

WinU and Full Control

Description and Technical Walkthrough

BARDON
DATA SYSTEMS

Introduction

This document provides a screen-by-screen walkthrough of WinU and Full Control, system management and security oversight products from Bardon Data Systems. It shows how to quickly set up and start using these products to provide system stabilization, real-time oversight, audit trail activity logging, and centralized remote administration. WinU also offers a *Simplified Replacement User Interface*. We'll look in detail at WinU, the Remote Administration Manager, then briefly at Full Control. Most of what we'll say about WinU also applies to Full Control.

Overview

WinU and Full Control are tools for remote administration, security, and management of computers, typically in a workplace. System administrators put WinU or Full Control on their managed computers so they could be centrally administered. This saves the administrator the work of running around to all those computers and managing them one by one. And a lot of that management is automated; the administrator just sets the policies which WinU or Full Control automatically implement.

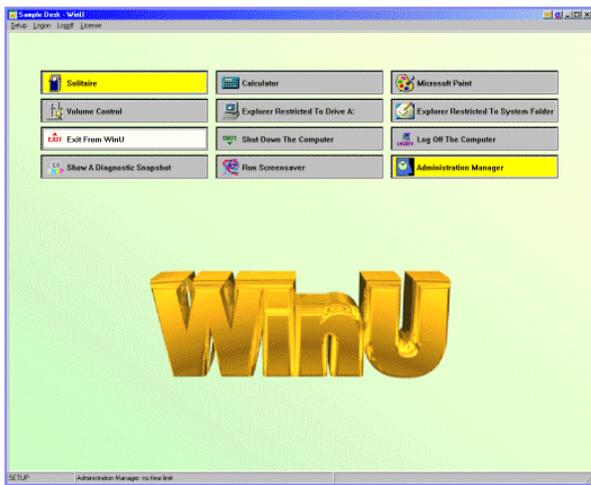
WinU and Full Control both provide system security, oversight, and remote management. The difference is that WinU also includes a *Simplified Replacement User Interface*, which replaces the regular Windows interface (taskbar, Start button, desktop icons) with simple, obvious labeled buttons against a clean background that you can design. This makes WinU very useful for novice users, public computers, task stations, etc. By contrast, Full Control is designed to provide oversight in the regular Windows interface (taskbar, Start button, desktop icons) so it's good for experienced Windows users and for situations where you want to present the regular "look and feel" of Windows.

Other than how they handle the interface, WinU and Full Control work in the same way. The setup screens are very similar, so after you learn one product you can administer both of them. After we go through WinU in detail, we'll talk about Full Control, and the differences between them.

WinU or Full Control do constant real-time oversight of what program windows are coming up and how they are being used. Whichever one you choose to use, it acts as an active real-time management agent running behind the scenes, watching what's going on. This provides a lot of advantages. It can provide an audit trail of what programs the user was in, and for how long. Browser-based applications can't bypass it, either. Maybe the user thinks "I'll just bring up a web browser and use Hotmail or Instant Messenger, so my messages won't go through the company's audited email system." With WinU or Full Control, those will show up too. All this is possible because we monitor in real-time everything that is going on.

A real-time audit trail is a powerful management tool. Standard management is to know what your people are doing so you can guide them into where they need to be. But how does a manager, looking across a sea of computers, grasp what all these people are doing? What if, through Bardon's reports, each manager could manage more people? Costs go down, productivity goes up. Another advantage is the ability to provide a written audit trail report for legal reasons, for example in sexual harassment issues or employee productivity issues.

WinU



Let's launch WinU. Notice how it fills the screen. No taskbar, no Start menu, no desktop icons. Just labeled buttons.

This is WinU's *Simplified Replacement User Interface*, which makes a computer with WinU very easy to use, even for novices.

The administrator can set up the WinU desktop layout in lots of different ways. This illustration shows the default "WinU" background wallpaper. But you can change the background to anything you want. You can also change the menu bar, what's on the buttons, the colors, icons, all sorts of things.

You can set it up to show the task bar at the bottom, if that's what you want to do, but generally people don't. Instead, they have WinU as a *Simplified Replacement User Interface*. The labeled buttons make it very obvious what programs people can run. Even novices can use it. Everybody that has a doorbell knows what you do with a button. It keeps training costs to an absolute bare minimum, because we've taken the Windows interface and we've cut out all the parts that confuse novices. This keeps maintenance costs low too.

To use a program, click its button. This launches the listed program. WinU tracks that program in real-time as it runs. You can have WinU log all activity, prevent access to Control Panel or other system components, limit that program's access to the file system, and more. The programs that you start from WinU buttons can be time-limited or controlled in other ways. And of course you can limit the actual files or programs that this user can access.

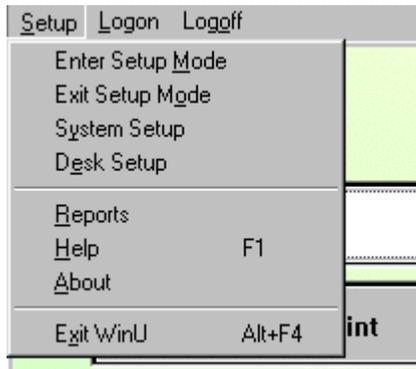
Meanwhile WinU is also on the alert for malware, spyware, trojans, and similar nasties that can sneak into your system, adding multiple layers of defense to your computers. And there's more. For example, Control+Alt+Delete and similar keys are also under our oversight. You can lock it down further, or open it up further. This is just the default sample configuration. There are lots of options.

WinU divides the presentation into multiple desktops (screens of buttons). There can be dozens or hundreds of linked desktops, and if allowed, the user can switch between them. Desktops can have passwords and other limits, so only certain people can get to them, perhaps only during certain times of day. Desktops simplify the presentation of what you want, and eliminate the presentation of what you don't want.

WinU can oversee the Windows logon too. It's easily bypassed, especially in Windows 9x where you can just hit Escape and log on as somebody else, or create a new logon on the fly. But when WinU is running you can't do that. Escape won't bypass the logon, and you can't use a logon name that hasn't already been set up. If you validate through your network, we work with and enhance any validation from the server. WinU can also do logon oversight on standalone computers like laptops.

Setup Options

Let's look at WinU's setup options. Click Setup on the menu bar. Using our Kiosk Mode options, you can hide the menu bar for a cleaner look, in which case click the System menu (the W at the left side of the title bar) and use the Setup options from there.



The menu bar has three entries: *Setup*, *Logon* (to a WinU desk), *Logoff* (to the default WinU desk).

Most of the Setup menu entries are self-explanatory.

Exit WinU is password protected; only administrators can exit.

About is the usual About box.

Help is designed for administrators, not end-users, so it is also password protected. In fact, when installing you can specify that the

Help information not be installed at all.

Reports is just a shortcut into the Reports section of the System Setup screen (which we'll see in a minute), so it's a quick way to run reports.

Enter Setup Mode and *Exit Setup Mode* control access to the password protected Setup Mode where the administrator can change the WinU settings.

So there are really only two menu options to know: *System Setup* and *Desk Setup*.

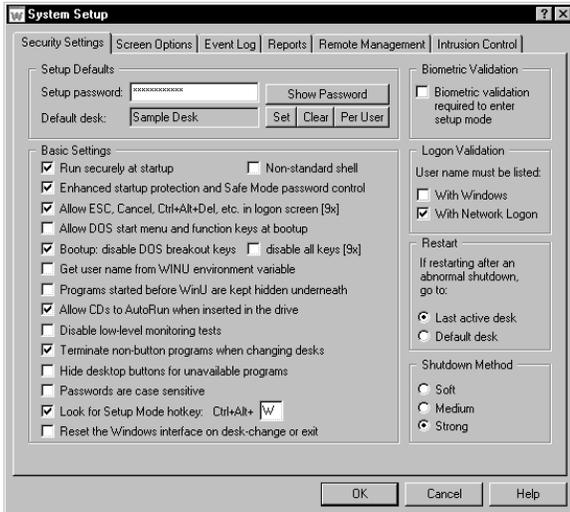
Desk Setup is where you give the per-desk settings. A desk's settings are used when a user switches to that desk. We'll look at them in a minute.

System Setup is where you give the overall settings that will apply to the entire WinU session, to all desks. Let's start there. I'll click the *System Setup* menu item. This will display the System Setup screen.

System Setup Screen

The System Setup screen has six tabs: Security Settings, Screen Options, Event Log, Reports, Remote Management and Intrusion Control. The Security Settings tab has general options. The other tabs have specific purposes. Let's start on the Security Settings tab.

Security Settings Tab



At the top of this tab is where you can change the administrator's password, and set the Default Desk. You can also set up here to use biometric authentication.

Next are the Basic Settings. These are general setup options.

Check the first box to Run securely at startup so WinU will automatically start every time the computer starts. This is a secure start, it doesn't use the StartUp folder, so it can't be bypassed.

For the strongest protection at startup, also check the Enhanced startup protection and Safe Mode password control box. With this box checked, your oversight kicks in

even before the Windows desktop starts. This lets us manage the actual logon process, and password-protects Safe Mode.

Non-standard shell is if you use a system shell other than the regular Windows shell. Most people won't need to use this option.

The next box will Allow ESC, Cancel, Ctrl+Alt+Del etc. in logon screens. This is a big issue in Windows 9x where hitting Escape or Cancel or Ctrl+Alt+Del at logon isn't handled by the operating system. (NT, 2K, and XP handle this itself, so we don't need to do it there.) In 9x those keys can totally bypass the logon process, allowing invalid program launching and system reconfiguration. Most administrators would love to enforce a valid logon under 9x. Well, here is how to do it.

Allow DOS start menu and function keys at bootup applies mainly under 9x because NT, 2K, and XP don't run DOS underneath. We've paid a lot of attention to Windows 9x because that's a less expensive operating system than NT, 2K, and XP. What we provide is the option of layering our oversight utility on top of the cheaper operating system and getting what you need. Contrast this with the typical Microsoft solution, which will be to blow away your hard disk, install XP, then reinstall all your applications, put back all your data, and hope everything runs. You can see that our solution is not only cheaper, but easier to set up. You don't have to reinstall anything, and you don't have to reconfigure anything.

Similarly, you would disable DOS breakout keys or disable all keys to ensure that nothing in your 9x autoexec startup process can bypass Windows and stay in DOS.

For older networks that don't understand where Windows keeps the logon name, we offer the option of grabbing the name at logon, then putting it into an environment variable and letting Full Control get

to it from there. Check Get user name from WINU environment variable if you have an older network that needs this. Usually this is done in a logon script. As we move forward into the future and those old networks get rarer, this particular feature will be used less and less. But it's still there. What you'll find is that we have options which can handle pretty much anything. There is no such thing as a standard version of Windows, and we have many ways of doing everything to ensure that we can handle as much as possible.

Check Programs started before WinU are kept hidden underneath if you will be running programs before WinU launches and want to ensure that the user can't access these programs, for example system-level utilities that automatically run at startup. If the user tries to Alt+Tab to such programs, the windows will be pushed underneath WinU again. However, remember that these programs will not even be able to display a message dialog, so you should only check this box if you are sure that your programs will never need to interact with the user.

Allow CDs to AutoRun when inserted in the drive. Some people want to do that, some people don't. When you put a CD in the drive, the standard Windows behavior is to run that CD's program. If you don't check this box, AutoRun won't work. That is, if you put a CD in the drive, it doesn't AutoRun.

(By the way, on the Desk Setup screen we also offer the ability to lock the CD into the drive. Let's say you've got a booth at a tradeshow, and you've got your product CD in your demo computer's CD drive. Now, how many thousands of CDs do you think you're going to need to take with you to keep replacing the ones that people walk away with by popping them out of the CD drive and putting them in their pocket? If you use WinU, you're going to have to take with you just one CD. Or in any kind of public access situation, or in a school or library, if you're allowing use of a CD to the public, the CD won't walk away.)

The ability to Disable low level monitoring is a diagnostic tool that we have available when you're working with Bardon tech support to isolate certain issues. In general, leave that unchecked.

Terminate non-button programs when changing desks controls whether a program that was started through other means than clicking a WinU button should be closed when exiting the current desk.

Hide desktop buttons for unavailable programs - if a program is not available from this computer 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 case sensitive - they can be case sensitive or not, as you choose.

Press the setup mode hotkey and WinU asks for the password. If you give it, WinU will go into Setup Mode. The default hotkey is Ctrl+Alt+W, but you can set it to anything you want.

Reset Windows interface on exit because under Windows 98 in order to get the full interface back that we locked down, you need to restart the interface, and we have come up with a way of doing that without a reboot. Most of the time you won't need this, though.

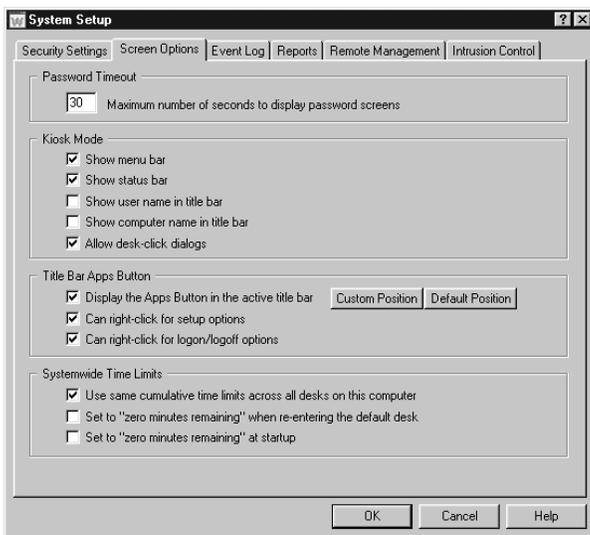
The next section of the Security Settings tab is concerned with Logon Validation. Earlier, I mentioned this logon validation mechanism where we can make sure you're validated with your server. We can also validate for peer-to-peer networks. Even a standalone Windows 95 machine, which is known for having pathetic security, you can't log on unless you're you.

Use the Restart options to control what happens if WinU is restarted after being shut down in a way it shouldn't (for example, turning off the computer's power switch). Should it go to the last active desk at the next restart, to pick up where it left off? Or to the default desk instead?

There are various ways to shut down a computer. Shutdown Method lets you select which is best in your situation. We recommend that you use Strong Shutdown, but you can always change it to one of the other methods if necessary.

Screen Options Tab

The, Screen Options tab controls systemwide display settings. (Other screen settings are per-desk, and are set on the Desk Setup screen.) WinU provides a *Simplified Replacement User Interface*. The administrator designs the interface, and the user can't change it. Compare this to regular Windows, where the user can move, change, and delete things. WinU ensures a consistent look and feel to your machines.



The first option is Password Timeout. When a password screen appears, how long should it display before WinU closes it? By default, after 30 seconds if you don't give a password, the screen closes.

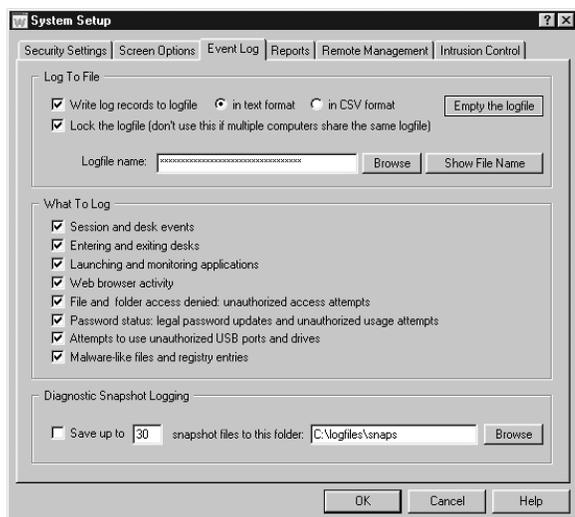
We have five options grouped under the Kiosk Mode section. You can hide the menu bar that's at the top of the WinU screen, with Setup, Logon, Logoff, etc. You can hide the status bar at the bottom of the screen, that shows time limits and active program. In the title bar, do you want to display the currently logged-on username? The computer name? Here's where to set that up.

Do you want to allow the user to click on the WinU desktop to bring up certain kinds of dialogs? On some setups those desk-click dialogs are handy. On others, the administrators would rather not have them, because they bring up dialogs that are inappropriate in that situation. It's up to you.

The next section controls the Title Bar Apps Button. What's that? When WinU is running, by default it puts a little W button in the upper right corner of the current active program. But you can turn this button off if you prefer. If allowed, left clicking on the Apps Button will list the programs that can be run from this WinU desktop. The programs can also be run from the button list, handy if the user is already running a program that is taking up the whole screen. And, if allowed, right-clicking on the Apps Button gives an administrative menu with password protected setup options.

The last section controls Systemwide Time Limits. Usually, each desktop has its own time limits, and when moving to a different desk, the next desk's time limits start. But what if you want the desk time to be cumulative, to allow the user to access any desk on the computer, and move between them for, say, one hour, allowing the user to switch desks during that period? With Systemwide Time Limits, the time keeps counting down as if it was all one big desk. Many public installations use this option.

Event Log Tab



The Event Log tab controls what events are being logged and where the log is saved.

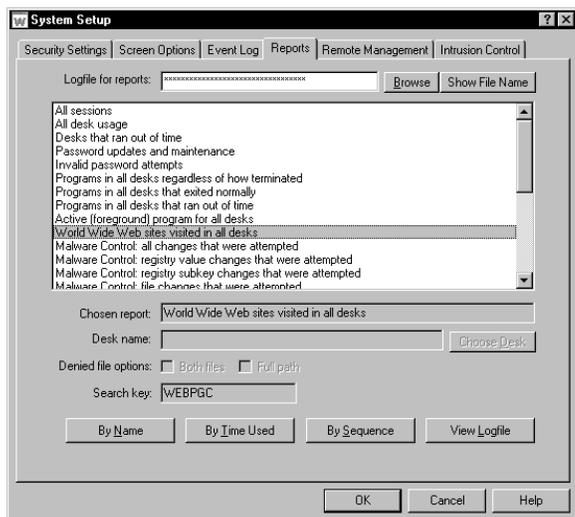
Locking the log file is something most people do but I'll give you an example of when you don't want to lock the log file. In general we recommend that each individual machine have its own log file. This gives you the ability to look at the events that happened on a particular machine, as well as on what happened on all machines taken together. Easy to do, it's a two-line batch file to take all of your log files and mush them together. If you have separate log files, you should lock the log file. But if you have one log file for a hundred different machines, you don't want to lock the log file, because everybody's getting at it. So that's why we give you the option.

You can also log in multiple formats, depending on where you are going to export it to. For example CSV format, comma-separated values, is good for importing into a database or spreadsheet. Most of the rest of the tab is what kinds of events to log.

And then at the bottom we have our Diagnostic Snapshot logging, which is a very interesting tool. You can set up, with the Diagnostic Snapshot logging, to save a minute-by-minute record of everything that was happening on the machine, down to the lowest levels, even the things that don't show up when you hit Ctrl+Alt+Del, including DLLs that are loading, system processes, in great detail.

Why would you want to do this? Well, let's say you have a machine that keeps crashing erratically, you don't know why, something funny is happening. Wouldn't you love to be able to look at a post-mortem log of everything that was going on, on that machine, leading up to the crash? Well, that's what a Diagnostic Snapshot log gives you.

Reports Tab



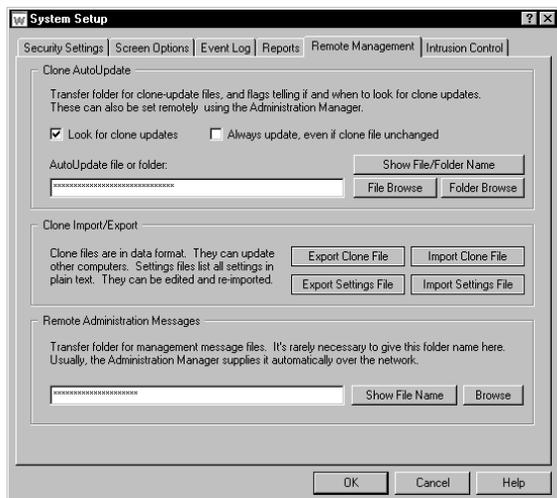
As you can see on the Reports tab, we've got dozens of different predefined reports.

If these aren't enough, you can run user-defined reports. In addition, you can view the raw logfile, or import it into your favorite spreadsheet or database, allowing you to run custom reports on any kind of query you want to.

Reports can be displayed according to a number of criteria. They can be systemwide or per-group, with or without certain details, and sorted in various ways.

The user-defined report work with events not covered in one of the predefined reports.

Remote Management Tab



There are three sections to the Remote Management tab: AutoUpdate, Import/Export, and Administration Messages.

It's worth noting, though, that on the Remote Management tab, it's not necessary to set most of these options yourself.

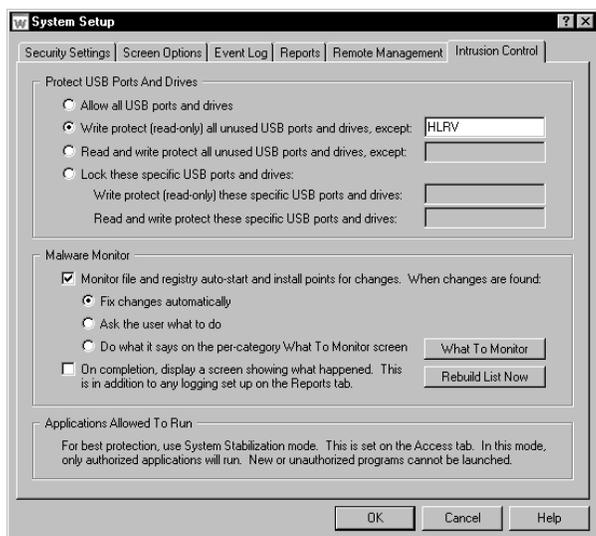
This is because the Clone AutoUpdate and Administration Messages fields can be set by the Remote Administration Manager from across your network. The Administration Manager can broadcast its preferred settings to the client.

That leaves just the Import and Export buttons. In WinU, the setup and configuration tools are part of the client. To set up WinU you install the client on one machine, use these

setup tools to configure that machine, then export a clone data file from that machine. That file has all the setup choices you've made. Send it to the clients and they all get those same settings. There are many ways to send it to the clients.

Each machine's client includes all the setup screens. So if you find that one particular client is acting funny you can go into setup mode on that one machine and fix it on the spot. You don't have to go back to your desk, make a change, then bring it back over to the client.

Intrusion Control Tab



The last tab on the System Setup screen is the Intrusion Control tab. The Intrusion Control tab stops malware, spyware, trojans, data theft, and similar threats.

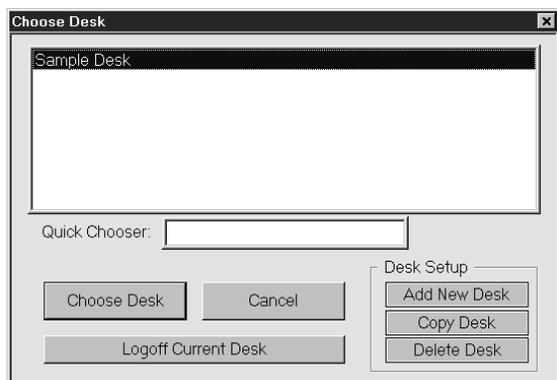
There are two sections to this tab. With the top section, you can lock USB ports (and actually, any other local drives such as CD or DVD writers). The drives can be set as read-only or completely invisible and unusable. This can go a long way to preventing data theft. It can be set to scan at startup 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.

The bottom section is our Malware Monitor. Malware is anything you (the administrator) don't want to 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.

When a problematic program is found, it can be logged, stopped, deleted, whatever you want. There's also an Advanced screen where you can set up to handle different kinds of threats in different ways.

Choose Desk Screen

In WinU, programs are run from desks. A "desk" is simply a screen full of labeled buttons. The administrator can customize the desk layout and settings. Each desk can have its own background image, buttons, security permissions, and other settings.



The user or administrator uses the Choose Desk screen to go to a desk. The administrator also uses this screen to add, copy, or delete a desk.

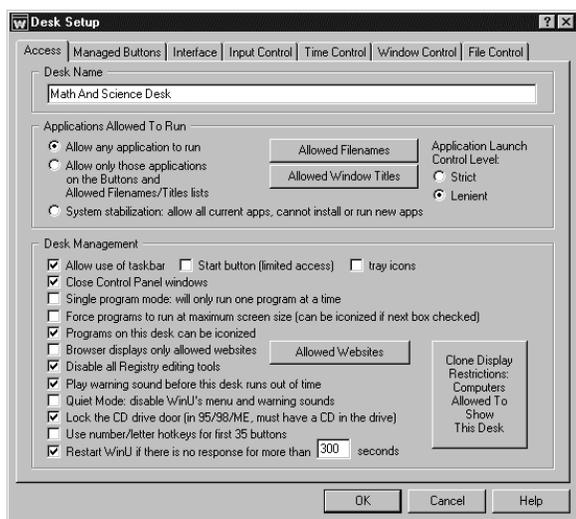
The buttons on a desk have labels and icons. Their color can be either the standard Windows gray or any other color. They can be in the bottom half of the screen, with an image in the top half of the screen, or the image can cover the entire WinU screen, with the buttons arranged in front of the image. You can display the buttons with a text label, or just as an icon, with no label.

There are many ways to add a button to a desk. Probably the simplest is to drag and drop a file or program from Explorer or the Windows desktop onto the WinU desktop. The administrator can do this but the user can't add a button. In fact, the user can't change the WinU desktop at all.

When you first install it, WinU creates a sample desk. Let's look at the settings for a desk. On the Setup menu, choose Desk Setup, or right-click on the desk itself, or on a button. Then give the password. This puts WinU into Setup Mode and displays the Desk Setup screen for the current desk. If you prefer, use the Choose Desk screen to display a different desk.

Desk Setup Screen

Access Tab



The first tab on the Desk Setup screen is the Access tab. Here's where you set the desk name.

While on this desk, what applications are allowed to run? Of course, the programs on the desktop buttons will run, but what else? You can allow specific Window titles, specific file names, control things at a very fine level of detail. The "System Stabilization" option here is especially powerful. With one click, all programs currently on the computer are allowed, but no new programs can be installed or run.

(The programs on the buttons, which the user can launch, are listed on the next tab, Managed Buttons. The programs listed here are the ones that will be allowed to run if they are launched in some other way, perhaps automatically by a button program.)

By the way, this is a very good complement to our Intrusion Control options. By combining System Stabilization with our Intrusion Control oversight, you can set up a very strong defense against viruses, malware, spyware, Trojans, adware, browser hijacks, and other sorts of nasties. It catches attacks that traditional tools like firewalls and antivirus often miss.

As with the System Setup screen, the first tab of the Desk Setup has a number of general options, while the other Desk Setup tabs control specific targeted capabilities.

The Desk Management options control various settings. You can allow the use of the taskbar (by default WinU covers the entire screen and hides the taskbar). If you allow the taskbar, it sits at the bottom of the screen under WinU, so instead of having WinU cover all the screen, it covers almost all the screen. If you let the taskbar show, you can manage it in many ways, for example you can lock the Start button or the tray icons.

Check Close Control Panel windows if you don't want users accessing those, for example through Explorer.

If you check Single program mode, WinU will only allow the user to run one button program at a time. You'd use this if you want the active button program to be closed when the user launches another managed program, maybe to prevent users from letting programs pile up and forgetting they're there.

You can force managed programs to run at maximum screen size. Again, this will keep less proficient users focused on one program at a time. Similarly, you can ensure users can't iconize button programs. A WinU button turns yellow ("lit up") when its program is running, even if it's been iconized. Re-clicking a yellow button brings up the running program, it doesn't start a new copy.

Browser displays only allowed websites - this is handy in a public access situation or maybe a school, where you might have a list of websites, and you want to have them only be able to access those particular websites. You can list those sites here, and no other websites will work.

Disable all registry editing tools is self-explanatory. The registry is the system database, and if it gets messed up, you can turn your computer into a very large paperweight. Not a good idea.

Play warning sound before the desk runs out of time. You can set up a desk to have time control. You can give them a grace period, a warning period of so many minutes before their time expires. It can put up a box and say "hey, it's going to expire." You can also play a sound. But if you don't want that warning sound, un-check this box.

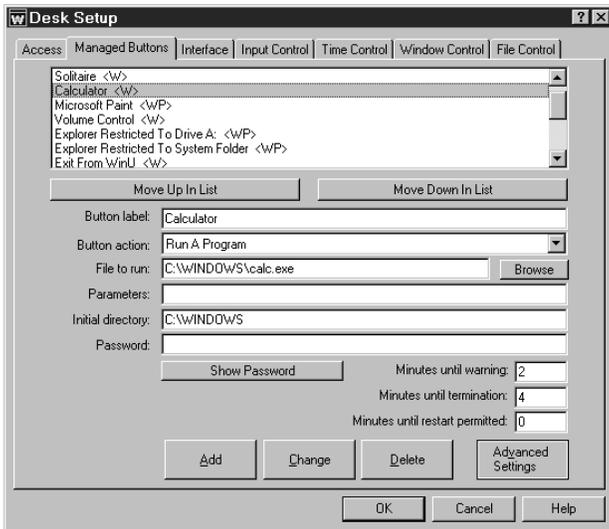
The Quiet Mode box is for if you don't want any sounds at all. It will disable all the WinU menu and warning sounds (not just the timeout warning sound). If you have a lot of computers, particularly all in a row in public, maybe you want to disable all the sounds.

Lock the CD drive door - if you have a CD in the drive and you don't want it walking away, check this box. Let's say you've got a booth at a tradeshow, and you've got your product CD in your demo computer's CD drive. Now, how many thousands of CDs do you think you're going to need to take with you to keep replacing the ones that people walk away with by popping them out of the CD drive and putting them in their pocket? If you use WinU, you're going to have to take with you just one CD. Or in any kind of public access situation, or in a school or library, if you're allowing use of a CD to the public, the CD won't walk away.

Use number/letter hotkeys to make it even easier for users to launch programs from WinU. The first 35 buttons are labeled 1-9 then A-Z. The user just presses one key to launch that program

Restart WinU if there's no response for more than so many seconds is one way WinU makes sure that nobody sneaks in and kills it. If you check this box, if WinU doesn't hear from its different components, which are always monitoring each other, it will restart and make sure that your computer is always protected.

Managed Buttons Tab



Next is the Managed Buttons tab. These are the buttons on the WinU desktop. You can have buttons to exit, logoff, start a screensaver, link to a particular desk, and a lot more. Choose the Button Action to specify this.

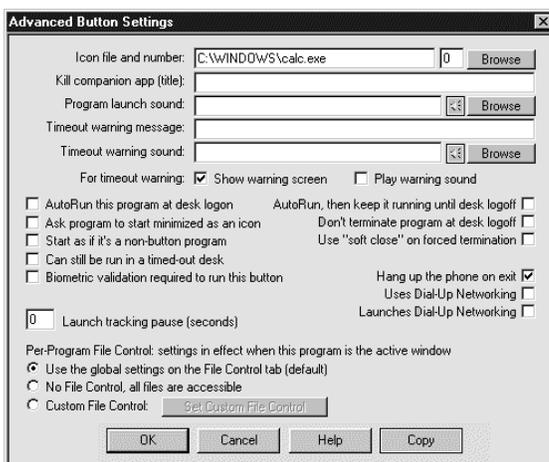
Of course, most buttons will launch programs. You can manage a program in many ways. You can give it a password.

You can give any button a password, or require biometric protection, which will be required to launch that program.

You can list how many minutes a program can run for, and how much warning the user gets before it is

terminated. You can indicate that after it exits (perhaps because it ran out of time), the user must wait before it will restart. This feature is very useful in public access situations.

Those are the basic options. There are advanced options too. You click on the Advanced button to set them. This brings up the Advanced Program Settings screen.



For example, you can have a program automatically start when a user logs on to this desk. Windows has its own Startup folder, but ours has more fine-grained control to it because of the way we've set up our users and desks. It's another way we can do things in a way that Windows doesn't offer.

We also have the ability to autorun a program and keep it running, so it will always be running during the entire desk session. You can't do that in Windows either.

Customized timeout warnings are handy. Remember we can have timeouts for various reasons. You can show a

timeout warning screen, play a timeout warning sound.

You can have it clean up after a modem, hang up the phone. If you do a Dial-Up Networking connection, say, with your web browser, yes, you can set up Windows so that it "connects to the

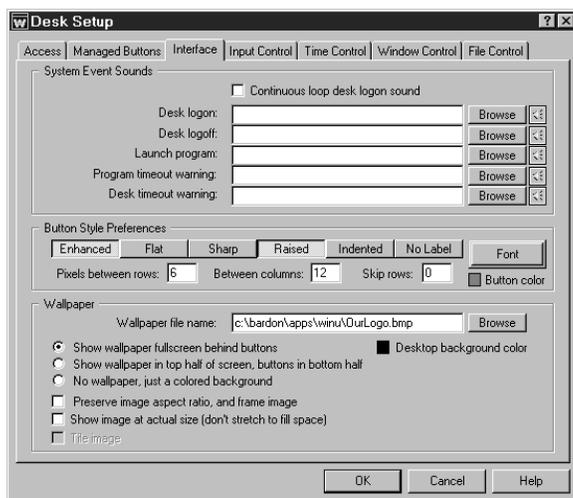
Internet as needed." But Windows won't disconnect when you're done. We add that capability.

Next there's an option saying that this managed button is allowed to run even if there is a time limit in effect and you've run out of time. Maybe there are certain things that you want to allow, some kind of management tools, for example, and this might be one of them.

We've got Per-Program File Control options. File Control lets the administrator specify ways to make parts of the file system available in different ways to different users. We'll talk about this more when we discuss the File Control tab.

For now, I'll just note that we can set up custom File Control settings per-program, so if you're running a particular program, you can have different file control settings. Let's say Word comes up. You can have different file control settings than when Excel comes up. That means you can see, open and read different files, you're forced to save to different places - depending on which program happens to be active.

Interface Tab



WinU has a *Simplified Replacement User Interface* which replaces the standard Windows interface (taskbar, Start button, desktop icons, etc.) with labeled buttons on a desk.

The Interface tab is where you set up how this desk should look - and how it should sound. You can have sounds that play when the user logs on to the desk, a looping logon sound that keeps playing if there are no programs running. That's used in public kiosks, to attract attention. There are also different sounds when the user logs off the desk, when the user launches a program, and for warnings.

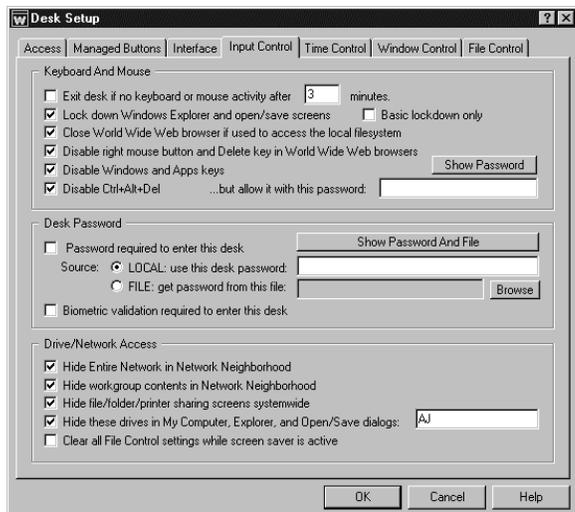
You can change the way the buttons look, give them different edges, colors, and fonts. For example, let's click the Button Color box and set a different color. And let's change the button style preferences, and put more space between the rows and columns. And we can skip some rows to push the buttons to a different place on the screen. You'll see that it looks quite different now.

And let's change the screen itself. Many administrators change the background wallpaper to an image that has their organization's logo. Often they show it fullscreen behind the buttons.

Here's an interesting technique. Want a button bar? Set the buttons to have No Label, set zero pixels between the rows and columns, and skip a few rows so the first buttons are at the bottom of the screen. Click OK, and there's the button bar. No labels, just a row of icons. That can be handy.

WinU is designed to be easy for people who are not graphic designers. They can create a very serviceable, pleasant screen without knowing anything about screen layout. We wanted to make it simple. Most people, all they'll need to do is drag and drop their programs or shortcuts onto the WinU desktop and let WinU automatically create their buttons. This gives administrators a fast way to generate a clean, easy interface, that's simple for their users to work with.

Input Control Tab



The next tab, Input Control, gives you the ability to handle user input. On the interface tab, it was system output. On the input control tab, it's user input.

What do you want to do about certain kinds of user input? Well, we can have an inactivity time out. A user that walks away from a logged-on computer will be logged out after the specified period of inactivity.

Lock down Windows Explorer, the desktop and Open & Save screens. If checked, WinU disables lots of things in Explorer, even from the keyboard. Delete, rename, cut, it also closes certain Explorer-related window titles like Options, Run, Find, etc.

Click the Help button to see the full details. Any time there's anything you're not sure of, click on Help to bring up our context-sensitive help screen for that tab.

Do you want to close World Wide Web browser if used to access the local file system? Check this box to prevent web browsers from showing files or directories on the local hard disk or network.

Many administrators disable the right mouse button and Delete key in World Wide Web browsers. The right mouse button in a browser can allow users to save programs to disk, set inappropriate pictures as Windows wallpaper, and change settings. Check this box if you don't want that to happen.

You might want to disable the Windows and Apps keys too. The Windows keys will bring up Explorer menus, system-level Property Sheets, and other screens that perhaps you don't want people to use.

Check the box to Disable Ctrl+Alt+Del to protect Ctrl+Alt+Del and the "close programs" or task manager screen. Or you can password-protect Ctrl+Alt+Del. If you password-protect it, when you hit Ctrl+Alt+Del it asks for a password. If you give the correct password, you can proceed. So, you can set up so your staff or your administrators can use Ctrl+Alt+Del but your regular users can't.

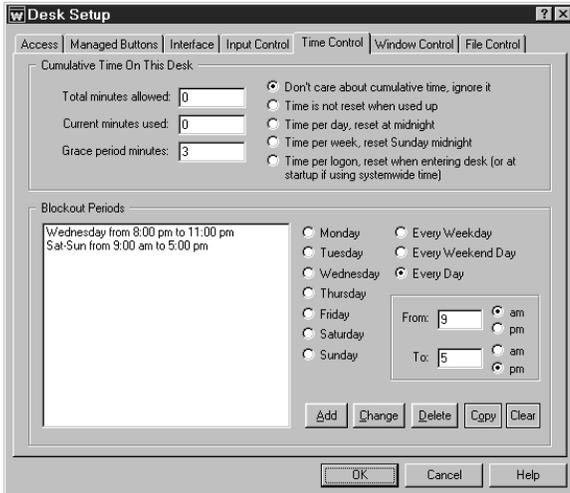
Next is the Desk Password section. Does the user need to give a password to enter this desk? You can set up biometric validation here too.

The next section is Drive/Network Access. Maybe you want to hide the computers that are listed in Network Neighborhood, if this is a public access machine where you don't want people to have access to the rest of the network. Or maybe you want to hide other things. You can even hide drives in My Computer, Explorer and Open/Save screens.

This way is actually not as strong as the way we provide in our Window Control, of forcing Open/Save screen to a particular location. But this one here is simple and easy to set up, and might cover enough for a lot of people. Actually, this is a setting that is provided with the Policy Editor, and we had people saying to us, "the Policy Editor gives us this, why don't you?" So we put it in. But it's not nearly as strong as the one we provide in Window Control.

Finally, there's a setting to clear all file control settings while the screen saver is active. There are certain screen savers we've run across that in addition to putting pictures on the screen, do antivirus scans or something like that. When those particular screen savers are active they want to have access to the whole machine. Fine, here's what they want in one easy check box.

Time Control Tab



The Time Control tab is where you set how long this user is allowed to use the desk, and during what times of day.

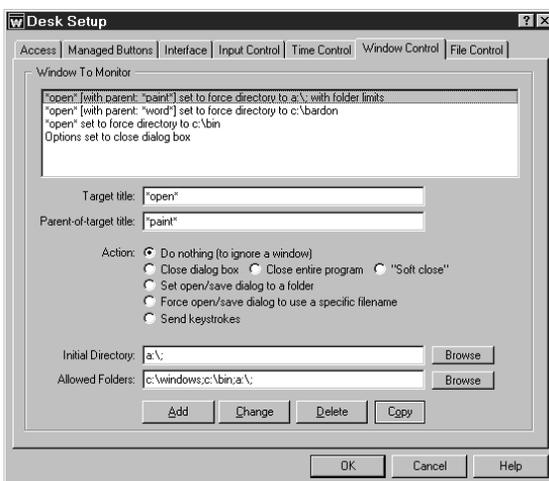
When setting the amount of time allowed, this can be time per day, per week, per session, etc. You can also set up a grace period, that is, how much warning they are given before being automatically logged off.

On the bottom of the Time Control tab you can set blockout periods. Blockout periods are times when nothing runs. Maybe you want to set thing up so nothing on this desk runs after hours, or perhaps you have a lab where a machine is supposed to be used only during certain periods of time. By setting up blockout periods for the

remaining times, no one can walk into the room and do things to that computer without supervision or control.

Remember, you can set certain Managed Buttons so they run even in a blockout period or on a timed-out desk. This is useful for "emergency" programs, perhaps programs that you have password-protected (through WinU) so only certain people can run them.

Window Control Tab



Window Control lets you list window titles, and when that window appears it is acted upon. You can list not only the main-window program titles but also titles of pop-up dialog screens, or web page titles, or folder titles, or anything that shows up in a title bar.

In addition to the title of the target window, you can also list the "parent of target" window title. You'd use this when you want to control a dialog from one particular program - in addition to the dialog's title, you'd list the main program's title as the "parent of target" title. This way, even if it has the same titlebar name as a window from another program, it will be treated differently. So for example you can control the Options screen in one program differently from the

Options screen in another program. You can also "do nothing" to a window, which lets you ignore it. It's a way of setting up "exceptions" to a general Window Control.

What can you do when you see a certain title? Say the user changes to a web page that you don't

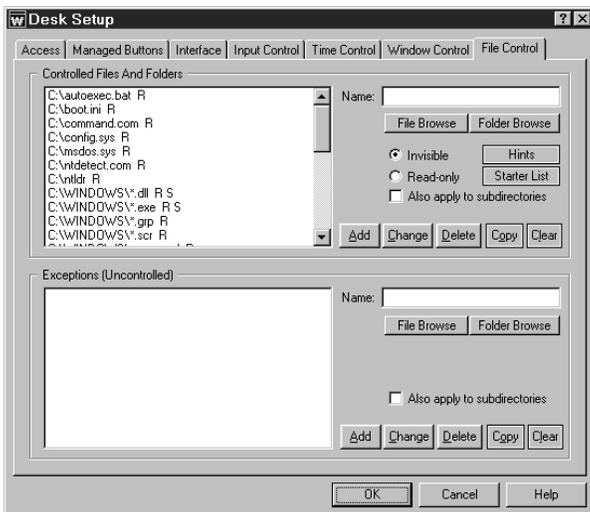
like, you can force it back to the previous screen, or close the browser. Or if you have an Open File screen, you can force it to open files only from a particular location. Or you can force the user to only save files to a particular place.

Another thing you can do is to send keystrokes to a screen. This is one of the most open-ended and powerful things in Full Control. If you see a particular screen come up, you can send it anything you want, just as if you had typed it from the keyboard.

For many of these options, you can set it so only certain folders are accessible while that option is active. If you set these Allowed Folders, only those folders will be accessible during that operation.

File Control Tab

The last tab is File Control. File control is a very powerful tool. We talked about it a little when we discussed per-program file control, above. Here is where you set the global file control.



With file control, you can set up so that when members of this group log on, they find that certain files, folders, even entire directory sub-trees are read-only, or completely invisible. Or maybe just certain files, or certain types of files, are controlled. For example, perhaps they find that all .doc files on the entire machine are read-only.

There's an exceptions mechanism that lets you protect all files or folders you specify "except" certain ones. For example, you can hide all .doc files except for the ones in this user's personal directory.

(The user's personal directory can be set up here, using File Control. Our documentation describes how to give all

your users personal directories, based on their logon names and set up so every other user's personal directory is invisible while this user is logged on.)

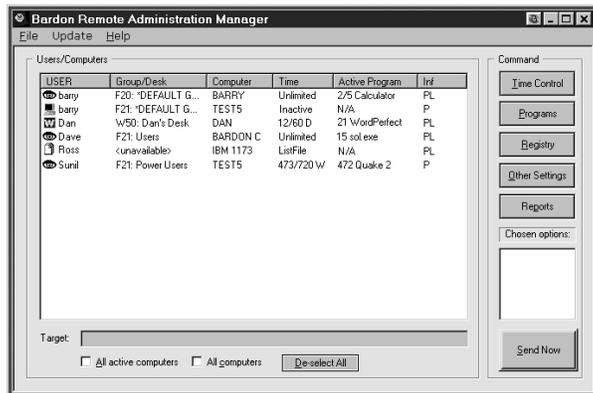
Now, as I mentioned before, you can have per-program file control where this all gets changed on the fly depending on which program happens to be active. They work together, the per-program file control and this global file control here on the file control tab.

Now that you've seen all the setup options in the client, the remote management tools will fall into place very quickly. You can close the client now if you like, or leave it open, whatever you prefer.

Let's look at our Remote Administration Manager.

Remote Administration Manager

In order to run the Remote Administration Manager you must give the Setup Password that was specified for the client installed on this computer. This ensures that only administrators can use it.



You'll also find that on your network, you can only run one copy of the Remote Administration Manager at a time. This means no one can bring up another copy and take over your network.

You use the same Remote Administration Manager whether you have WinU, or Full Control, or a mixture of the two. In fact, the Remote Administration Manager will even tell you whether a particular client machine is running WinU or Full Control, what version is installed, and lots of other useful information about what's going on remotely on the clients, up to date in real-time.

When you run the Remote Administration Manager, you'll see the machine icons pop up. This is our process of discovery across the network, where we find all the running managed computers and bring them into our list.

The Remote Administration Manager shows the users that are currently active, the WinU desk (or Full Control group) that is currently active for them, as well as the computer name, their time control settings, their current active program and how many minutes that program has been running.

The Remote Administration Manager can also generate reports showing the user's entire "audit trail" usage history.

What else can you do from the Remote Administration Manager? There are five buttons on the right side of the main screen. These control the main functions you can do from here.

The Time Control button manages the amount of time on the remote computer. Remember I mentioned you can start off a desk with zero time remaining, and then shoot some time over the network when they come up to the front desk? Well, here's how you do it.

Use the Programs button to get a list of what's going on currently at a remote machine. It can also show what has been going on historically. What do I mean by that? Remember the Diagnostic Snapshot mechanism that I mentioned before? Here's another way we use that. We show a list of the Diagnostic Snapshots going back over time. This gives you a very detailed look at what is running, and what has been running.

If you see that some program is running, that you'd rather not be running, you can close it. Or if something ought to be running that isn't, you can launch it.

The Registry button lets you manipulate their registry remotely. It's true that Windows has a way to set up a registry for remote editing, but if the remote registry has not been set up to allow this, you can't do it through Windows. With our software, you can always do it. This emergency repair tool lets the administrator go in and fix things remotely if needed.

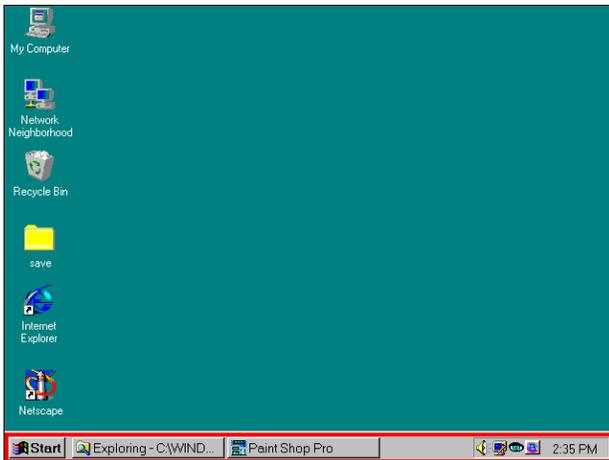
With the Other Settings button, we can update the clone file settings (to say where the remote client machine should read the settings information from), shut down or log off the computer, or get remote file/directory listing (like doing a DOS dir command).

Finally, there's a Reports button. Remember all the reports we looked at on the WinU client setup screens? From the Remote Administration Manager, you can remotely run all the same reports, against the remote machine's information.

The Remote Administration Manager is designed to be used across your LAN, but it is not necessary to run this server component in order to run Full Control or WinU. That's because the clients are very smart. They know what to do whether they are connected to the Remote Administration Manager or not. So, because you don't need to run a server all the time it works fine on standalone computers or on a travelling laptop - or if your server goes down. It's designed to be run on standalone machines just as well and just as securely as on a network.

Now that you've seen WinU and the Remote Administration Manager, we'll go through Full Control. It will look very familiar. Full Control and WinU are designed to be managed the same way through the Remote Administration Manager.

A Brief Look At Full Control



Let's launch Full Control. After it's running, look at the Windows desktop. Unlike WinU, nothing has changed. Full Control provides real-time oversight and monitoring of the regular Windows interface. While it's running, the only change you'll see is the eyeball in the corner of the taskbar next to the clock.

But while it's running, you can't move icons on the desktop, you can't right-click, you can't bring up any properties screens. The administrator can set up so icons like My Computer and Recycle Bin can be deactivated - you click on them and nothing happens. And more.

This is the default configuration. Remember, all these settings are optional, they can be changed and configured the way you want them.

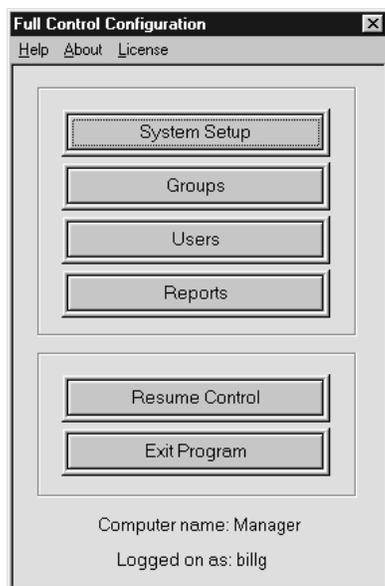
Let's take a look at Full Control, and compare it to WinU. Click on the eyeball and choose Setup Options to see the main menu. You need to give the password of course.

Full Control Setup Options

The Full Control Configuration screen has six buttons on it: Systems Setup, Groups, Users, Reports, Resume Control and Exit Program.

The three buttons at the bottom are pretty much self-explanatory. Starting from the bottom of the

Configuration screen:



Exit Program closes Full Control and returns to regular Windows.

Resume Control takes you out of Setup Mode to again protect the computer. Setup Mode is where the system administrator configures this computer. The settings can be exported and sent to any or all of your other managed computers

The *Reports* button is just a shortcut into the Reports section of the System Setup screen, it's a quick way to run reports.

So there are really only three buttons to know: *Users*, *Groups*, and *System Setup*.

Users is where you add your users and indicate what group each user is in. When that user logs on, that group's settings are activated, so those settings will control that session. If an unlisted user logs on, the Default Group settings are used. You really only have to list your few

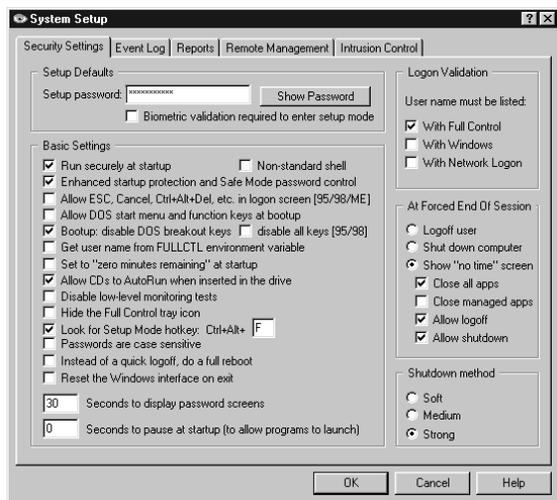
"exception" users, and let the Default Group handle the bulk of them automatically.

Groups is where you give the properties of the groups themselves. These settings are used when a member of that group logs on.

System Setup is where you give the overall settings that will apply to members of all groups. Let's start there. I'll click the *System Setup* button. This will display the System Setup screen.

Full Control System Setup Screen

Full Control's System Setup screen looks very similar to the System Setup screen we saw in WinU,



with similar options on the Security Settings tab to run at startup, set enhanced startup protection, allow Escape, Cancel and Ctrl+Alt+Del, get a user name from an environment variable, allowing CDs to run, etc.

You'll also see similar options for password or biometric validation, logon validation, restart control, and shutdown method. You've seen these before, they're just the same here in Full Control.

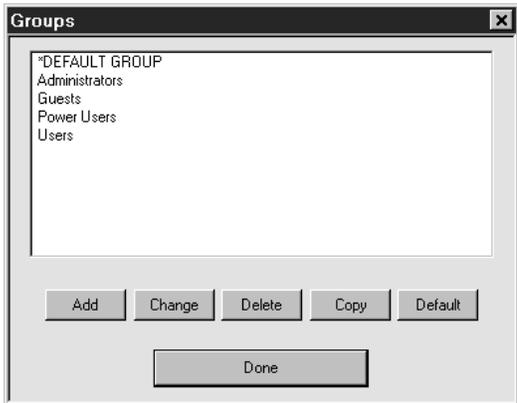
The Event Log tab is the same as with WinU. So are the Reports tab, the Remote Management tab, and the Intrusion Control tab. Full Control has no Screen Options tab, because Full Control has no screen.

The rest of the System Setup tabs are the same as you've already seen in WinU. We've tried to make the Full Control setup as much like WinU as possible, to make it easy for people to use both programs. Most people will switch back and forth, because if you subscribe to our Maintenance Plan,

you can mix and match your licenses. Let's say you've got ten licenses and you want to run three Full Control instead of WinU. Fine, you swap out three of your WinU and swap in three Full Control.

Just as in WinU, Full Control's System Setup screen has systemwide options. You'll see on the Group Setup screen that there are per-group options as well. Groups in Full Control are much like Desks in WinU. Close the System Setup screen and open the Group Setup screen for the current group.

Full Control Choose Group Screen



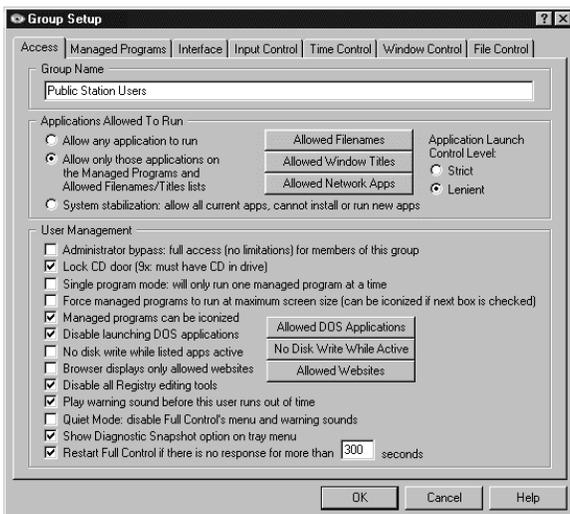
In Full Control, users are members of groups. When users log on, Full Control sees what group they're in and give them that group's attributes and security permissions.

The administrator uses the Groups screen to add, copy, or delete a group, or to select a group to change its settings.

By default when you first install it onto the system, Full Control creates some sample groups - Administrators, Guests, Power Users, Users and the Default Group. This is similar to groups in XP or Windows 2000.

So, what can we manage in a group? On the Groups screen, double-click a group, or select a group and click the Change button, to display that group.

Full Control Group Setup Screen



A Full Control group is much like a WinU desk, so the Full Control Group Setup screen is much like the WinU Desk Setup screen. There's an Access tab, a Managed Programs tab, Interface tab, Input Control tab, Time Control tab, Window Control tab and File Control tab. Just the same as we saw in WinU.

On the Access tab you name the group and set allowed applications, just as in WinU. At the bottom are User Management options. These are things like single program mode, allowed web sites, all that you saw before for WinU is here as well.

On the next tab, Full Control's managed programs are much like WinU's managed buttons, except in Full Control

the user launches programs through the regular Windows interface, not through a button. Like WinU, Full Control will oversee it after it launches.

Here we also have the same minutes until termination, password protection, etc. Advanced settings including per program file controls, etc.

Next is the Interface tab. In WinU, this controls WinU's interface. In Full Control, it controls the Windows interface. You can set the wallpaper, disable or lock certain desktop icons, hide desktop icons, even hide the taskbar.

After that is the Input Control tab which allows you to manage the Start button options as well as the same keyboard and mouse options as we saw in WinU.

After the Input Control tab are the Time Control tab, Window Control tab, and File Control tab. These are virtually identical to WinU's. We've tried to make the setup screens as close as possible, so if you know how to set up WinU, you'll know how to set up Full Control.

Full Control or WinU?

People ask, should I run WinU or should I run Full Control? It depends on your needs. The security and management options are very similar, but the way they treat the user interface is different, and addresses different needs. But it's up to you. Now, you're not locked in. Under our Maintenance Plan, you can pick whichever one you want, switch back and forth if you like, so if you run Full Control and you decide you need WinU, you swap out Full Control, swap in WinU, set it up, and you're done.

And that's it. You set up your configuration, save it as a clone file, and distribute it out to all the client computers. The client computers act on that configuration, and report to the Remote Administration Manager so you can monitor the clients on the fly. We've tried to make it as easy as possible to get good comprehensive oversight.

We hope you like using WinU and Full Control as much as we've enjoyed creating them.