Full Control and WinU

Description and Technical Walkthrough

BARDON DATA SYSTEMS

Introduction

This document provides a screen-by-screen walkthrough of Full Control and WinU, 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. We'll look in detail at Full Control, the Remote Administration Manager, then briefly at WinU. Most of what we'll say about Full Control also applies to WinU.

Overview

Full Control and WinU 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 can 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 provides oversight to 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.

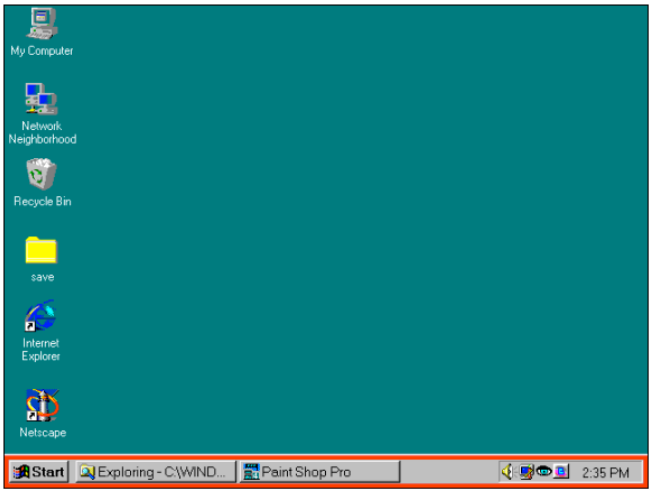
Other than how it handles the interface, WinU and Full Control work in the same way. The setup screens are very similar, so after you learn one product you can administer both of them. After we go through Full Control in detail, we'll talk about WinU, and the differences between them.

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.

BARDON DATA SYSTEMS • 1164 SOLANO AVENUE #415 • ALBANY CA 94706 • 510/526-8470 VOICE • 510/526-1271 FAX
http://www.bardon.com • info@bardon.com • sales@bardon.com

Full Control



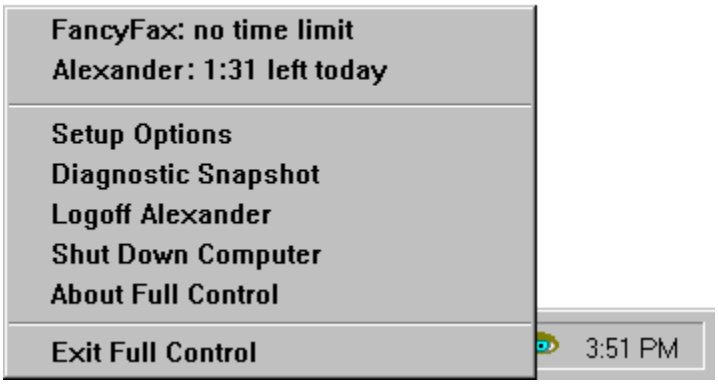
Let's launch Full Control. After it's running, look at the Windows desktop. Nothing has changed. It still looks like Windows because it is Windows. Full Control provides real-time oversight and monitoring of the regular Windows interface. While it's running, the only change you'll see is the eyeball 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 are 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.

Control-Alt-Delete and similar keys are under our oversight too. For example, if we press Ctrl+Alt+Del, nothing happens. Can the user go to the Start menu and close from there? Try it. Open Start and choose Shut Down. Nothing happens. That's under our control too.

Windows has a very insecure logon process. It's easily bypassed, especially Windows 9x where you jcan just hit Escape and log on as somebody else, or create a new logon on the fly. But when our software 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 Novell or NT, we work with and enhance any validation from the server. But we even offer logon oversight on standalone computers like laptops.



On the desktop, if you click on the eye, you get a menu showing the active program, and giving some options.

Hmmm, Shut Down Computer, let's click on that. Well, you can't do that without the password. And if you don't know the password, it's just not going to work.

You can lock it down further, or open it up further. This is just the default sample configuration. There are lots of options.

BARDON DATA SYSTEMS • 1164 SOLANO AVENUE #415 • ALBANY CA 94706 • 510/526-8470 VOICE • 510/526-1271 FAX
http://www.bardon.com • info@bardon.com • sales@bardon.com

Setup Options

Let's look at Full Control's setup options. Click on the eyeball and choose Setup Options to see the main menu. You need to give the password of course.

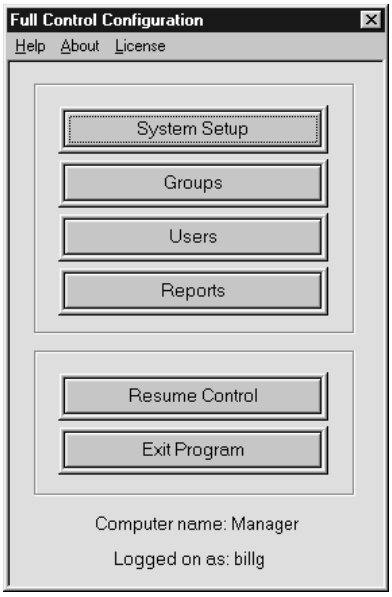
The Full Control Configuration screen has six buttons on it: Systems Setup, Groups, Users, Reports, Resume Control and Exit Program.

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.

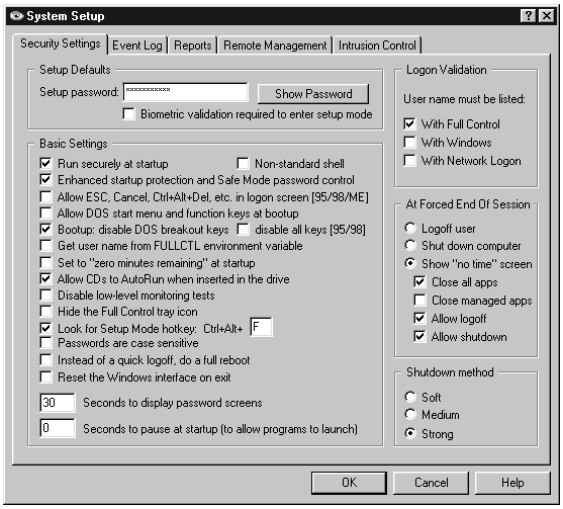
System Setup is where you give the overall settings that will apply to members of all groups. Let's start there. I'll click the *System Setup* button. This will display the System Setup screen.

BARDON DATA SYSTEMS • 1164 SOLANO AVENUE #415 • ALBANY CA 94706 • 510/526-8470 VOICE • 510/526-1271 FAX
http://www.bardon.com • info@bardon.com • sales@bardon.com

System Setup Screen

The System Setup screen has five tabs: Security Settings, 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. 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 Full Control 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 FULLCTL 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.

Set to "zero minutes remaining" at startup is a way of setting up public access machines. You turn on the machine in the morning, up comes our system managing everything that's going on, yet anyone that wanders in and sits down at the machine can't do anything until the administrator, at another machine across the network, sends over some time. That happens when the patron goes up to the desk and says "I'd like to use the computer please." So check this box to manage the time remotely.

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 Groups 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 Full Control, 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.

Hide the Full Control tray icon: the little eye in the tray can be turned off. Remember when I was talking about the audit trail? You can set up Full Control so you don't change any of the Windows behaviors at all, and simply use it as an audit trail generator. For situations like that, when you don't want people to know you're using the software, you could hide the tray icon.

If the tray icon is hidden, or if the whole task bar is hidden (we can do that too) you're going to want to Look for the setup mode hotkey. The default is Ctrl+Alt+F, but you can set it to anything you want. You hit Ctrl+Alt+F, and Full Control asks for its setup password. If you give the password, it goes into Setup Mode.

Passwords case sensitive - they can be case sensitive or not as you choose.

And then at the bottom, a few options that aren't used much, but they're used occasionally for unusual kinds of systems. Logoff versus reboot is to accommodate those rare computers that work better if you do a full reboot instead of using the logoff process. 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. How many seconds to display the password screens that I've been showing you, and a way to pause at startup to allow certain programs to launch.

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

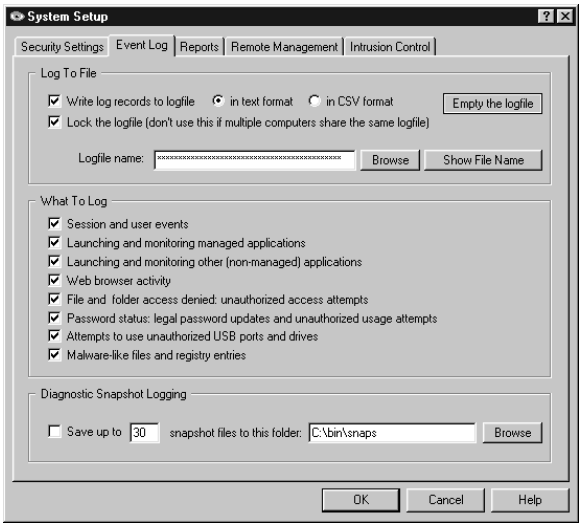
also validate for peer-to-peer networks. Even a standalone Windows 95 machine, which is known for having pathetic security, you can't log on unless you're you.

What happens At Forced End Of Session? Let's say the user runs out of time, do you want to log the user off? Do you want to shut down the computer? Do you want to show a screen saying there's no more time left?

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.

So as you can see, you set these up one by one and there you go. The rest of the tabs on the System Setup are for specific things.

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.

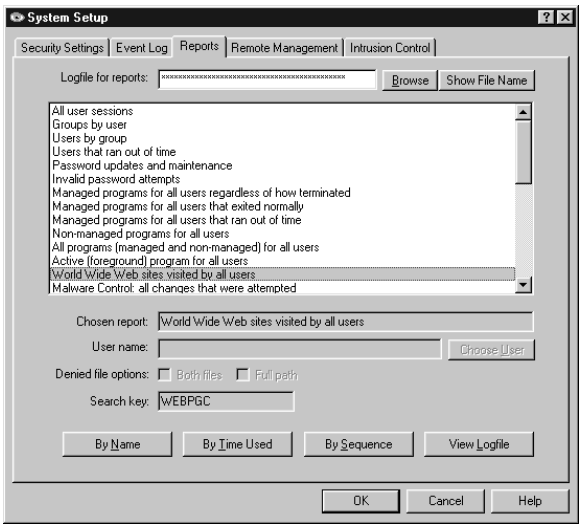
You can also log in multiple formats, depending on where you are going to export it to. For example CSV format, comma-separated values, is good for importing into a database or spreadsheet. Most of the rest of the tab is what kinds of events to log.

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.

BARDON DATA SYSTEMS • 1164 SOLANO AVENUE #415 • ALBANY CA 94706 • 510/526-8470 VOICE • 510/526-1271 FAX
http://www.bardon.com • info@bardon.com • sales@bardon.com

Reports Tab



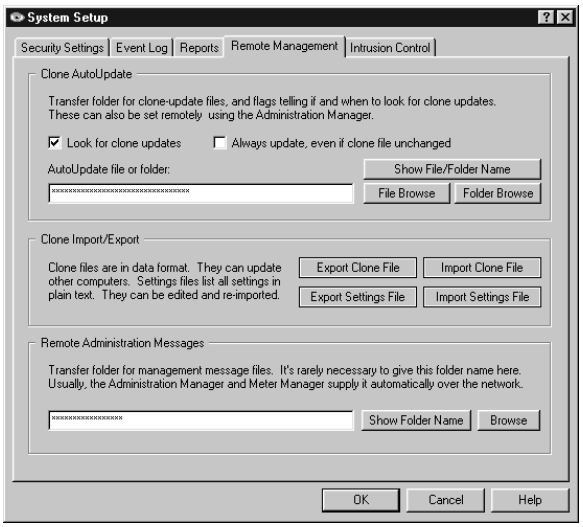
As you can see on the Reports tab, we've got dozens of different predefined reports.

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. We'll look at each of these sections in turn.

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

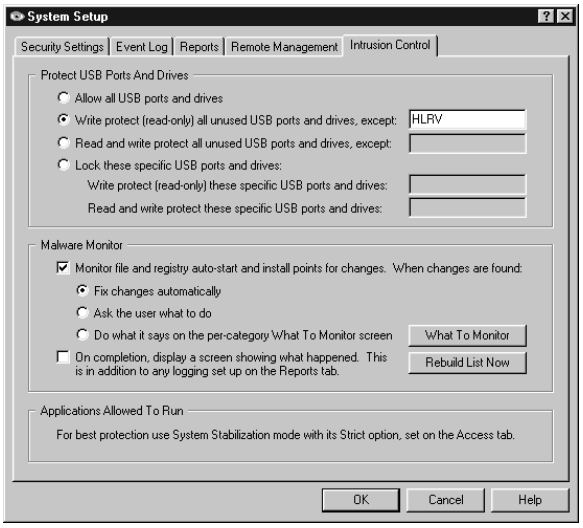
This is because the Clone AutoUpdate and Administration Messages fields can be set by the Remote Administration Manager automatically from across your network. The Remote Administration Manager can broadcast its preferred settings to the client.

That leaves just the Import and Export buttons. In Full Control, the setup and configuration tools are part of the client. To set up Full Control 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, both manually and automatically.

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.

BARDON DATA SYSTEMS • 1164 SOLANO AVENUE #415 • ALBANY CA 94706 • 510/526-8470 VOICE • 510/526-1271 FAX
http://www.bardon.com • info@bardon.com • sales@bardon.com

Intrusion Control Tab



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

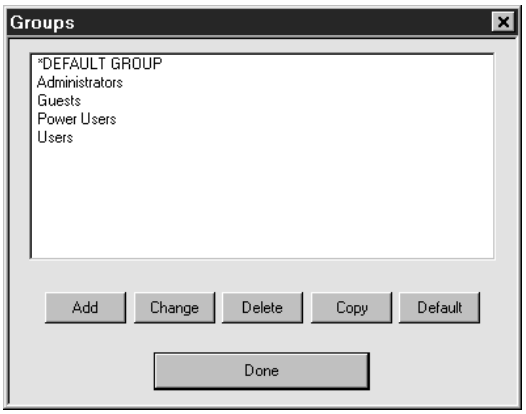
There are two sections to this tab. With the top section, you can lock USB ports (and actually, any other local drives such as CD or DVD writers). The drives can be set as read-only or completely invisible and unusable. This can go a long way to preventing data theft. It can be set to scan at startup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

And that's the entire System Setup screen. Now let's close the System Setup screen, which takes us back to the Full Control Configuration screen. On that screen, click the Groups button. This brings up the Choose Group screen.

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.

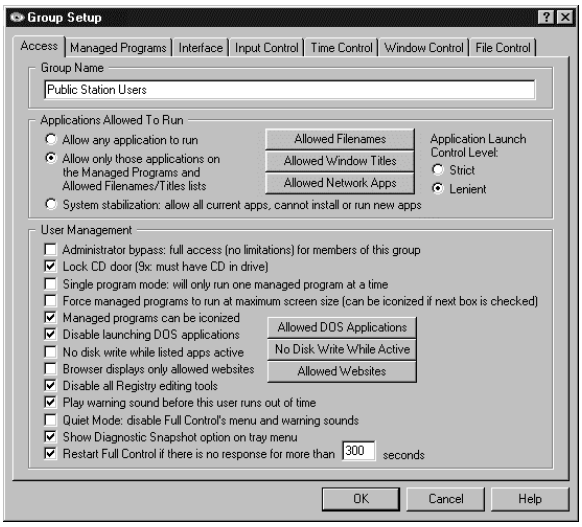
The administrator uses the Groups screen to add, copy, or delete a group, or to select a group to change its settings.

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.

Group Setup Screen

Access Tab



The first tab on the Group Setup screen is the Access tab. Here's where you set the group name. Other than the Default Group, all group names can be changed on the fly.

For members of this group, what applications are allowed to run? 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.

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 Group Setup has a number of general options, while the other Group Setup tabs control specific targeted capabilities.

We have an administrator bypass. Let's say a user is logging on, and that user's name is in a group with administrator bypass privileges. In that case, Full Control just instantly gets out of the way. This lets your designated people do their work, yet you don't have to give them the Full Control password.

Locking 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 Full Control, 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.

If you check Single program mode, Full Control will only allow the user to run one managed program at a time. You'd use this if you want the active program to close if another managed program is launched, maybe because you're afraid people will just let programs pile up and forget 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 make sure they can't iconize programs, maybe because you're concerned that users will lose programs if they're not as familiar with Windows as perhaps one would like. Or maybe you've used Full Control to hide the taskbar.

You might want to disable launching DOS applications because DOS can be an end-run around Windows. We can allow certain DOS applications to run, even if DOS applications are disabled in general, if you want to say no to everything except, say, one particular DOS app.

BARDON DATA SYSTEMS • 1164 SOLANO AVENUE #415 • ALBANY CA 94706 • 510/526-8470 VOICE • 510/526-1271 FAX
http://www.bardon.com • info@bardon.com • sales@bardon.com

No disk-write while listed apps active is an interesting one. Check this box to accommodate applications that behave badly when another program writes to disk, for example certain scandisk, defrag, or backup programs. You know how some of these restart themselves when another program writes to disk? Check this box and Full Control won't write to disk while a listed program is active.

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.

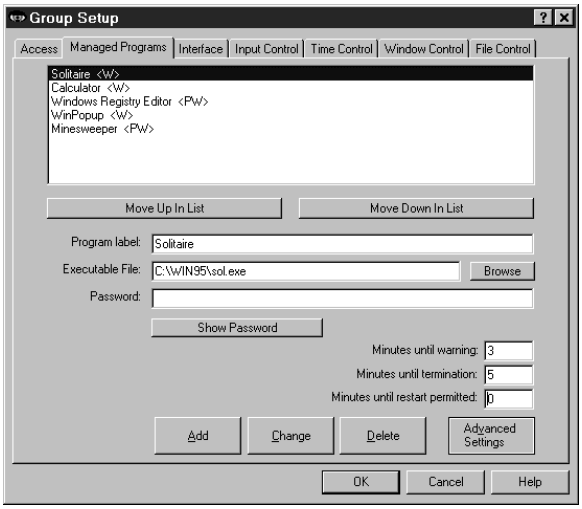
Play warning sound before the user runs out of time. I mentioned that users are members of groups, and you can set up a group to have time control. You can give them a grace period, a warning period of so many minutes before their time expires. It can put up a box and say “hey, it’s going to expire.” 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 Full Control 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.

Show Diagnostic Snapshot option. I mentioned before how you can generate Diagnostic Snapshots automatically, so you'd have a minute-by-minute record of everything that was happening on the computer. If you want to, you can also put an item on the popup menu from the eyeball, if you click it you generate and show a Diagnostic Snapshot immediately. So you can get an instant, behind the scenes look at what’s happening on this machine, right now.

Restart Full Control if there’s no response for more than so many seconds is one way Full Control makes sure that nobody sneaks in and kills it. We have a number of mechanisms for that, this is one of them. If you check this box, if it 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 Programs Tab



Next is the Managed Programs tab. Managed programs are applications that we choose to manage.

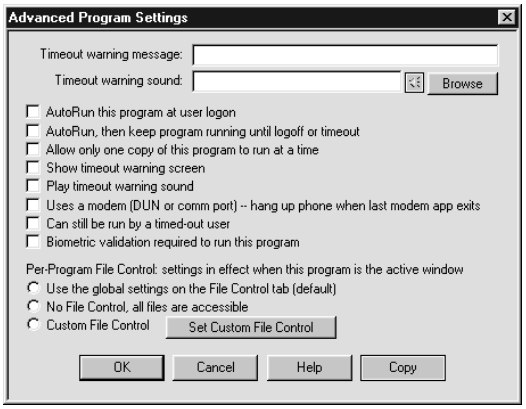
You can manage a program in many ways. You can give any program a password, or require biometric protection, which will be required to launch that program.

You can indicate how many minutes a program is allowed to run, and how much warning the user gets before it is terminated.

You can indicate that if it does run, and it stops, how many minutes that you need to wait before you can restart it. This one can be very useful in certain kinds of 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 run when a particular user logs on. 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 groups. 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 session. You can't do that in Windows either.

Allow only one copy of the program to run at one time, that setting is used if you don't want them starting an extra copy every time, because they get confused. Some people who don't know better just click on documents, and run nine instances of the same program. If you don't want that happening, check this box.

There are some options at timeout. Remember we can have timeouts for various reasons. Here, you can set up to show a timeout warning screen and play a timeout warning sound.

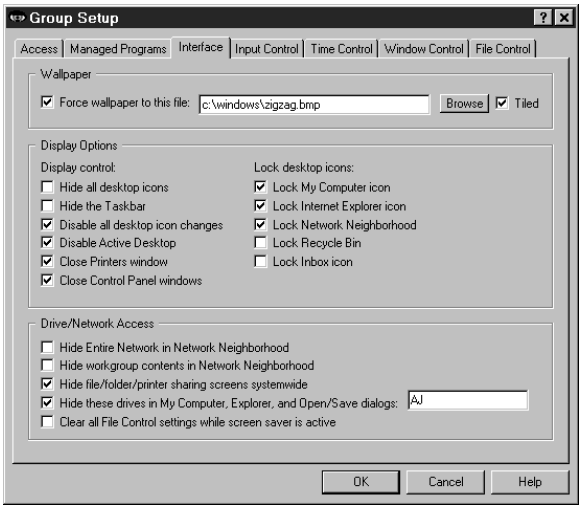
You can have it clean up after a modem, hang up the phone. If you do a Dial-Up Networking connection, say, with your web browser, yes, you can set up Windows so that it "connects to the Internet as needed." But Windows won't disconnect when you're done. We add that capability.

Next there's an option saying that this managed program 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



The interface tab lets you set a number of things having to do with the Windows user interface. Force the wallpaper to a particular file, or force it to a blank screen by checking the box and not filling in anything. You know how you can go to a website and right-click on a graphic and you say "set as wallpaper"? With Full Control, can't do it. So no more porn on your desktops.

The display control section covers what's visible, and what's accessible. Some things that I mentioned before - hiding desktop icons, hiding the taskbar.

The way we hide the taskbar makes the whole thing goes away, not like in Windows where it kind of slides down underneath, and then it comes back as soon as you mouse over it. When we hide the taskbar it's gone, it doesn't exist. Windows can't do that.

Disabling desktop icon changes means the desktop icons can't be moved, renamed, or deleted.

Disabling Active Desktop is very popular. The problem is that Active Desktop allows things like live-update of system components. That's fine if you've got one machine at home and you're managing and maintaining it, but if you've got 200 machines in an office, the last thing you want is to have everyone updating them willy-nilly and getting the components out of sync, because then when something goes wrong, you don't know what you're managing. Many people that manage lots of computers would just as soon turn Active Desktop off.

You'd check the box to close the printers windows so users can't change the printer configuration. They can still use the printer, but not its configuration screen.

And of course closing Control Panel windows, as I mentioned before, lets you disallow all the Control Panel windows. Oddly enough, Microsoft's Policy Editor can only disallow a few of the twenty-five or thirty of them.

Locking desktop icons is in the next column. What does that mean? Well, we looked before at how nothing happened when I clicked on the My Computer icon. Now that we're in Setup Mode, I will click on it again. Notice how it highlights (lights up) now. You can open it up and do things. But if you try to click on a locked desktop icon (when you're not in Setup Mode), nothing happens.

You can lock the My Computer icon, the Internet Explorer icon, and a few other things that are standard on the Windows interface. If you want to manage icons that are different than the standard desktop icons listed here, you can also do that, through File Control or Window Control.

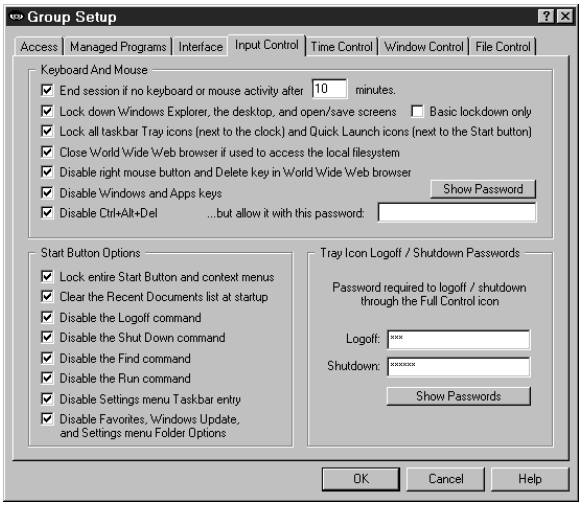
The next section is Drive/Network Access. Maybe you want to hide the computers that are listed in Network Neighborhood, if this is a public access machine where you don't want people to have access to the rest of the network. Or maybe you want to hide other things. You can even hide drives in My Computer,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

BARDON DATA SYSTEMS • 1164 SOLANO AVENUE #415 • ALBANY CA 94706 • 510/526-8470 VOICE • 510/526-1271 FAX
http://www.bardon.com • info@bardon.com • sales@bardon.com

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.

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, Full Control 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.

Will you need to Lock all tray icons? Maybe you need to run certain tools that put icons in the tray (the little icons next to the clock) but you don't want a regular user to get to them. Some tools give you the option of putting a tray icon there or not, but some tools don't. If you want to run the tool but you don't want a user popping up its tray icon menu, you can lock the icons on the tray, so when they try to click on a tray icon, nothing happens.

This also locks all the Quick Launch icons, which are typically next to the Start button in the taskbar. As with the tray icons, if you click on a locked Quick Launch icon, nothing happens. By the way, another way to handle Quick Launch icons is to make them invisible for this particular user, by using File Control. That way they don't appear on the taskbar at all. You can do this with Start Button entries as well by the way. The entries simply won't be there. It's a nice clean way of configuring a different interface for different users. I'll come back to this in a second.

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 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.

On the Input control screen there are also options for the Start button. This provides oversight to what you can and can't do with the Start button.

You can lock the entire Start button, so if your users click the Start button, nothing happens.

You can clear the Recent Documents list when the session starts. The recent documents list has the files that the previous user opened. Maybe you don't want that list to be there for the next user.

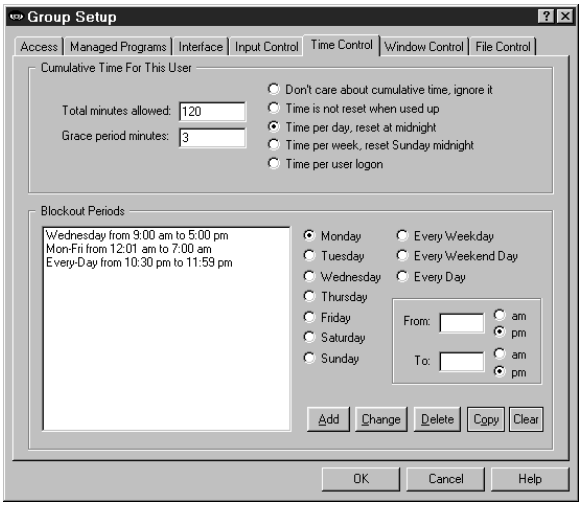
Disabling logoff and disabling shutdown are pretty obvious - do you want members of this group to be able to log off or shut down. If you disable logoff or shutdown, you can give passwords to these options. This allows people who know the password to log off or shut down from the Full Control "eye" while disallowing this for a regular user.

Disabling Find, disabling Run, disabling settings menu task bar entry, disabling Favorites, Window update, setting menu folder options, these are Start button options that give you fine-grained control over what they can do.

You can even get even more fine-grained control than that, because most of the entries on the Start button are little shortcut files, and you can use our file control to make files like these invisible. If you do that, the Start button entries vanish. So you could set it so if this user logs on, a whole bunch of Start button entries become invisible.

So there are lots of flexible ways to handle user input.

Time Control Tab



The Time Control tab is where you set how long this user is allowed to use the computer, 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.

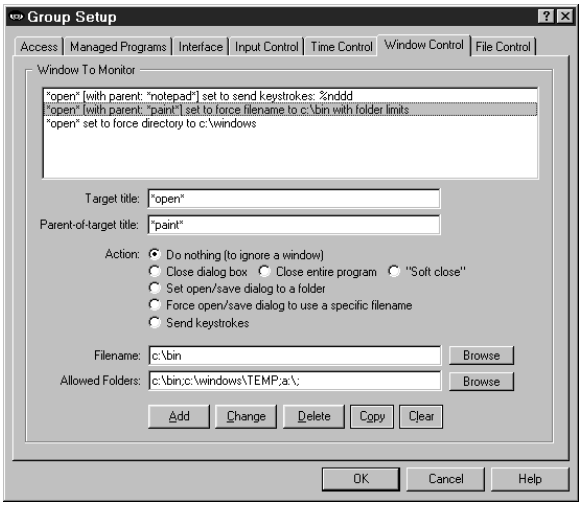
On the bottom of the Time Control tab you can set blockout periods. Blockout periods are times when nothing runs. Maybe you want to set thing up so nothing runs after hours, or perhaps you have a lab where a machine is supposed to be used only during certain periods of time.

BARDON DATA SYSTEMS • 1164 SOLANO AVENUE #415 • ALBANY CA 94706 • 510/526-8470 VOICE • 510/526-1271 FAX
http://www.bardon.com • info@bardon.com • sales@bardon.com

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 Programs so they run even in a blockout period. This is useful for "emergency" programs, perhaps programs that you have password-protected (through Full Control) 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.

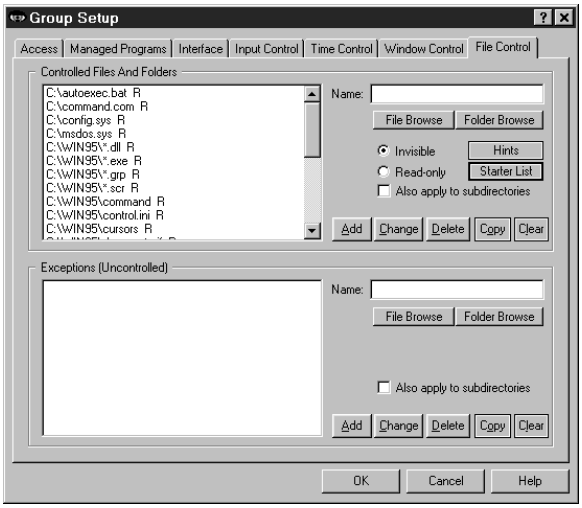
Another thing you can do is to send keystrokes to a screen. This is one of the most open-ended and powerful things in Full Control. If you see a particular screen come up, you can send it anything you want, just as if you had typed it from the keyboard.

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.

BARDON DATA SYSTEMS • 1164 SOLANO AVENUE #415 • ALBANY CA 94706 • 510/526-8470 VOICE • 510/526-1271 FAX
http://www.bardon.com • info@bardon.com • sales@bardon.com

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.

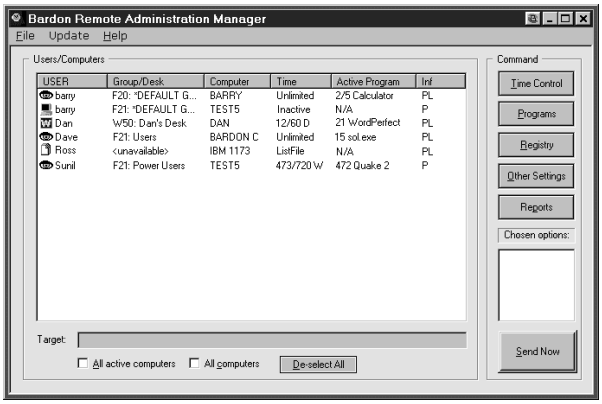
Now that you've seen all the setup options in the client, the remote management tools will fall into place very quickly. You can close the client now if you like, or leave it open, whatever you prefer.

Let's look at our Remote Administration Manager.

BARDON DATA SYSTEMS • 1164 SOLANO AVENUE #415 • ALBANY CA 94706 • 510/526-8470 VOICE • 510/526-1271 FAX
http://www.bardon.com • info@bardon.com • sales@bardon.com

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 Manger 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 Full Control group (or WinU desk) 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 how you can start off 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 Full Control client setup screens? From the Remote Administration Manager, you can remotely run all the same reports, against the remote machine's information.

So, the Remote Administration Manager lets you see what's running now, what's been running in the past, what files and folders are on the hard disk, and what's in the registry. You have the ability to fully view everything that's going on, on the remote machine, in real-time whenever you want to. And you can remotely change anything you can see, modify any of these settings on the fly.

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

BARDON DATA SYSTEMS • 1164 SOLANO AVENUE #415 • ALBANY CA 94706 • 510/526-8470 VOICE • 510/526-1271 FAX
http://www.bardon.com • info@bardon.com • sales@bardon.com

WinU

When you start WinU, notice how it completely takes over the screen. No taskbar, no Start menu, no desktop icons. Just labeled buttons.

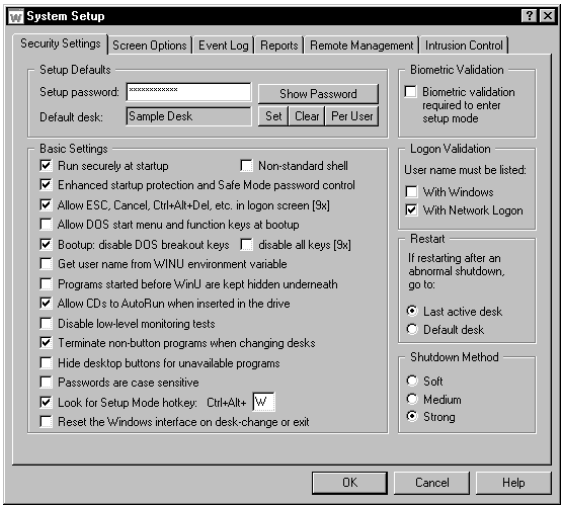
This is WinU's *Simplified Replacement User Interface*, which makes a computer with WinU very easy to use, even for novices.

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.

Let's take a quick look at WinU, and compare it to Full Control.

WinU System Setup Screen



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

As for the rest of the tabs, the Event Log tab is also just like in Full Control. So are the Reports tab, the Remote Management tab, and the Intrusion Control tab.

The only new tab for WinU is the Screen Options tab. That's needed here because WinU has a screen while Full Control doesn't. This tab has settings for showing the menu bar, showing the status bar, handling the title bar apps button, showing the user's name in title bar, different things of that nature around the WinU screen itself.

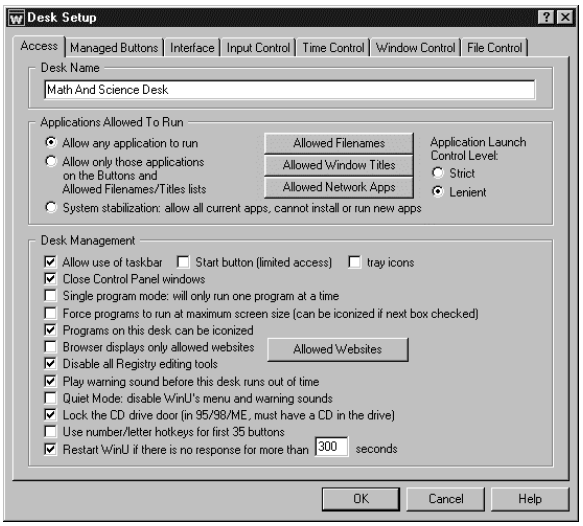
The rest of the System Setup tabs are the same as you've already seen in Full Control. We've tried to make the WinU setup as much like Full Control as possible, to make it easy for people to use both products. Most people will switch back and forth, because if you subscribe to our Maintenance Plan, you can mix and match your licenses. Let's say you've got ten licenses and you want to run three WinU instead of Full Control. Fine, you swap out three of your Full Control and swap in three WinU.

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

WinU Desk Setup Screen

WinU can have hundreds of different desks, and they can be linked together or not, as you choose. When you, the administrator, set up this desk's layout you choose what buttons will be on that desktop, and how those buttons will work.

Let's look at how you set up desks in WinU, and compare it to setting up groups in Full Control.



The Desk Setup screen is a lot like the Group Setup screen in Full Control. There's an Access tab, a Managed Buttons tab, (because in WinU all programs are run from buttons) Interface tab, Input Control tab, Time Control tab, Window Control tab and File Control tab. Just the same as we saw in Full Control.

On the Access tab you name the desk and set allowed applications, just as in Full Control. At the bottom are desk management options. There is a slight difference here with WinU in that 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. You can lock the Start button, you can lock the tray icons (we saw how that worked in Full Control), and other things. Close control panel windows, single program mode, allowed web sites, all that you saw before is here as well. WinU's managed buttons are set up a lot like Full Control's managed programs. We have the same minutes until termination, password protection, etc. Advanced settings including per-program file controls, etc.

There are many ways to create a WinU button. Perhaps the easiest way is to drag-and-drop a program or Shortcut onto the WinU desktop. Everything will then be set up automatically. For example, let's say we want to create a button from a shortcut that happens to be on the regular Windows desktop. Just drag-and-drop it onto the WinU desktop, and there's a button, with a name and an icon and everything. When you click it, it runs that desktop shortcut we originally dropped onto WinU. If the program or Shortcut is elsewhere than on the desktop, just navigate there in Explorer and drag-and-drop it from there.

BARDON DATA SYSTEMS • 1164 SOLANO AVENUE #415 • ALBANY CA 94706 • 510/526-8470 VOICE • 510/526-1271 FAX
http://www.bardon.com • info@bardon.com • sales@bardon.com

When you (the administrator) set up the desk you can move the buttons around, change the size of them, the width of them, their icons, layout, color and font. It's very easy. You don't have to be an artist to lay out these screens. Just create the buttons and it sets up a pleasing default layout, which is generally perfectly fine for most purposes. After that, however, you can change the interface in many ways. This is done on the Interface tab of the Desk Setup screen.

On the Interface tab, you can play with the button positions, change the background wallpaper and colors, change the button layout and spacing, change other things too.

You can set up sounds here too. You can have different sounds that play when you log on to a desk, log off a desk, run a program, etc.

Now that we've changed a few things, let's click OK on the Desk Setup screen to save our changes and put them in place. Let's take a look. As you can see, now there's a different background image and the buttons are different. It's easy to make these desk layout changes.

The rest is pretty much exactly as you saw before. Other than the desk layout tab, the remaining tabs here are just the same as you saw in Full Control. So if you know how to set up Full Control, you'll know how to set up WinU.

Each desk can have its own password. In regular Windows the user can only change from one desktop to another by re-logging on. But in WinU you can set up hundreds of desktops and allow the user to change between them without going through the Windows logon first. You can link these desktops together in various ways. Of course, you can also restrict who can log on to which desks.

This multiple desktop business is very powerful. Regular Windows doesn't offer it. If you use Full Control you'll log on and you only have one desk – the regular Windows desktop with the Start button, desktop icons, and taskbar. But with WinU, the user logs on and might have hundreds of desks available, be able to flip between them. So in some ways, WinU is a lot more flexible.

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.