

Full Control Internet

Description and Technical Walkthrough

BARDON
DATA SYSTEMS

Introduction

This document provides a screen-by-screen walkthrough of Full Control Internet (including the *Compliance Edition*), the enterprise-level system management oversight product from Bardon Data Systems. It shows how to quickly set up and start using this product to provide system stabilization, audit trail activity logging, real-time oversight, and centralized remote administration.

Overview

Full Control Internet is a tool for remote administration and management of computers. It is intended for enterprise situations in which client computers must be managed from one central location. The managed computers do not have to be on the same LAN, or even in the same country. They need to have an Internet connection, but the Internet connection does not have to be a permanent connection, it can be an intermittent connection through, say, Dial-Up Networking. The tool that manages these computers centrally, from anywhere in the world over the Internet, is the Remote Administration Manager.

Full Control Internet does constant real-time oversight of what windows appear, and how they are used. It includes an active real-time client-side agent that runs behind the scenes on each managed computer. It can provide an audit trail of what programs each user ran, when, and for how long. Browser-based applications can't bypass it. Maybe the user thinks "I'll use Hotmail or Instant Messenger, so my messages won't go through the company's audited email system." With Full Control Internet, those will show up too. All this is possible because we monitor from the client, in real-time, everything that is going on.

A real-time audit trail is a powerful management tool. Managers need to know what their people are doing so they can guide them to where they need to be. But these days, staff is geographically scattered. How does a manager grasp what all these people are doing? Full Control Internet captures data and provides detailed reports. What if, through Bardon's reports, each manager could manage more people? Costs go down, productivity goes up.

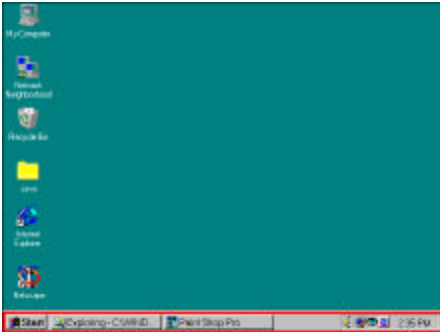
There's nothing unusual or new about the idea of keeping an activity audit trail. But here's an easy way of overlaying it across what's already on your system. You don't have to change what's already installed, what already works, to see who is doing what, and when. An audit trail activity report can also be useful for legal reasons.

But Full Control Internet is more than just an audit trail tool. It can actively manage the capabilities of the workstation, depending on who is currently logged on, the time of day, and other factors. It can add password protection or biometric control to any application, even programs already installed on the computer. It includes a checkpoint/rollback mechanism, administration communications tools, file distribution capabilities, and other active features that make enterprise computers more reliable, more manageable, and easier for authorized staff to modify and fix when necessary.

Further, through the use of the *Full Control Internet Compliance Edition*, Full Control Internet provides the enhanced oversight mandated by HIPAA, 21 CFR Part 11, and similar government regulations. The *Full Control Internet Compliance Edition* is an enhanced version of Full Control Internet that adds specific features to address these regulations.

Let's look briefly at the managed client computers, then spend some time with the heart of the system, the Remote Administration Manager, to see how the client systems would be managed.

Full Control Internet Client Agent



First let's launch Full Control Internet's client component on some workstations, so we can manage them remotely. After Full Control Internet is running on the clients, look at the Windows desktop. Nothing has changed. It still looks like Windows because it is Windows. Full Control Internet provides real-time oversight and monitoring of the regular Windows interface. While it's running, the only change you'll see is the blue 'eye' icon in the corner of the taskbar next to the clock (and if you like, that can be removed as well).

But while it's running, in the default configuration you can't move icons on the desktop, you can't right-click on the desktop, you can't bring up any properties screens, you can't shut down or log off without a password. Icons like My Computer and Recycle Bin can be deactivated - you click on them and nothing happens. Control-Alt-Delete and similar keys are under our oversight, too.

This is just the default sample configuration. All these settings are optional. They can be changed and configured the way you want them.

Full Control Internet's client manages the user's interaction with the computer on behalf of the Remote Administration Manager, in the ways that the administrator has specified, and will provide to the administrator an audit trail of the user's activities. It will start automatically when Windows launches, and it will keep running until Windows closes.

The client can manage the logon process. Windows has a very insecure, easily bypassed logon process, especially Windows 95, 98 and ME, which are still on the majority of enterprise computers. On these systems, a user can just hit Escape and log on as somebody else, or even create a new logon on the fly. But when Full Control Internet is running the user can't do that. Do you really need to purchase Windows 2000 or XP for all your computers? And you might need to upgrade your hardware to run it properly. And then there's the time and expense to install it, and re-install all your software. What if there was another way to get a secure logon, without replacing the setup you already have, that already works?

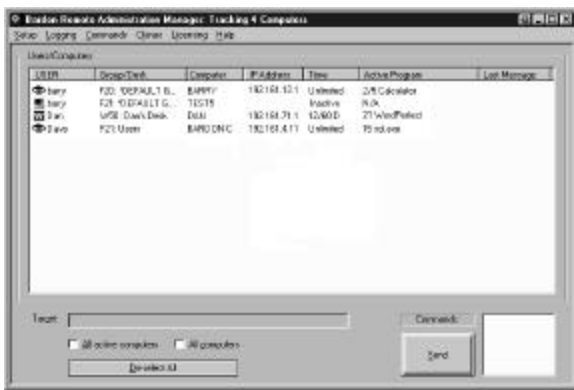
There are also security holes in Windows NT, 2000 and XP. That's why the Full Control Internet client is designed to address issues on those platforms as well, both during the logon process and while the user is working with the computer. Now, it will take advantage of existing administrative resources, if these are available. For example, if you validate through a Novell or NT-class server, we work with

and enhance the server-based validation. But we even offer logon oversight on standalone computers like laptops.

One of the keys to this is that it's a 'smart' client. It can understand and react even when it's not connected to the Remote Administration Manager, for example if your Internet connection goes down. But the core of Full Control Internet is the way the Remote Administration Manager can oversee and manage the user experience in real-time, across the Internet from anywhere in the world.

If you need to, you can manipulate the Full Control Internet settings on an individual client by clicking on the 'eye' icon, giving the password, and changing the settings locally. You can even export clone settings files from the client, to save a copy of your changed settings. But in general, the client functions unobtrusively on the managed computer, and simply acts as the Remote Administration Manager's channel into that computer so it can effect your policies and your management style on those distributed computers. Let's look at the Remote Administration Manager.

Remote Administration Manager Overview



The Remote Administration Manager oversees and controls the managed client computers. Its centralized logging provides a user activity audit trail, and its remote management capabilities let you update and modify the client computers from your central location.

It displays a line of information about each client computer in its main-screen list. By selecting from this list, the administrator can further query the managed client computers for more details about their situation, or send commands over the Internet to update them in many ways.

You can run the client-side component in a standalone mode, not connected to a Remote Administration Manager. But generally, the Remote Administration Manager is always running as a server. The managed clients are pointed at that server, and the system administrator oversees and controls those clients through the Remote Administration Manager.

The Remote Administration Manager is installed on only one computer. This is the central computer from which you (the administrator) will do your remote administration. This computer should have good physical security. It should not be out in the open where 'just anybody' can get at it. It is a server.

In general the Remote Administration Manager is always running so it can stay in contact with the desktop clients, keep the central event log up to date, and send your commands to the managed computers. If it exits the desktop clients will try periodically to reconnect, and cache their event log records locally until they do.

The event log collects many different kinds of information. The built-in reports cover the most common queries, but other queries are also possible. The event log format is documented, allowing you to construct any query that is of interest. Many file formats are supported. Most production

environments will prefer to log to a standard format like Access, Excel, or a SQL database, but we also offer a Bardon Default logging format.

When certain events occur you can have the system generate an Event Alert to display a message, play a sound, or remotely notify you by email (including an SMS email to your cell phone).

If your managed computers are on different LANs, the Remote Administration Manager must be run on a computer with a static IP address (one that is directly visible to the Internet) so it is visible to all your various desktop client computers. As with all static IP computers (for example, web servers), you should run appropriate security software on this computer such as firewall, antivirus, etc. The desktop clients can be on either static IP computers or masqueraded computers. If the desktop clients are run in static IP computers, appropriate security software should be run there as well.

For added security you may want to list with the Remote Administration Manager the IP addresses of all desktop clients allowed to contact it. Connection requests from other IP addresses will be refused. Refused connections are logged. Look at these items in the event log to list computers that were not allowed access. Perhaps someone is trying to break into your system. Or perhaps some are legitimate desktop clients that should be added to the list.

If a licensed copy of WinU Internet or Full Control Internet is also installed on your administration computer, its setup password is required in order to use any Administration Manager feature which modifies the remote computers. To those without this password, the Administration Manager is only a 'read-only' screen that cannot send commands to the connected computers. After the password is given, the Administration Manager won't ask again for fifteen minutes. Use the Password Lock Now option to re-lock the system before the fifteen minute period expires.

To see what a desktop client is doing, use the Commands | Program Management screen to list running programs. Need to close one of them? Copy/paste from this report the filename of the program to close, also on the Commands | Program Management screen. Something isn't running that should be active? Launch it from the Commands | Program Management screen. If your launched program requires a more open security situation (for example, an installer or uninstaller) check the box to temporarily disable security control.

Need to move a new program to one or more desktop clients (as opposed to running a program that is already there)? Use the Commands | File Transfer screen. After it is transferred, you can run it using the Commands | Program Management screen.

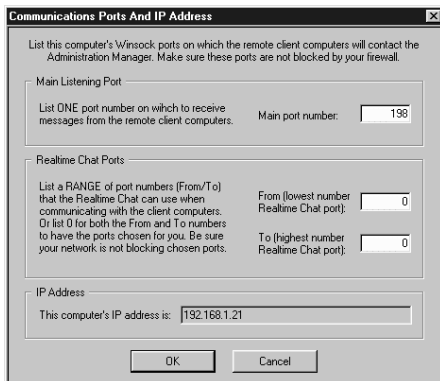
Need to remotely mass-install a new-version update of WinU Internet or Full Control Internet on all your managed computers? You can't simply remotely run the installer, because WinU Internet or Full Control Internet is already running, and it might not allow an installer to run on that computer, not to mention that Windows won't let you overwrite a running program. The solution is to use the Commands | Version Update screen.

If you need to have a conversation with a user, connect to that user with Realtime Chat. The administrator can initiate a Chat session from the Commands | Other Settings screen at any time. The user can initiate a Chat session if the administrator has allowed the Chat item to be displayed on the tray icon menu.

To distribute licenses to your connected computers, enter them on the Managed License Numbers screen. The license will be sent to the client computers as they connect to the Remote Administration Manager. Multiple license numbers can be entered.

Remote Administration Manager Screen By Screen

The Remote Administration Manager's menu items offers options to communicate with the listed computer and send them updated information. Let's look at each menu item in detail and see how these options can be used to manage your remote computers.

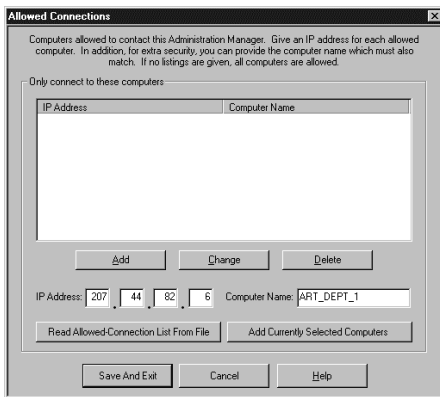


Setup Menu

The Setup menu has options to control communications between the Remote Administration Manager and the clients. There are also a few housekeeping options.

The first item is *Communications Ports and IP Address*, which lists the port and IP address on which the clients will contact the Remote Administration Manager. You can set whatever port you like.

This screen is also where you set up to use the real-time chat. With this feature, the administrator can have a real-time dialogue with the user. The *Communications Ports and IP Address* screen is where you set up the ports through which the client and the Remote Administration Manager can communicate. If the port is left blank, a random port is used.



The next Setup menu item is the *Allowed Connections* screen. We've built a lot of security into Full Control Internet. This option restricts the IP addresses that can communicate with the Remote Administration Manager. Communication from an unlisted IP address is rejected. If the list is empty, all addresses are allowed.

We also have other security mechanisms to validate incoming messages, but the *Allowed Connections* option is certainly something that should be considered if your goal is to create a fully secure configuration.

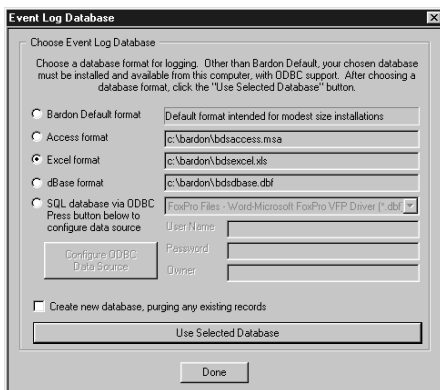
The remaining Setup menu items don't have screens. They are toggled from the menu.

The options to *Delete Selected Users/Computers* and *Show Inactive Users/Computers* are to clean up and display various classes of users and computers on the screen. It's convenient for keeping your display focused on the machines that are of interest.

Password Lock Now protects the Remote Administration Manager. This runs all the time as a server, but there isn't always someone sitting in front of that server. So, its options are password protected. It would be inconvenient to constantly ask for a password, so we let it stay valid for about fifteen minutes before asking again. *Password Lock Now* is used if the administrator chooses to walk away from the machine before the password expires, to immediately protect the computer.

Logging Menu

The Logging menu is used to set up the Event Log Database, archive it, set Event Alerts, and run reports. We'll look at each of these in detail.



The first menu item is *Event Log Database*. Full Control Internet client computers observe events, and they send event messages to the Remote Administration Manager, which logs those events to its database. What kind of database should the Remote Administration Manager log those events into? The Remote Administration Manager has a number of database options.

Full Control Internet's event log can use the format of most industry-standard databases. We offer *Access format*, *Excel format*, *dBase format*, or you can log to any *SQL database via ODBC*. This allows your event log to be read by those database products. We also offer

a *Bardon Default* format for situations where no other database is available. In fact the next Logging menu item has to do with archiving the event log when using a Bardon Default database. Other database products have their own mechanisms for archiving their data. This item is designed to back up a Bardon Default database.

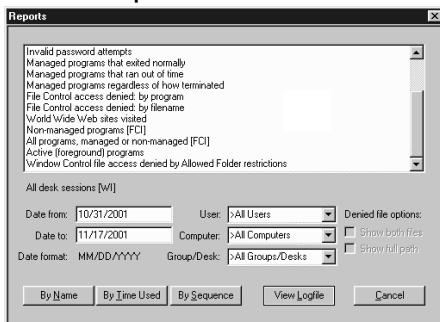


The next Logging menu items are *Set Event Alerts* and *Show Alerts Window*. Event Alerts are things logged by the client that you want emphasized. When the Remote Administration Manager receives those events, in addition to logging them it displays them in its Alerts window, and can optionally send an email or play a sound. It can even send an email to your cell phone or text pager.

Each event that can generate an alert is listed here. If you check its box, it will come up in the Alerts window, which we'll look at below. Everything that shows up in the alerts window also shows up in the

database log. The Alerts mechanism is simply a way to bring the event to the attention of the administrator, or to contact that person if they're not in front of that computer.

In addition to the alert conditions listed on the *Set Event Alerts* screen, you can also have alerts sent when other conditions are observed on the client computer. These conditions are set up using the Window Control options. We'll look at how that's done when we get to Window Control. Briefly, you can set up so that when certain windows appear, when certain programs start, when certain actions take place, you can trigger events that aren't predefined. So you have a lot of flexibility there.

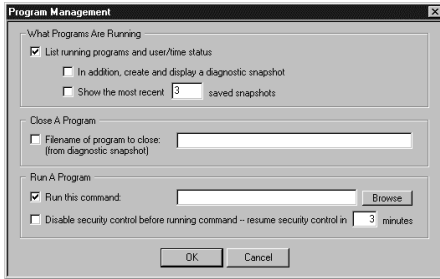


The next Logging menu item lets you *Run Reports*. Like the Alerts, reports are based on the information logged to your chosen event database. You can run reports on all the data that was sent to the event database, whether the event generated an alert or not. The Remote Administration Manager has a few dozen built-in reports, or you can run your own reports through whatever database program

you're using. One of the advantages of using the standard database format is that data is natively available for whatever further queries you want to develop, giving you a lot of flexibility. The built-in reports are quite flexible too. You can run reports within a particular date range, within a particular user range, for certain computers, certain groups or desks, by the amount of time it took, by sequence, etc.

Commands Menu

Next is the Commands menu. Just as the Logging menu dealt with information coming in from the client computers, the Commands menu deals with information going in the other direction: commands sent from the Remote Administration Manager to one or more client computers.



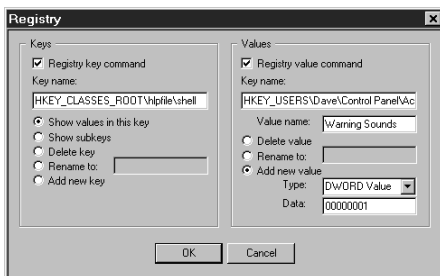
Commands are sent to the computers that you highlight on the Remote Administration Manager main screen. Select the computers of interest, set up your commands, then click the Send button in the lower right corner of the screen. If you don't want the commands sent immediately, the *Send Command Later* option can queue them to be sent at a future time.

Let's look at the commands that you can send. The first item on the Commands menu is *Program Management*. With this, you can list the programs that are running, in great detail if you need to.



When you get the list back of what programs are running, you can use that information to perhaps close one of the programs, if that's what you want to do. Or if there's something that should be running that isn't, you can Run A Program. This might be to install new software, make application changes, or delete files. To facilitate this, you have the option to temporarily and invisibly disabling the user's security settings while the change is taking place.

The next item on the Commands menu is *Time Management*, which provides the option of adding or changing the amount of time currently in the user's session, and in general updating the way the time limits are used on the client computer.

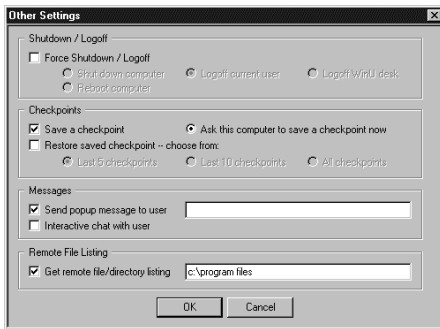


You can add time, change the current time, or delete time from one or more client computers.

The *Registry* screen is next. This screen lets you manipulate the remote computer's registry, for example to add or change keys, perhaps on many computers at the same time.

One advantage of Full Control Internet is that, unlike 'remote screen viewer' programs, it can manipulate all your computers simultaneously by sending commands to more than one computer at a time. For example, on the Commands menu, the *File Transfer* option lets you send files to all your computers, with just one command. Compare this to products with which you can manipulate only one computer at a time, and where you have to connect to each computer individually in order to do so. Full Control Internet's approach is much more efficient.

The next item on the Commands menu is the *Version Update* option. You already know that you can use the *File Transfer* and *Program Management* options to update other files and programs. Here is how to update the Full Control Internet software itself, by broadcasting that new-version update to all your managed computers. They will install the new version of our software on top the old version.



Next is the *Other Settings* screen, which lets you remotely shut down your other machines, log off, and so on. Maybe you've just remotely installed a new application, and you need to remotely reboot all the machines. Before you do that remote install and reboot, you might want to remotely save a checkpoint, to have each machine back up its working configuration before you update it. You also might want to mass-broadcast a popup message to everybody, saying "In five minutes I'm going to update all your computers, then reboot you, so save your work now."

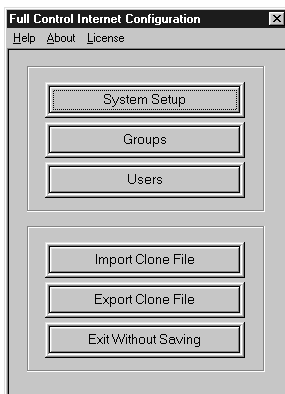
The *Other Settings* screen can also start an interactive chat session with the user. Real time chat is a very powerful tool for communicating with your users when they're spread all over the country, or the world. You as the administrator can start the chat session at any time. The user can be given the option of starting a chat session with the administrator, but by default the user doesn't have the option to initiate the chat session.

Finally, the *Other Settings* screen can provide a remote file listing, perhaps to make sure that that file you transferred actually got there. Never hurts to check!

The last items on the Commands menu are ones we've already mentioned, options for *File Transfer* and for queuing commands to be sent later.

Clones Menu

The Clones menu lets you create clone settings files and send them to the managed computers. A clone file can change anything and everything about how the client agent works with the user. You create a clone file, then send it to all the selected computers, which will automatically update themselves with the new settings. Full Control Internet's clone file mechanism is very flexible. It can implement your management style and employee policies in exactly the way you want. After the menu walkthrough, we'll go through the process in detail, but here's an overview.



First, click the Clones menu and choose *Full Control Internet Clone Settings*. The Configuration screen appears. We'll look at this later in detail. For now, here is a brief overview.

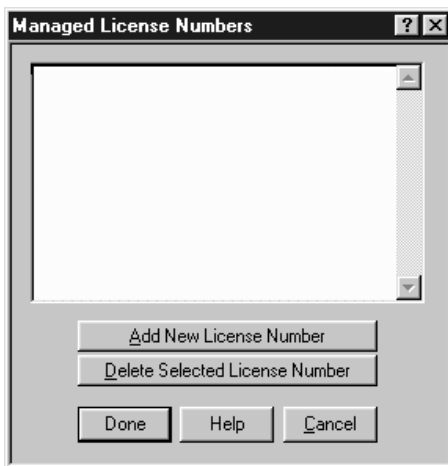
Click System Setup to configure the system-wide settings that will be in effect no matter who is logged onto the managed computer. When you click OK you'll return to the Configuration screen.

The Groups screen configures the options for members of each group. As before, click OK to return to the Configuration screen.

On the Users screen you can name who will be a member of what group. Or you can let Full Control Internet get this from your user's network domain rights. This is how it's generally done; you rarely need to keep a separate, parallel list of users in Full Control Internet when you've already got your list of users in Windows, through your domain.

When you have all the settings as you want them, come back to the Configuration screen and click Export Clone File. Save the clone file under any name you want. On the main-screen list, select the computers that should receive this clone file, then use the Clones menu to send it to those computers.

Licensing Menu



The last item is the Licensing menu, which lets you manage the Full Control Internet license numbers provided by Bardon Data Systems. Each license number is valid for a certain number of computers and, in some cases, a certain period of time. Here's where you enter those licenses.

After the numbers are entered, they are distributed to the managed computers when they connect to the Remote Administration Manager. You don't need to go to each individual machine to do this kind of update, any more than you need to go to each machine to do a version update or a clone-settings update. You can do it all from the Remote Administration Manager.

We've now seen all the menus and options offered by the Remote Administration Manager.

Creating And Using A Clone Settings File

When we discussed the *Clones* menu, we touched only briefly on the clone settings file itself. Let's look at that in detail. A clone settings file is the way Full Control Internet saves a 'set of settings'. Once you create the clone settings file, you can send it to one or more of your client computers. They will read it in, and implement the management policies you have chosen.

The clone file can be used in other ways, as well. For example, when you're initially installing the client software agent, the installer can automatically use a clone file to give the client computer its initial batch of settings. By using a clone file at installation, you can assure that the clients are connected to the Remote Administration Manager, and have all the other settings you choose, from the very beginning.

To create a clone file, click the Clones menu and choose the *Full Control Internet Clone Settings* item. The Configuration screen appears. As a starting point, you can import an existing clone file that you want to update, or you can use the default settings. Either way, you then change the settings to suit, then export the updated clone file.

Click System Setup to configure the system-wide settings that will be in effect no matter who is logged onto the managed computer. When you click OK you'll return to the Configuration screen.

Next, click Groups to configure the options for members of each group. As before, click OK to return to the Configuration screen.

The Users button is next. Which users are members of what group? On the Users screen you can explicitly name who will be a member of what group. Or you can let Full Control Internet get this from your user's network domain rights; this is how it's generally done. You rarely need to keep a separate, parallel list of users in Full Control Internet when you've already got your list of users in Windows, through your domain.

Here's how it works. If the user is named on the Users list, Full Control Internet uses that user's group. But if that user isn't there, Full Control Internet can see the network domain groups in which this user has rights, and compare them to its own groups. Full Control Internet groups have priority numbers. It will use the highest-priority group to which this user belongs. For example, if the user is a member of network domain groups A, B and C, and the administrator has set up in Full Control Internet that B has the highest priority, the user gets the settings for Full Control Internet group B.

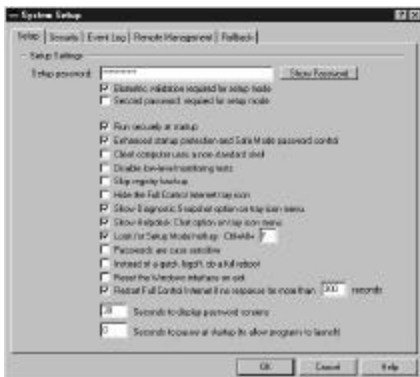
So all you have to do is name your Full Control Internet groups so they sync up, and your existing network settings will take care of the rest.

Okay, that's the overview. Let's look at the System Setup, Groups, and Users screens in detail.

System Setup Screen

On the Configuration screen, click on the System Setup button to show that screen.

The first tab of the System Setup screen is called *Setup*. This is where you give the setup password, boot-time options, and other systemwide preferences.



The setup password is needed to change the administration settings from a client computer. Settings can be changed there as well as through the Remote Administration Manager, handy if you're in a jam. The administrator can even export clone settings from the client computer. You can save your work that way, even use it elsewhere if that's what you choose.

In addition to the setup password, we also support biometric validation. If you check the Identix biometric validation box, Full Control Internet will request biometric validation before going into setup mode, or using other password screens.

In the Standard Edition, use the Show Password button to see the actual password text. In the *Compliance Edition*, check the box labeled Second password required for setup mode to require two

separate passwords to enter Setup Mode, change settings, or perform certain other administrator overrides. This "two-key" security means that both administrator passwords must be given in order to modify the security oversight.

If that box is checked, the "Setup password" control and button at the top of this screen are replaced with two buttons, each of which separately changes one of the two administrator passwords. These two buttons are themselves password protected by the password they manage. As a further security precaution, there is no "show password" option for these two passwords. Instead, asterisks are always displayed for their characters.

If a licensed copy of Full Control Internet is installed on the computer running the Remote Administration Manager, the Setup password is required to make changes through the Remote Administration Manager. If a licensed copy of the *Compliance Edition* is installed on the computer running the Remote Administration Manager, and the box labeled Second password required for setup mode is checked, both of the Setup passwords are required to make changes through the Remote Administration Manager.

In addition, on the *Setup* tab you can indicate that Full Control Internet should run securely at startup, automatically when Windows starts. You can use Enhanced Startup Protection And Safe Mode Password Control to ensure the logon is valid and that the user doesn't make inappropriate use of Safe Mode. If you've checked that box, the user has to give a password in order to get into safe mode, so Safe Mode becomes an extension of our own setup mode.

Other options here include settings like using a non-standard shell, disabling low-level monitoring, and skipping registry backup. They're mostly for tweaking computer systems with unusual hardware or configurations.

Moving down the *Setup* tab ... hiding the Full Control Internet tray icon is something that is occasionally used. By default, when Full Control Internet starts, its 'eye' icon shows in the system tray. If the administrator chooses, it doesn't have to be there.

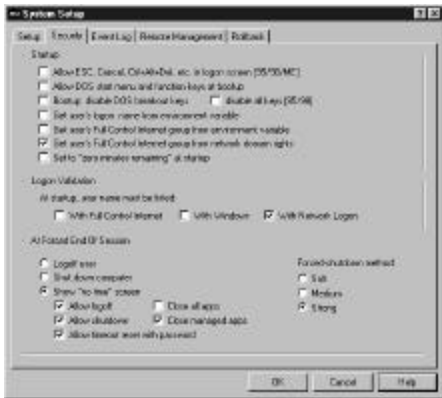
If the 'eye' icon isn't going to show, you'll want another way to get into Setup Mode in an emergency. That's why we offer a Setup Mode hot key, which is also set on the *Setup* tab. When you press the hotkey the password screen appears, plus optionally the biometric validation.

As mentioned above, Help Desk Chat can always be initiated by the administrator, but can only be initiated by the user if the administrator has allowed this. Here on the Setup screen is where the administrator can allow the user to initiate a Chat session.

The other options on the *Setup* tab are rarely used. Full Reboot is for machines where a logoff doesn't clear settings properly. Reset Interface on Exit is used to work around a documented Microsoft bug in Windows 98 and its Internet Explorer shell. And Restart If No Response is a security option so a rogue program can't take over your computer and knock out Full Control Internet.

The second tab of the System Setup screen is called *Security*. It controls user logon validation and what happens at startup, shutdown, and at forced end of session.

Many options are geared towards 95 / 98 / ME machines, which are still the majority of computers on the corporate desktop. We don't force you to upgrade to other operating systems; instead, we harden the operating system you already have.



That's why we pay special attention to Windows 9x, to make sure it's going to work for you, without paying extra money for an OS upgrade.

In general, you won't want to Allow Esc, Cancel, Ctrl-Alt-Del, etc. in logon screens. Everyone knows by now how easy it is to bypass the logon in Windows 9x. When the logon screen comes up, you just press Escape, and go to the default configuration. We've plugged that hole, and made the 9x logon pretty much as secure as the NT/2000 logon. So, you can continue to use the operating system you already have installed. You don't have to reinstall another

version of Windows, you don't have to reinstall your applications, you don't have to worry about whether the new setup is going to work like the old setup, and you don't have to wonder if your hardware will support an upgraded operating system. You just put Full Control Internet on top of what you already have, and harden the operating system that is already installed.

Similarly, disallowing the DOS start menu and function keys at bootup handles the character mode screens that can come up when you start Windows 9x, and sometimes in NT as well. The Disabling DOS Breakout Keys and Disabling All Keys is also useful for older operating systems.

Because some older Novell networks don't store the user's logon name correctly in Windows, we can get the user name from an environment variable, which is typically set in a Novell logon script.

You can get the user's Full Control Internet group from an environment variable, handy if you want to force all users on a particular machine to use a certain group's settings.

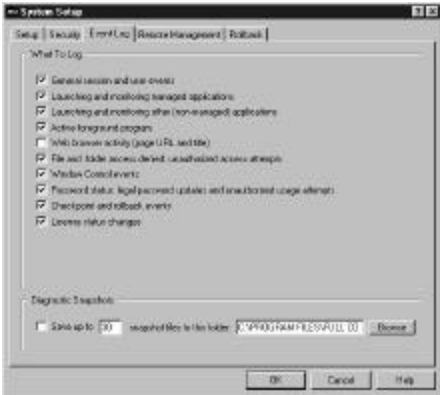
You can get the user's Full Control Internet group from the network domain rights, as we discussed earlier, so a user who is a member of many domain groups will be given the settings of one Full Control Internet group. This way you don't have to list your users in both Full Control Internet and in Windows.

The next checkbox on the *Security* tab, "Set to zero minutes remaining at startup", is often used for public access machines that need to be locked until they are explicitly enabled through the Remote Administration Manager.

Full Control Internet offers a number of options for Logon Validation. At logon, does the user name need to be validated through Full Control Internet, that is, must that user name be listed on the User screen? Does it need to be validated through Windows, that is, in Windows on the local machine? Or does the user need to be validated through a network logon? On many NT based networks, even if the user is not validated through the network, the local machine is still accessible. Full Control Internet plugs this hole.

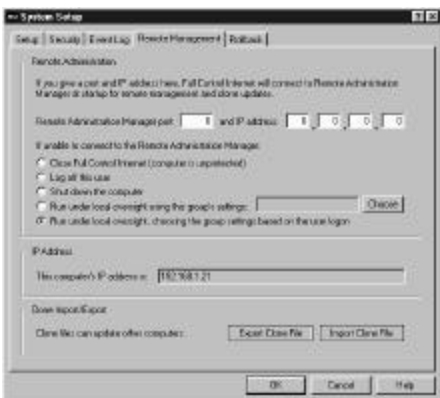
Recall that the last section of the *Security* tab controls what happens At Forced End Of Session, that is, when a user runs out of time, or is made to log off involuntarily. One option is to log off the user.

Another is to shut down the computer. A third option is to neither log off nor shut down, but make the computer session unavailable, and this is something that a lot of people use. At that point, Full Control Internet can display a screen saying there is no time left, the machine's been locked. There are many options that force this. Here you can set what happens when that screen is displayed. On that screen can be up to three buttons: log off the session, shut down the computer, and a third button that will ask for a password, and if the password is given the session is unlocked again. The third button is handy if, for example, you have an inactivity timeout. Up comes the screen and the computer is locked. To unlock the computer when the user returns, click the button to add more time to this session.



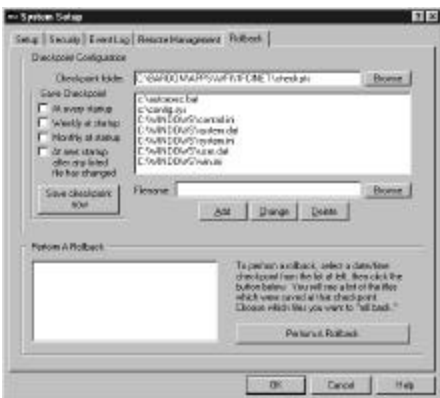
The third tab of the System Setup screen is called *Event Log*. We touched on this when we discussed the Logging menu. Here you list the classes of events you want to log. Data is generated and logged for events within those classes.

Use the bottom of the *Event Log* tab to set up the diagnostic snapshot option. This can save a minute-by-minute log showing a good deal of information about everything that's running on the computer. This can be handy when trying to diagnose intermittent crashes and similar problems, because it shows exactly what was running right before the crash, including many technical details.



The fourth tab of the System Setup screen is called *Remote Management*. This is where you list the port and IP address of the Remote Administration Manager, and what should happen if a client can't connect. You can even automatically make crucial files invisible, for example when a thief looks for data on a stolen laptop.

The Clone Import/Export section at the bottom of the screen is used only on the client computer. If you got here from the Remote Administration Manager and you try to use these buttons to export or import a clone file, Full Control Internet will tell you to use the Configuration screen buttons.



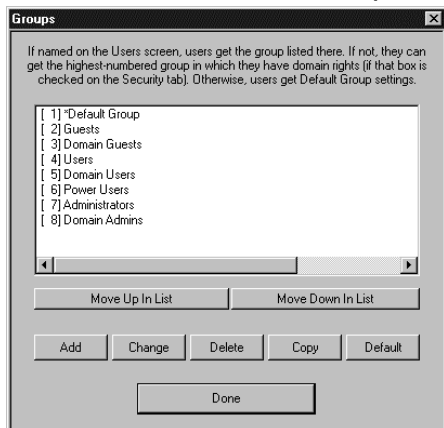
The fifth tab of the System Setup screen is called *Rollback*. This is where you set up your checkpoint/rollback file lists, so the client can save a checkpoint on a regular basis, allowing it to rollback to that configuration later.

Checkpoints are saved by the client. You can initiate a rollback either from the client or from your Remote Administration Manager.

That's the entire System Setup screen.

Groups Screen

Now let's look at the Groups screen. If you haven't done so already, close the *System Setup* screen, and on the Configuration screen, click the *Groups* button.



We mentioned the Groups screen before, when we discussed prioritization of the groups at logon when you're pulling in the information from network domain rights.

This screen is also where you add, change, or delete a group's settings. Or you can make a Copy of a group's settings, or move settings into the Default group.

Let's choose a group and click the Change button. Up comes the Group Setup screen.

The first tab of the Group Setup screen is called *Access*. As you can see, the group name and priority number are at the top. The name can be anything you like, though if you're going to be pulling in logon information from network domain rights, you'll want to include the same names you've set up for your domain groups.



Below that is where you list what applications are allowed to run. All programs? Just certain programs? It's up to you. There's also a System Stabilization option that generates a list of all programs currently on that computer. Those programs will run, but newly installed or downloaded programs won't. This is a good way to ensure that your staff are always dealing with the same system image when they need to fix something. It's also helpful for antivirus protection, because a downloaded program that can't run, can't spread viruses. And if you don't want your users to bring in games

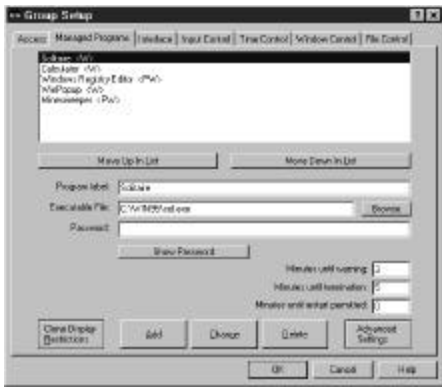
from home, this takes care of that problem as well.

Below that are the User Management settings. You can lock the CD door so your CDs don't walk away. You can have your users run only one managed program at a time, a nice way to avoid user confusion. You can force managed programs to run fullscreen, and set it so managed programs can't be iconized to the task bar. These options are also handy for confused users.

Next are more system security options. Do you want to not allow users to run DOS programs? Do you want to provide a list of allowed websites, and disallow other sites? Do you want to disable Registry tools? Most administrators do.

There are a few more options here. As with the others, if anything needs clarification just click on the Help button or press F1 to bring up the context-sensitive help for that screen. This is true for all the screens in all the programs.

The second tab of the Group Setup screen is called *Managed Programs*, where you can set more detailed program oversight. You can password protect any program, or require biometric authentication.

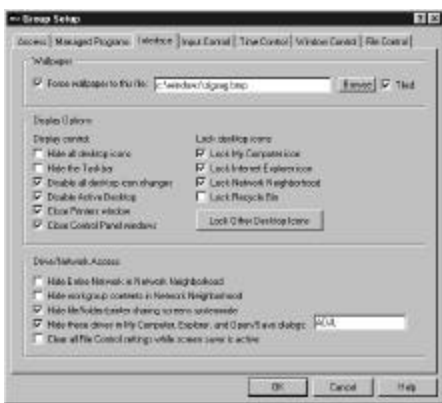


You can also set per-program time limits, display restrictions, even list the files this program can and can't access.

A program can be run automatically at startup, or be made to keep running so that it can't be shut down.

On the Advanced screen, you can set sounds or warning messages for certain situations.

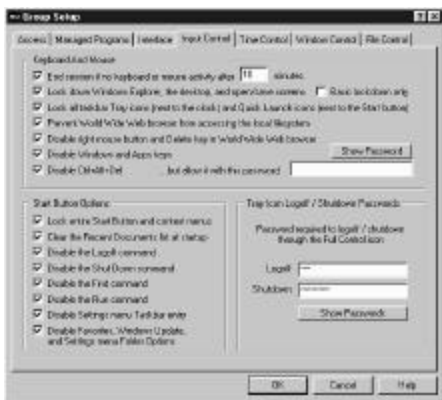
The third tab of the Group Setup screen is called *Interface*. Use this to stabilize and standardize the user interface.



You can indicate the wallpaper the users see, or no wallpaper. You can indicate how the desktop can or can't be changed, how the desktop can or can't be used.

Finally, you can indicate how printer and LAN resources can be accessed.

The fourth tab of the Group Setup screen is called *Input Control*. Just as the Interface tab indicated what resources the user could access, the Input Control tab indicates what input the user can provide.



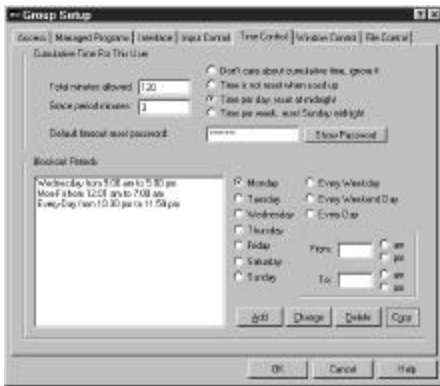
At the top of this tab is where you set the inactivity timeout. If the user provides no input for a certain period of time, the inactivity timer will be triggered. What happens then depends on the Forced End Of Session option given on the System Setup screen.

The next item, Lock Down Windows Explorer, The Desktop, And Open And Save Screens, is often used in conjunction with Disabling All Desktop Icon Changes on the Interface tab. The two together secure access to setup and configuration options.

Next is an option to lock the taskbar and Quick Launch icons when the user clicks on them, perhaps so the user can't get into their setup options, followed by an option to allow browsers to access the web but not files on the local computer. As we get more blurred lines between the web browser and the file browser, this becomes more of an issue. Administrators have asked for this capability and we are happy to provide it.

We offer ways to disable various keys, including Ctrl-Alt-Del. Many administrators prefer a computer which can't use Ctrl-Alt-Del, so the user can't bypass what's running. Ctrl-Alt-Del can have a password, too, so a special person can access it if needed.

Our Start Button options can disable or change what's listed on the Start button, or even make it completely dead, so clicking on the Start button won't do anything at all. If you disable Logoff or Shut Down, you can give them passwords, so certain people can log off or shut down, but others can't.



The fifth tab of the Group Setup screen is called *Time Control*. This is where you set up the allowed length of this session, and whether that time limit is per day, per week, per month, or other options.

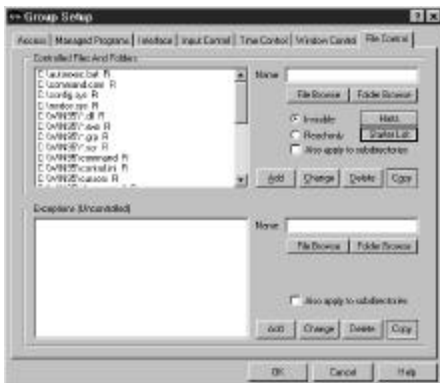
From here you can also set blockout periods, times when nothing will run. When this triggers, the user will see a screen saying "You're in a blockout period" and, until the blockout is over, nothing will run. That is, the screen stays there until the blockout period is over.

The sixth tab of the Group Setup screen is called *Window Control*. This is where you can set what should happen when certain windows appear. Full Control Internet can look for the main window of a program, or a dialog sub-window. When it appears, you can close it (in one of three ways), or you can make the user open or save from a particular folder, or you can automatically open or save using a generated file name. You can send keystrokes to a window to put it into a particular state. In the *Compliance Edition*, you can log keystrokes from a particular window.



Or you can do nothing. There are two reasons why you'd want to do nothing. You may want to log an administrator-defined Event Alert to the Remote Administration Manager when a certain window appears or event happens. Or you may want to set up an exception, perhaps to close all Options dialogs except from one particular program. To

do that, you'd set up one window control to close Options dialogs, and a second window control to do nothing to an Options dialog whose parent window is a program the user is allowed to use Options from.



The seventh tab of the Group Setup screen is called *File Control*. You can make files, folders or entire directory subtrees read-only or invisible. Or just certain files within them, for example, maybe you want to make all .doc files read-only for this user or group. You can also set exceptions to file control, for example so all .doc files will be read-only except for .doc files that are particular to this user. The exceptions mechanism is also how you can set up a per-user work area, even when multiple users share the same computer. The documentation describes this in detail.

You're done: We've now seen the entire process of setting up a clone settings file. Now that all your options are set, you can export the clone file and distribute it to your users.