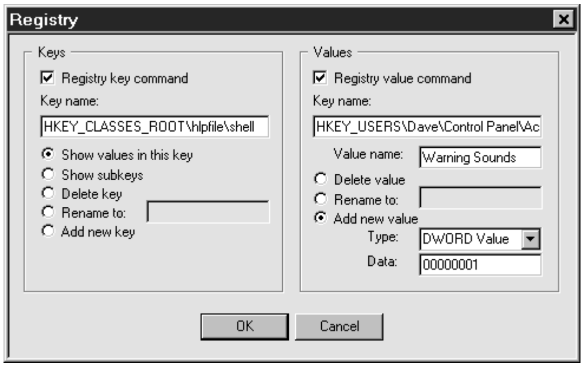
Close A Program: Give the full-path filename of the program you want to close on the target computer. A diagnostic snapshot can show a list of programs currently running on that computer, or you can type in the full-path filename manually.

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

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

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?

Administration Manager Registry Control



Keys

☑ Registry key command

Key name: HKEY_CLASSES_ROOT\hlpfile\shell

● Show values in this key
○ Show subkeys
○ Delete key
○ Rename to:
○ Add new key

Values

☑ Registry value command

Key name: HKEY_USERS\Dave\Control Panel\Ac

Value name: Warning Sounds

○ Delete value
○ Rename to:
● Add new value

Type: DWORD Value

Data: 00000001

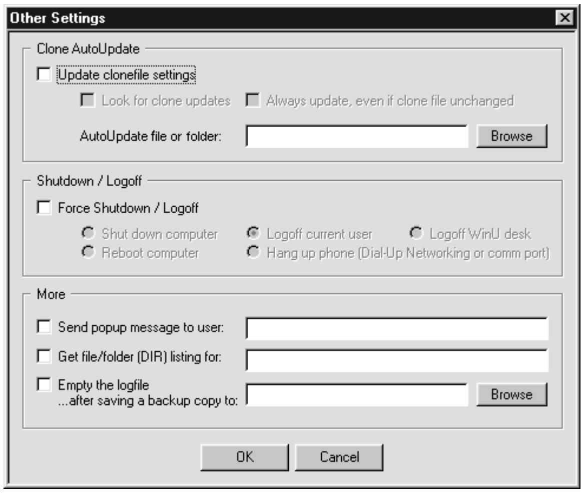
Options are available from the Administration Manager Registry screen which allow you to view and modify registry settings on the remote computer, even if that computer has not been set up for remote registry editing. It is intended for occasional use, especially in emergencies.

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

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

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

Administration Manager Other Settings



Other Settings

Clone AutoUpdate

☐ Update clonefile settings

☐ Look for clone updates ☐ Always update, even if clone file unchanged

AutoUpdate file or folder: [Browse]

Shutdown / Logoff

☐ Force Shutdown / Logoff

○ Shut down computer ● Logoff current user ○ Logoff WinU desk

○ Reboot computer ○ Hang up phone (Dial-Up Networking or comm port)

More

☐ Send popup message to user:

☐ Get file/folder (DIR) listing for:

☐ Empty the logfile
...after saving a backup copy to: [Browse]

[OK] [Cancel]

This sets the same options described on the Remote Management tab, which allow you to update a computer's clone data file/folder name and check the *Look for clone updates* box. WinU or Full Control can look in that directory at startup or shutdown for a specific clone data file, or you can list just the folder name and it will look for a clone data file named *clone.bds* (for WinU) or *clonefc.bds* (for Full Control). If you list a clone file name (not just a folder name) remember that WinU and Full Control clone files are not interchangable; they use different formats and settings. You can update all your WinU computers with one file, and all your Full Control computers with a second file, but you can't use the same file for both. However, if you list a folder name (not a specific clone file name) the settings for WinU and Full Control are the same. There's no problem sending those settings to both WinU and Full Control at the same time. Just put separate *clone.bds* (for WinU) and *clonefc.bds* (for Full Control) files in the named folder. If a file is found, WinU or Full Control will overwrite its current configuration with the new data. You can also set whether the clone update is performed whenever a clonefile is found, or only when it has a different filedate from the last clonefile.

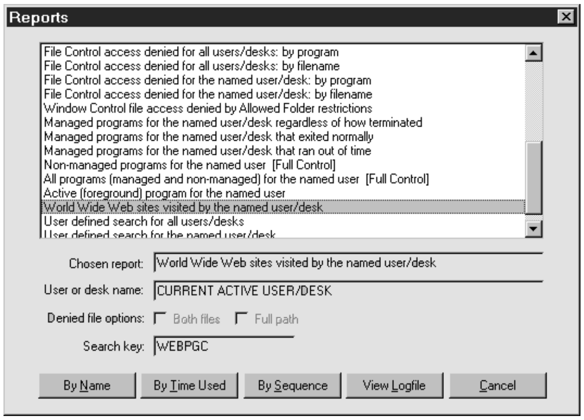
Shutdown / Logoff: *Logoff Current User* will log off from this Windows session. *Logoff WinU Desk* will immediately set the target computer to the default WinU desk. *Shutdown* and *Reboot* act the same on some computers. For those computers that can handle the distinction, both choices are provided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

Send popup message to user: Often, in conjunction with taking some action you'll want to send a popup text message to the affected WinU or Full Control computer users on the network. To do this, type your brief message (150 characters or less) here. The message will pop up on the user's computer before any other specified action is done. So, for example, the user will get to read the attached message before the computer is shut down. Those big-font popup messages time out in two minutes, so if no user is at that particular computer, there will be very little delay.

Remote File/Folder Listing: Use this to list the files and subdirectories contained in a particular folder on the target computer. The results are displayed in alphabetical order, much like the DOS *dir* command.

Empty the logfile: It's sometimes handy to be able to remotely reinitialize the logfile. If you like, you can also save a backup copy of the logfile before it is emptied. Give the folder to save the backup into. The filename of the backup is unique, so you can save all your logfile backups to the same place if you prefer.

Administration Manager Reports



File Control access denied for all users/desks: by program
File Control access denied for all users/desks: by filename
File Control access denied for the named user/desk: by program
File Control access denied for the named user/desk: by filename
Window Control file access denied by Allowed Folder restrictions
Managed programs for the named user/desk regardless of how terminated
Managed programs for the named user/desk that exited normally
Managed programs for the named user/desk that ran out of time
Non-managed programs for the named user [Full Control]
All programs (managed and non-managed) for the named user [Full Control]
Active (foreground) program for the named user
World Wide Web sites visited by the named user/desk
User defined search for all users/desks
User defined search for the named user/desk

Chosen report: World Wide Web sites visited by the named user/desk
User or desk name: CURRENT ACTIVE USER/DESK
Denied file options: □ Both files □ Full path
Search key: WEBPGC

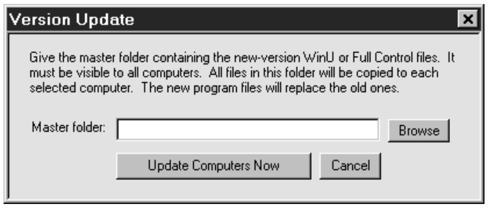
These reports can be run from the Administration Manager to show activity on the remote computer. They are essentially the same reports that can be run against a local computer from the System Setup screen's Reports tab, and are described in detail on the Usage Tracking Reports page.

As with all the Administration Manager options, you can select as many computers as you want on the main Administration Manager screen. A report will be run against each selected computer. So, for example, if you select a report on "all users" or "all desks", each computer's report will display information on all the Full Control users or WinU desks known to that one specific computer. Similarly, when running "per-user" or "per-desk" reports from the Administration Manager, the User Name is set to CURRENT ACTIVE USER/DESK indicating that the report will display information about the active Full Control user or WinU desk currently logged in to that computer.

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

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

Administration Manager Version Update Control



Give the master folder containing the new-version WinU or Full Control files. It must be visible to all computers. All files in this folder will be copied to each selected computer. The new program files will replace the old ones.

Let's say you have a new-version update of WinU or Full Control and you want to install it on all your current managed computers. You can't simply run the installer, because WinU or Full Control is already running, and it might not allow an installer to run on that computer. Also, Windows won't let you overwrite a running program. So how do you update all your computers?

Here is how to do this. First, copy all the new-version files to a visible shared directory on your file server. Make sure these are the only files in the directory. The Administration Manager's computer must have read/write access to this directory, but your users just need read-only access.

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

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

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

The only exception is ".sys" files under NT/2000/XP/Vista/Win7. Instead of being copied to the "home" directory, they will be copied to the target computer's designated Drivers directory. This user must have permission to do so. See below for more on this.

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

NT/2000/XP/Vista/Win7 Drivers: To update the Bardon NT/2000/XP/Vista/Win7 driver files, the currently logged on user must have permission to copy files to NT/2000/XP/Vista/Win7's System32\Drivers directory and overwrite files already there. Members of NT/2000/XP/Vista/Win7's "Administrators" group generally have this privilege; other groups may also, depending on your NT/2000/XP/Vista/Win7 setup. If these files need to be updated remotely, arrange for the user to be logged in to an account with appropriate privileges when you do the Version Update.

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

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

Logoff And Shutdown Applets

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

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

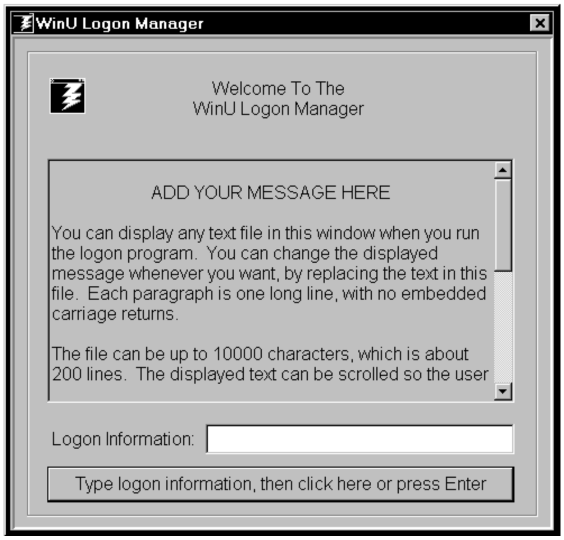
These are installed into WinU's section of the Start menu so you will always have Logoff and Shutdown menu items. Don’t worry, if WinU is running they first require a password.

WinU Extended Administration Kit

The WinU Extended Administration Kit includes the Logon Manager, Password Manager, and WinU Timer utilities. These optional tools extend WinU's capabilities. This add-on toolkit is available from Bardon Data Systems.

These tools are described briefly below. Full documentation is included with the Extended Administration Kit.

Logon Manager



ADD YOUR MESSAGE HERE

You can display any text file in this window when you run the logon program. You can change the displayed message whenever you want, by replacing the text in this file. Each paragraph is one long line, with no embedded carriage returns.

The file can be up to 10000 characters, which is about 200 lines. The displayed text can be scrolled so the user

Would you like to set up WinU so users have to log on to a desk with their own individual name/password combination? That's what the Logon Manager program is for.

Generally, people set up WinU to run the Logon Manager when the user clicks on a WinU button. It can also be run in an autologon mode.

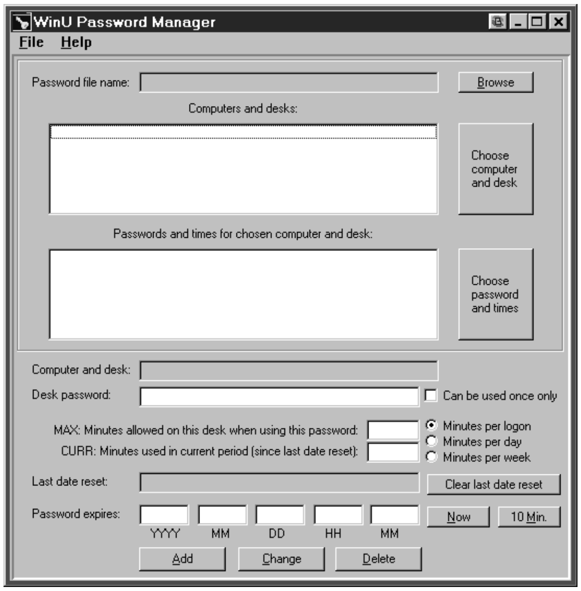
Virtually everything it displays can be customized to your needs. It can show your specified policies text in its scrolling window. After reading this, the patron types in the logon information (name, authorization number, or whatever you choose) and presses Enter or clicks the displayed button.

The typed information is passed to your customized validation function in VALIDL.DLL. A sample VALIDL.DLL is included to demonstrate how it works.

If the validation function accepts the information, the logon program asks WinU to switch to the target desk. If this WinU computer is set up for logging to file, a ULOGON record is written to the logfile containing the validated logon information (as typed in by the user, or specified by the validation routine).

The Logon Manager is part of the WinU Extended Administration Kit, which is available to WinU users from Bardon Data Systems. Its full documentation is included there.

Password Manager



We include the Password Manager program for the convenience of those users upgrading from older versions of WinU. You can probably meet your needs better with the Administration Manager.

The Password Manager allows the administrator to add or change passwords in a central password file. Manipulating this file lets the administrator dynamically control access to all desks on all WinU computers on the network.

The Password Manager is part of the WinU Extended Administration Kit, which is available to WinU users from Bardon Data Systems. Its full documentation is included there.

WinU Timer

The timer program lets you run an application or command at a particular time. It can run the command every day, every weekday, every weekend day, once a week on a specific day of the week, or once a month on a specific date of the month. It runs these commands through WinU, and is designed for situations where is would be inappropriate or difficult to run them through the Windows task scheduler.

The timer program is part of the WinU Extended Administration Kit, which is available to WinU users from Bardon Data Systems. Its full documentation is included there.

Appendix A

File Formats

Log File Formats

WinU 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*, WinU records all actions to a log file in a more or less "human-readable" format. If *CSV format* is chosen, WinU 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 WinU'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, n, computer, desk, app, msg
```

The comma-separated values records are of this form:

```
"dd","mm","YYYY","HH","MM","SS","nnn","ffffff","n","computer","desk","app","msg"
```

The abbreviations used in the above description forms are:

dd	two digit day (01-31)
mm	two digit month (01-12)
YYYY	four digit year (ex: 1997)
HH	two digit hour in 24 hour time (00-23)
MM	two digit minute (00-59)
SS	two digit second (00-59)
nnn	three digit current desk number (1-500)
ffffff	six-character "action flag" code (see below)
n	usually, minutes in program, desk or session (see below)
computer	the computer name of this WinU machine
desk	current desk name (text)
app	usually, the button title of this 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
ADMCLU	R	Administration Manager changed clone update settings
ADVSRY	S	Advisory message, or internal action flagged
AMQUIT	S	Administration Manager is exiting
BADPWA	S	Invalid biometric validation or password for drag-drop file program add
BADPWC	S	Invalid password for Ctrl+Alt+Del
BADPWD	S	Invalid biometric validation or password for desk setup
BADPWH	S	Invalid biometric validation or password for Help
BADPWI	S	Invalid biometric validation or password to add desk
BADPWJ	S	Invalid biometric validation or password to copy desk
BADPWK	S	Invalid biometric validation or password to delete desk
BADPWL	S	Invalid biometric validation or password for desk logon
BADPWM	S	Invalid biometric validation or password for setup mode
BADPWP	S	Invalid biometric validation or password for program launch
BADPWR	S	Invalid biometric validation or password for reports

BADPWS	S	Invalid biometric validation or password for system setup
BADPWU	S	Invalid password for external security level upgrade
BADPWV	S	Invalid biometric validation or password for reset mode
BADPWX	S	Invalid biometric validation or password for WinU exit
BDCKPT	D	Could not save desk time checkpoint
CHGDSK	D	Leaving Desk M (DeskName) - Entering Desk N
CHPWDD	S	Desk Password Changed
CHPWDE	S	Used emergency password to gain access
CHPWDF	S	Desk Password File Name Changed
CHPWDP	S	Program Password Changed
CHPWDS	S	Setup Password Changed
DENACC	S	Access denied (web browser, task manager, etc)
DRVACC	S	Drive access denied by USB port/drive restrictions
ENDAPT	M	Application Terminated Due To Program/Desk Timeout
ENDAPU	M	Application Terminated By User
ENDSES	S	End Of WinU Session
ESETUP	S	Entered Setup Mode
FGPRGM	M	Active (foreground) program
FILACC	S	File Control access denied
FILACD	S	Window Control file access denied due to Allowed Folder restrictions
MALACC	S	File access denied by Malware restrictions
MALcnn	X	Malware-related action (see below)
STRAPP	Z	Managed Program Started
STRSES	Z	Start Of WinU Session
TBMOVE	S	User tried to move taskbar: not allowed
TBTERM	S	Session terminated: taskbar move not allowed
TBWARN	S	User warned: taskbar move not allowed
TIMDSK	D	All Applications Terminated Due To Desk Timeout
ULOGON	T	User Logon (generated by Logon program)
USRNMW	S	Logon name of user
WCCAPP	Z	Window Control closed an application
WCCDLG	Z	Window Control closed a dialog
WCCSOF	Z	Window Control "soft-closed" a window
WCKEYS	Z	Window Control sent keystrokes to a window
WCNULL	Z	Window found by Window Control (do nothing)
WCSDIR	Z	Window Control set a window to a directory
WCSFIL	Z	Window Control auto-generated a filename
WEBBRN	Z	A new Web brower 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
XSETUP	S	Exited Setup Mode

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

```
S: minutes in session
D: minutes in desk
M: minutes in program
R: remote setup information
T: logon program switched WinU to this target desk number
W: minutes in browser window (WEBBRX) or at website (WEBPGC)
X: internal index (see below)
Z: will always be zero for this record type
```

For ULOGON records, the App field contains the text typed into the WinU logon program by the user. If you have set up to do so, this text may have been massaged by your site-specific validation function.

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

For MALcnn records, c is the A-R letter group on the What To Monitor list, and shows what category or action was triggered. The nn part is a two digit internal index which gives more detail about the particular file or registry entry that triggered this action as listed on the What To Monitor page.

Appendix B

Miscellaneous

Software License and Warranty

SOFTWARE LICENSE AGREEMENT

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

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

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

b) Purchased Licenses. Upon your purchase of the Software license, Licensor grants you and you accept a non-exclusive license to use one (1) copy of the software, on one (1) computer, and make one (1) copy of it for archival purposes. For purposes of this section, "use" means loading the Software into RAM, as well as installation on a hard disk or other storage device.

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

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

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

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

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

Unauthorized copying of the Software or failure to comply with the above restrictions, will result in automatic termination of this Agreement. Unauthorized copying or distribution of the Software constitutes copyright infringement and may be punishable in a federal criminal action by a fine of up to U.S. $250,000 and imprisonment up to five (5) years. In addition, federal civil remedies for copyright infringement allow for the recovery of actual damages based on the number of copies produced or statutory damages of up to U.S. $100,000 for willful copyright infringement.

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

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

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

5. LIMITATION OF LIABILITY. THE LIMITATION OF LIABILITY IS TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL LICENSOR OR ITS SUPPLIERS BE LIABLE FOR DAMAGES, WHETHER ARISING IN CONTRACT OR TORT AND INCLUDING, BUT NOT LIMITED TO, ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION OR OTHER DATA, COST OF COVER, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR THE FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF LICENSOR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. YOU ACKNOWLEDGE THAT THE LICENSE FEE AMOUNT REFLECTS THIS ALLOCATION OF RISK. IN ANY CASE, LICENSOR'S ENTIRE LIABILITY UNDER ANY PROVISION OF THIS AGREEMENT SHALL BE LIMITED TO THIRTY PERCENT (30%) OF THE LICENSE FEE AMOUNT ACTUALLY PAID BY YOU FOR THE SOFTWARE. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

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

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

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

9. Governing Law/Jurisdiction. This Agreement shall be governed by and construed under the laws of the State of California without reference to principles of conflicts of laws. Any action or proceeding brought by either party against the other arising out of or related to this agreement shall be resolved exclusively in the appropriate state court in Alameda County, California or federal court for the Northern District of California, U.S.A. You consent to exclusive jurisdiction in such venue and expressly waive any objection to same.

10. General. This Agreement sets forth the entire agreement and understanding of the parties relating to the subject matter herein and

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

Notices

VERSION: WinU version 7.0

SYSTEM REQUIREMENTS: Requires Windows 95/98/ME/NT/2000/XP/Vista/Win7/Vista/Win7.

TECHNICAL SUPPORT: For technical support, contact Bardon Data Systems through email (support@bardon.com), the World Wide Web (http://www.bardon.com), fax (510-526-1271), or telephone (510-526-8470).