

A hand is shown holding a clear plastic RJ45 network cable connector. The background is a soft, out-of-focus light color.

FULL ARMOR

**Enterprise
Policy
Management
Guide**

A collage of images related to IT and business. It includes a hand holding a network cable connector, a man in a suit, a computer monitor, a keyboard, and a mouse. The text "KEEPING PCs UP AND RUNNING" is overlaid on the collage.

KEEPING PCs UP AND RUNNING

Reducing the Total Cost of Ownership of Distributed Computing using Full Armor and Enterprise Policy Management

An executive guide by Thomas Pisello

Table of Contents

Preface.....	1
Introduction.....	1
1 The Total Cost of Ownership.....	2
The TCO of Distributed Computers.....	2
Formal and Informal Support Costs	3
Getting the Out of Control, Under Control.....	3
Applying Enterprise Policy Management to Reduce Costs.....	4
2 Enterprise Policy Management	6
Enterprise Policy Management Defined	6
Substantial Savings Using Enterprise Policy Management.....	8
Policy Management Using Microsoft Windows 9x and NT 4.0.....	9
Group Policy Management: Substantial Advancement in Windows 2000	9
3 Full Armor	13
Full Armor: Policy Management Made Easy.....	13
Full Armor – Enterprise Policy Manager	15
Full Armor Zero Administration – Keeping PCs Up and Running	15
Full Armor Network Configurator – Policy Management Made Easy.....	16
Step 1: User and Computer Classifications	17
Step 2: Interface Configuration and Lock-Down.....	18
Step 3: Creating Policies	19
Step 4: Enterprise Installation.....	20
Step 5: Maintenance / Updates.....	20
Full Armor Summary.....	21
Keeping PCs Up and Running	21
Maintain Y2K Compliance	21
Enterprise Policy Management Made Easy	21
Author's Biography.....	22

1 The Total Cost of Ownership

The TCO of Distributed Computers

The Total Cost of Ownership (TCO) of distributed computers has been documented in several studies to be much more expensive than originally expected. One of the primary reasons for the migration to distributed personal computers was to overcome the expense of mainframe computing. But studies by Gartner Group and other analysts over the past 10 years have placed today's annual expense for each Windows 95 computer at over \$9,500. When examining TCO, the expenditures for capital constitutes only 20% of the total, but the cost of labor to deploy, manage and support the environment contributes a whopping 80% of the \$9,500 annual cost. Direct management and support of the distributed computing environment costs over \$2,400 annually per computer, much more than the annual amortized purchase cost for hardware and software. To reduce these high costs, IS departments must focus on reducing the management and support labor burden, which contributes 25% to the TCO, and to reduce indirect user costs, constituting over \$4100 annually to the total per user costs.

	Annual cost per user
Direct Costs (budgeted)	
Hardware and Software	\$ 1,903
Management	\$ 1,354
Support	\$ 1,094
Development	\$ 345
Communications	\$ 610
Total Direct Costs	\$ 5,306
Indirect Costs (unbudgeted)	
End User Operations	\$ 3,357
Downtime	\$ 830
Total Indirect Costs	\$ 4,186
Annual TCO per User	\$ 9,493

Figure 1: From studies by GartnerGroup in 1998, the annual TCO per user of a typical Windows 95 corporate desktop is estimated to be just under \$9,500 annually. Mobile computer costs are some 56% higher, presenting an even greater management challenge and annual expense.

The TCO of each distributed computer is almost \$9,500 every year, with over 80% of the costs attributable to labor costs. These labor costs represent a great opportunity to reduce costs and improve the value of distributed computing investments.

Formal and Informal Support Costs

Support costs in the distributed computing environment have risen over the past three years as desktop systems continue to increase in capability and complexity, and more of the systems are located in remote offices and become mobile. Users are provided with an increasing array of applications and network capabilities, each having the equivalent of a small mainframe on their desks. With an average of two (2) help desk calls per month per user, and each support call costing \$15 on average, the cost of formal help desk and dispatched support can exceed \$360 annually per seat.¹

In the distributed environment, support is not only performed by the service desk and dispatched Tier II and III personnel, but is borne by users supporting themselves and each other. The personal computer provides the capability for anyone to be an administrator of their desktop or mobile system. Most support is obtained not through formal support, but by asking a neighbor or non-IS group PC expert for assistance (which usually involves several neighbors pitching in to assist), or figuring out the problem by yourself through costly trial and error. Peer and self-support have been found to cost most organizations over \$3,000 annually per user in lost productivity. Per incident, peer and self support typically costs 4:1 over formal support. The peer and self support comprises the majority of total support costs, and because it is user based, has proven very difficult to control and reduce.

The total cost of formal and peer/self support is a lofty \$3,700 annual expense.

Getting the Out of Control, Under Control

Distributed computing support costs have proven higher than expected. One of the most effective ways to get desktop TCO under control, particularly the high formal and informal support costs, is to proactively eliminate the reasons for the support need. Some help desk problems can be resolved through automation including password reset, while others can be resolved through break-fix maintenance contracts. But many of the support burden is generated by lack of configuration control for the distributed computers being supported.

Issues highlighting the lack of configuration control include:

1. Users who make errant changes to their configuration and settings which cause faults in the operating system or destroys access to key local and network resources;
2. Users who accidentally destroy important application or data files;
3. Users who are provided or install applications for which they are not trained;
4. Users who are provided more computing power and flexibility than they need for the job at hand.

¹ The cost per call in this analysis utilizes a total call cost which includes a fully burdened labor rate for Tier 0, I, II, and III support personnel. The calls are modeled to reflect that some are resolved by the help desk while others require dispatch to resolve.

A quick review of the help desk call logs will reveal that the majority of the issues can be traced to these types of configuration control problems. What would the annual savings be if you could eliminate 40% of these formal help desk calls, and also reduce the need for users seeking informal support?

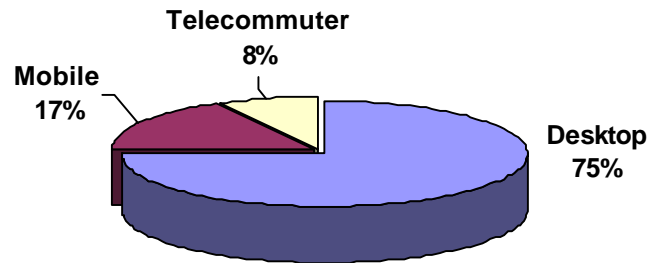
Almost 40% of support calls are related to configuration control issues, most of which can be prevented through pro-active policy management.

Applying Enterprise Policy Management to Reduce Costs

An organization can reduce formal help desk and dispatched support, peer/self support and downtime by providing a managed environment where users are provided computing configurations that are standardized and controlled, but aligned to their business needs.

Picture an organization where IS and business units would segment users to provide the right computing power for each user, and make sure that the systems proactively remained standardized. TCO could be reduced, while computing power is balanced to match user needs for flexibility and freedom. Data entry workers would be provided with policies that delivered an extremely limited application set and system flexibility, providing easy support and maintenance. Structured Task workers would be provided with a somewhat expanded application set but remain under tight control. High Performance and Knowledge workers would be provided with policies to enable a more unstructured work environment, but prevent accidental damage to the system and applications, and errant departure too far afield of supportable standards. Special policies would be deployed for telecommuters and mobile road warriors to provide additional control in these hostile and costly remote environments where support is not always readily available. These standardized configurations would be managed by a set of customized enterprise policies which provide various levels of lockdown, assuring that the configurations do not change and cannot be corrupted. Support and downtime are reduced, while productivity is maintained.

Worker Locations in a Typical Organization



Worker Types in a Typical Organization

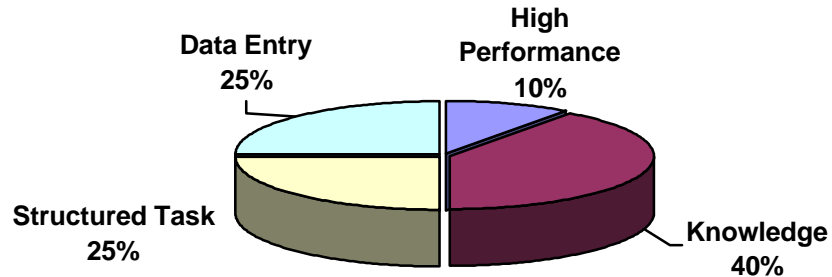


Figure 2: Workers in a typical organization can be classified based on job type and location as segmented by GartnerGroup stratification in 1998. Costs and requirements can be segmented to optimize planned spending against benefits. Enterprise policy management can be used to specify and control this segmentation.²

Enterprise Policy Management allows an administrator to establish standardization and control over the entire company's desktops and mobile computers. With policy management, distributed computer systems are grouped and managed such that users receive a standard configuration, and this configuration is maintained.

Providing Enterprise Policy Management based on user and computer type can help substantially reduce formal and peer/self support costs and downtime.

² In 1998 GartnerGroup uniquely defined users by type and location: High Performance Workers - dependent on technology for performing mission critical tasks (e.g., brokers, engineers); Knowledge Workers - add value and communicate information (e.g., marketing manager); Structured Task Workers - perform repetitive tasks as part of a workflow (e.g., accounting); Data Entry Workers -input data into computer systems (e.g., clerk); Mobile Workers - spend more than 50% of the time on the road; Telecommuter – spend more than 50% of the time from a fixed location outside of corporate offices.

2 Enterprise Policy Management

Enterprise Policy Management Defined

Policy Management provides various degrees of configuration control for the desktop. For all users, an IS Professional can establish policies that protect the operating and file system and settings from errant changes and deletions. For high performance and knowledge workers, policies can be established to deploy specific applications which are approved and assure that other applications are not installed. Furthermore, the installed applications are maintained from accidental change. For users who require a more basic computing environment, policies are established to simplify the look and feel of the Windows environment, only providing the applications needed to do the job at hand, and strictly enforcing this environment. Each policy is proactively enforced, not just tracking system and application changes, but preventing changes and errors before they occur.

Enterprise Policy Management enables an IS professional to take policy management to the next level, easily establishing and administering standardized configurations for the entire enterprise. Enterprise Policy Management enables these policies to be created and administered without having to visit each desktop. Any time a user logs on to the network, a new policy can be downloaded for automatic distribution and updating of corporate standards as they are changed.

Using tools that establish, lock down, and secure the PC's settings, Enterprise Policy Management provides the capability for IS professionals to enforce rules such as:

- Which applications a user has access to and appear on the desktop;
- Which applications a user can change or update on their own;
- What data a user has access to and can edit;
- Whether a user can install applications on their own;
- The look and feel of the PC interface, from a locked down browser, to a fully functional desktop;
- What directories data can be saved to;
- What network resources can be accessed and used;
- Which hardware devices (floppy disks, CD-ROMs) a user can access and use;
- Which CD-ROM titles a user can have access to;
- What printers the user can have access to;
- Which parts of the operating system, registry and settings can be edited;
- What scripts (startup and shutdown, and logon and log off) are enabled.

Enterprise Policy Management can be used to establish various levels of critical system protection, assuring that users can no longer change or delete critical system files or edit/destroy settings.

Enterprise Policy Management provides the ability to:

- Setup, deploy, and administer these standards for distributed computers across the network;
- Establish an interface for easy setup, deployment and administering of these policies across corporate computers and users whether they are in corporate offices, remote, mobile, or at home. Using this interface, unique policies can be easily created and enforced based on the standards for the entire corporation, type of user, the type of computer, the group the user works in or computer belongs to, the organization the user/computer belongs to, or any other unique classification the IS professional or business groups wish to create standards upon.

Enterprise Policy Management doesn't just lock down every PC and blindly apply limited functionality and restrictions on users. Enterprise Policy Management provides configuration control in a scalable fashion, providing just the right amount of management control based on user needs, balancing costs against freedom.

Enterprise Policy Management easily allows setup, deployment and administration of standardized PCs for the entire corporation.

Substantial Savings Using Enterprise Policy Management

Using Enterprise Policy Management, any organization can benefit through simplification of the computing environment, prevention of errant changes and maintenance of standard configurations. The annual TCO savings for organizations which have implement Enterprise Policy Management has been estimated by GartnerGroup to be 12.7%, or \$1,208 per user per year. In a mid-sized 2,500 user computing environment the PCs managed by Enterprise Policy Management best practices can save companies over \$3 million each year.

Windows 95 TCO	Typical annual TCO per user	Managed PC annual TCO per user	Annual Savings from Managed PC
Direct Costs (budgeted)			
Hardware and Software	\$ 1,903	\$ 1,903	\$ 0
Management (dispatched support)	\$ 1,354	\$ 1,096	\$ 258
Support (formal help desk)	\$ 1,094	\$ 964	\$ 130
Development	\$ 345	\$ 345	\$ 0
Communications	\$ 610	\$ 610	\$ 0
Total Direct Costs	\$ 5,306	\$ 4,917	\$ 388
Indirect Costs (unbudgeted)			
End User Operations (self and peer support, and futz factor)	\$ 3,357	\$ 2,769	\$ 588
Downtime (lost productivity)	\$ 830	\$ 598	\$ 232
Total Indirect Costs	\$ 4,186	\$ 3,366	\$ 820
Annual TCO per User	\$ 9,493	\$ 8,283	\$ 1,208
Savings (%)			12.7%

Figure 4: A Managed PC using Enterprise Policy Management best practices can deliver \$388 per user each year in direct IS staff savings due to the direct elimination of formal help desk and dispatched service calls. An organization can save an additional \$820 per user annually in increased end user productivity through the elimination of peer/self support, futzing, and downtime.

A Managed PC created using Enterprise Policy Management best practices can deliver \$1,208 in TCO savings per user every year!

Policy Management Using Microsoft Windows 9x and NT 4.0

In 1996 Bill Gates determined that Microsoft could help to reduce the rising cost of distributed computer ownership by providing administrators with tools to establish configuration control over desktops. In this manner, desktops could be configured with just the right views, menus, applications, and system flexibility. With a system that was simplified for lower end users, but more powerful and flexible for power users, administrators could deploy a single system to meet all corporate computing needs. This could avoid proposed migrations to simpler computing environments such as the Network Computer (NC).

From the need to decrease total ownership costs, Microsoft developed the Zero Administration Windows (ZAW) initiative to incrementally implement this strategy with each Windows release.

For Windows 95, 98, and NT 4.0, Microsoft developed the Zero Administration Kit (ZAK). ZAK used the embedded Windows policies to provide a very limited, restrictive lock-down. ZAK implemented the Policy Editor templates to enforce a strict operating environment.

With NT 4.0, using the System Policy Editor, an IS professional can create a system policy to control the look and feel of the users work environment, what actions a user could take, and the enforcement of system configuration settings for all computers running Windows NT Workstation and Windows NT Server. System policies are registry settings that define the behavior of various components of the desktop environment. The System Policy Editor, Poedit, assigns policies based on User, Group, or Computer within the organization.

***Microsoft's Zero Administration Kit provided basic implementation
of policies for Windows 9x and NT 4.0.***

Group Policy Management: Substantial Advancement in Windows 2000

Zero Administration Windows advances in Windows 2000 (formerly NT 5.0) with the introduction of Group Policy Management. Microsoft defines Group Policy Management as “the ability for the Administrator to state a wish about the state of their Users environment once, and then rely on the system to enforce that wish.”

In Windows NT 4.0, you could use the System Policy Editor tool to configure user and computer settings stored in the Windows NT Registry database. But as discussed in the previous section, policies were difficult to edit and establish for the entire enterprise, and were not as comprehensive as IS professionals needed to establish complete configuration control.

To resolve this issue Windows 2000 introduces the Group Policy Editor, a tool that extends the functionality of the NT 4.0 System Policy Editor providing enhanced capabilities for configuring settings for groups of computers and users. With the Group Policy Editor an administrator can establish more powerful and flexible policies for software distribution and management, user documents, scripts and settings. Group Policy Editor is a Microsoft Management Console snap-in that includes built-in features for setting Group Policies. Group Policies define the various components of the user's environment that system administrators need to manage, and include software settings, application deployment options, scripts, user settings and document options, and security settings. Using Windows 2000 policies, an IS professional can install, assign, publish, update, repair, and remove software for groups of users and computers. An IS professional can also use the User Documents and Settings extension to add files, shortcuts, or folders to special folders that represent the user's desktop.

Group Policy Management in Windows 2000 utilizes two different settings for users and computers:

- *Computer Settings* include policies that specify operating system behavior, desktop appearance, application settings, assigned applications, file deployment options, security settings, and computer startup and shutdown scripts. Computer-related Group Policies are applied when the operating system initializes;
- *User Settings* include all user-specific information such as operating system behavior, desktop settings, application settings, assigned and published applications, file deployment options, security settings, and user logon and logoff scripts. User-related Group Policy is applied when users log on to the computer.

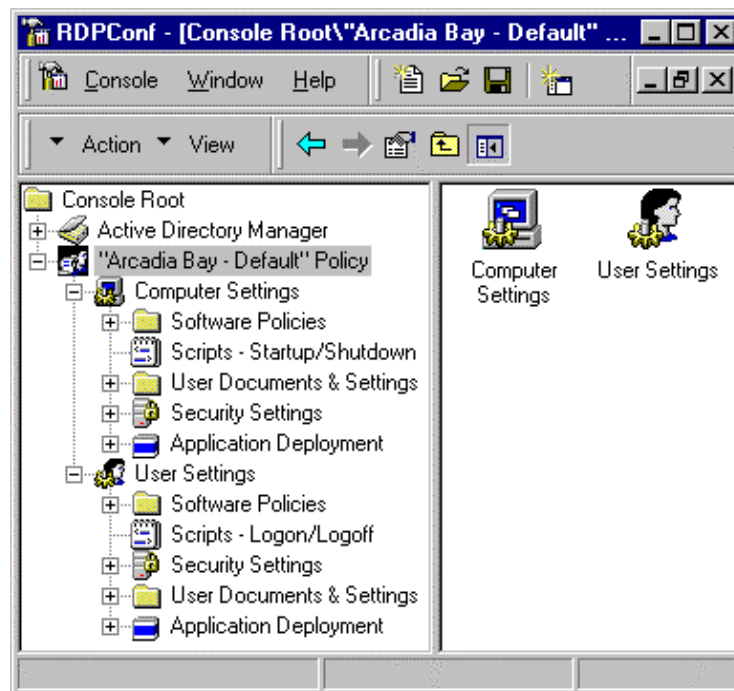


Figure 5: The Group Policy Editor provides for creation of Group Policy Objects (GPOs) using a graphical user interface. Policies are set for computers and users. The policies are assigned to specific sites, domains, organizational units, groups and users by creating policies in the correct location in the Active Directory. By default, these policies are active, they are inherited and they are cumulative, but can be filtered using membership in a security group (ACL controls).

Group policies include the following options based on Computers or Users:

Computers	Users
Application Data	Application Data
Desktop look and feel	Desktop look and feel
Start Menu	Favorites
Programs Startup	Local Settings
	My Documents My Pictures
	Network Neighborhood
	Printer Neighborhood
	Send To
	Start Menu
	Programs Startup

Group Policies in Windows 2000 work hand in hand with the Active Directory Services to distribute and determine the policies for users and computers. Therefore, Active Directory Services *must* be enabled. Using the Active Directory and Group Policies, the IS professional can establish policies for the corporation, business units, organizations, and user groups, using login, inheritance and security settings of the directory structure to help deploy and manage these policies automatically across the enterprise. For each policy to be in effect, security to accept or block the policy from being used are set for each set of users, groups and organization units in the active directory structure.

Microsoft has implemented a powerful engine in Windows 2000 for creating and distributing group policy management, but these policies can be difficult to manage and debug for an enterprise deployment.

The Group Policy Editor provides detailed control of various policy settings but does not provide assistance for an IS professional who wants to establish settings for many users in a typical enterprise environment. Key questions are difficult to answer without proper guidance and support including:

- How do I segment computers and users in my enterprise?
- Which policies should be established per user or per computer type?
- How much or how little control should I establish?
- Where should the policy control files (called Group Policy Objects - GPOs) be deployed in the Active Directory Hierarchy and Domain structure?
- Once established, within the complex hierarchy of the active directory, inheritance rules and security administration how can I be sure the policies I wanted to establish are in effect?

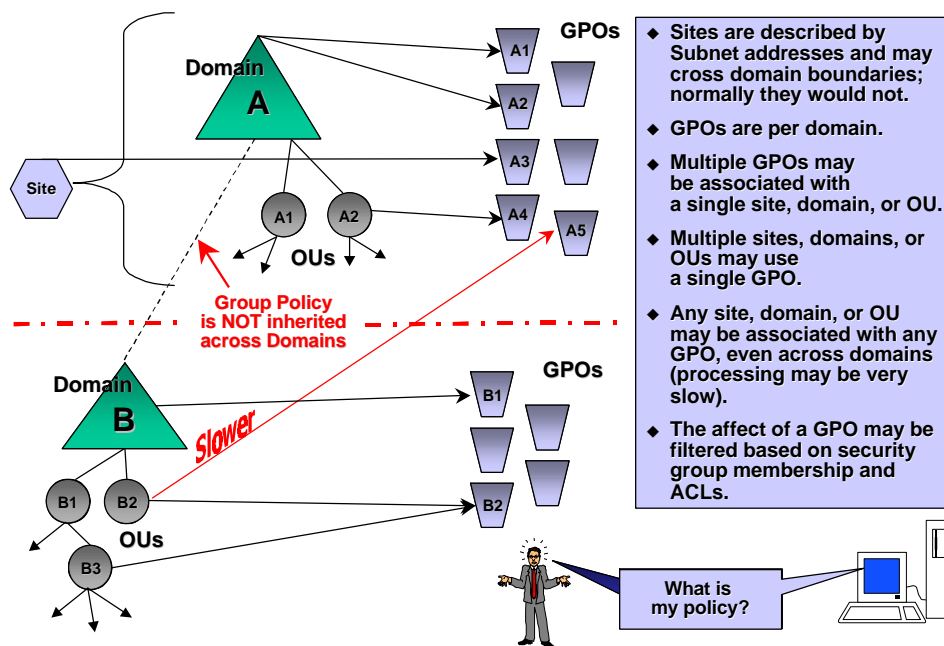


Figure 6: As can be seen by this diagram, Policy Management is very powerful, but is also very complex. An administrator must be cognizant of users, computers, OUs, domains, inheritance rules, and security to setup, deploy and administer policies. Even then, it is often difficult to determine which policies are indeed in effect for any user, or why policies are loading slow across the system. If policy management could provide all of the benefits, but be abstracted from this complexity using the intelligence of a management program, policies could be setup, deployed and administered more effectively and less expensively.

In a Windows 2000 environment, we have seen that powerful tools have been provided for establishing policies for the PCs. According to Microsoft however, “the Windows 2000 Group Policy Editor tool does *not* provide client support for Windows NT 4.0 and computers running Windows 95 and Windows 98.” This will unfortunately require IS professionals to utilize two administrative tools for setting up and deploying policies in a mixed Windows environment, and in the mixed environment, policies will not utilize the Active Directory for distribution, inheritance and determination of the policies.

Group Policy Management in Windows 2000 implements advanced policy management features and administration using Active Directory Services, but, policies are still difficult for IS professionals to understand, setup, deploy, and manage. Moreover, IS professionals can only get the new features in Windows 2000, as Windows 9.x and NT 4.0 are not supported.

3 Full Armor

Full Armor: Policy Management Made Easy

Microsoft recognizes that policy management is a very effective method to reduce costs. The Zero Administration Windows initiative has advanced since its inception in 1996 to provide the tools to help IS professionals configure and control desktop configuration for lower TCO. With these initiatives however, several issues with Microsoft's Zero Administration Windows policy management are present:

- Different tools are required for an IS professional to setup, deploy, and administer policies on Windows 95, Windows 98, NT 4.0 and Windows 2000;
- Policy management capabilities are different amongst the various operating system platforms ;
- Policy management tools do not provide a roadmap for an organization to easily determine how various users and computers should get certain policies and provide easy tools to deploy these standard policies;
- Application protection on Windows NT 4.0 requires NTFS be enabled. Many organizations cannot enable NTFS on all systems and will require a reformat of the hard drive. Application protection is not enabled with Windows 95 or 98;
- Policy management on Windows 2000 requires that active directory be enabled;
- Tools do not provide an easy way to protect standard application configurations;
- An IS professional must be intimate with the domain and security structure in order to properly establish and deploy policies;
- It is very difficult for a support person to determine which policies are set on a given client;

Full Armor embraces and extends Microsoft's policy management engine and tools into true Enterprise Policy Management. Improvements that Full Armor provides include:

- A single administrative tool, Full Armor Network Configurator is provided to setup, deploy, and administer policies across Windows 95, 98, and NT 4.0, as well as Windows 2000;
- Full Armor Network Configurator delivers tools to guide users through corporate setup, deployment, and administration of policies according to an easy to use implementation roadmap, preset policies for user and computer types (based on standard classifications from the GartnerGroup), a certification class, and with the release of Windows 2000, the inclusion of application templates for easy protection and configuration control of various desktop applications;
- A single client tool, Full Armor Zero Administration is provided to deliver a common set of advanced policies across all platforms, standardizing and extending the basic client policies for Windows 9x and NT 4 platforms, and adding several additional features to the advanced set of embedded Windows 2000 policies;

-
- Active Directory and NTFS are supported but not required to implement policies or application lockdown, enabling deployment to occur easily in mixed environments without costly reformats or reconfigurations;
 - Full Armor Network Configurator abstracts implementation issues with the active directory, domains, and inheritance making policies easier to setup and deploy across the enterprise;
 - Microsoft policy management editing, active directory, security, policy management files, policy distribution, and MMC are utilized to maintain and extend Microsoft's standards and provide for enterprise scalability;
 - Compliance with Desktop Management Interface (DMI) 2.0 and Web Based Enterprise Management (WBEM) for remote diagnostics and management of policies;
 - Full Armor Zero Administration provides a utility for identifying which policies are implemented on the desktop, taking the mystery out of active directory inheritance, security and policy administration (Windows 2000 release);
 - Full Armor Network Configurator provides administrative tools to enable support personnel to view which policies are implemented (Windows 2000 release)
 - Full Armor provides the only Enterprise Policy Management training and certification courses (Managed PC Certification) and implementation services so IS professionals can learn about planning, setup, deployment, and administration of Enterprise Policy Management using Microsoft policies and Full Armor administration and configuration tools, and obtain various levels of consulting assistance.

Microsoft delivers good policy management components and tools. Full Armor embraces and extends what Microsoft provides making it better. Full Armor delivers software tools, training, and services to make policy management easier.

Full Armor – Enterprise Policy Manager

Full Armor is comprised of two software tools to automate Enterprise Policy Management in order to keep all your PCs up and running:

- **Full Armor Zero Administration:** the client tool for implementing a standard set of advanced policies across all Windows platforms including: Windows 95, Windows 98, Windows NT 4.0 and Windows 2000;
- **Full Armor Network Configurator :** the network management tool that makes policy management easy, controlling Full Armor Zero Administration's settings on client PCs throughout the organization.

***Used together, FULL ARMOR ZERO ADMINISTRATION
and FULL ARMOR NETWORK CONFIGURATOR provide the
client and network configuration management tools necessary to implement
Enterprise Policy Management quickly and easily in your enterprise.***

Full Armor Zero Administration – Keeping PCs Up and Running

The Full Armor Zero Administration software provides client configuration control using policy management. Full Armor Zero Administration works quickly and easily to set policies on most corporate PC clients, providing advanced policy management for Windows 9x, NT 4.0 and Windows 2000. Full Armor Zero Administration provides the following features:

- **Protecting the Operating System:** Key system files and settings can be protected and can no longer be edited and destroyed;
- **Protecting the File System:** Specific files, directories, and drives can be protected. For instance, administrators can protect the standard applications and related files from being accidentally deleted, changed, moved, or edited. Application installation can be restricted assuring that only standard applications are installed. Workspace for each user can be established to maintain standard file structures and document storage. Once established, Year 2000 compliance can be easily maintained and proactively ensured;
- **Desktop Look and Feel:** Configuring the look and feel of the desktop to provide a scalable interface based on user sophistication and capability. A user can be presented with a completely locked down desktop, a simplified interface, or the standard desktop. Administrators can control scripts, icons, application lists, start-up menu and programmable desktop look and feel setting;
- **Scripts (Windows 2000 release):** Provides for management and distribution of the computer startup and shutdown scripts, and user logon and logoff scripts;
- **Installed programs and documents (Windows 2000 release):** Provides for the distribution of application settings, assigned applications and file deployment options;
- **Restricting the use of Removable Media Devices.** Floppy drives, CD-ROMs, and network drives can be selectively locked out from user access. The CD-ROM protection takes the protection a step further by allowing administrators to only allow authorized CD volume labels to be read;

- **Policy Inheritance.** Full Armor Zero Administration inherits and extends Windows policies;
- **Recovery.** Full Armor Zero Administration includes an Undo32 feature that allows for the quick recovery of the PC configuration settings such as the registry, INI files, Start menu, shortcuts, and other critical files that the administrator chose not to protect;
- **Easy Setup and Administration:** Policy management is provided consistently across all Windows platforms, delivered without having to reformat, and without needing Windows 2000 and Active Directory. Policies work with servers including NT server, as well as NetWare, Banyan, and Unix. Tools are provided to easily see which policies are in effect and provide remote diagnostics and management;
- **Mobile User Support** – Full Armor fully supports mobile users for enhanced control and support for these expensive environments.

Full Armor Zero Administration keeps PCs up and running with powerful and easy to use PC configuration control tools

Full Armor Network Configurator – Policy Management Made Easy

How can you easily establish policies for your users and groups? Where do you start? How do you deploy policies enterprise wide? How can you setup, deploy, and implement policies across all Windows and NT platforms using a single management tool?

Full Armor Network Configurator provides IS professionals with the tools to easily implement Enterprise Policy Management using Full Armor Zero Administration.

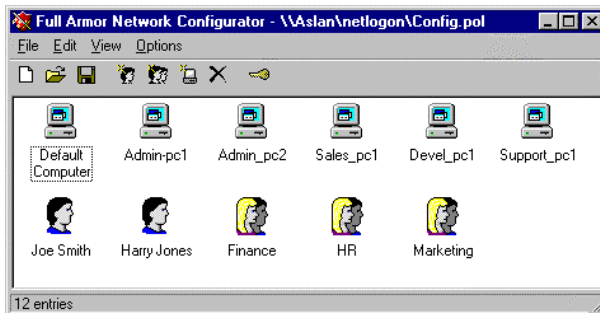


Figure 7: Full Armor Network Configurator provides the tools and profiles to setup, deploy, and manage policies enterprise wide. Profiles are established for various users and groups, and the policies are automatically distributed. When Windows 2000 is released, this interface migrates to an MMC that is integrated with Active Directory to enhance the Group Policy Editor, providing a single interface for all policies regardless of target system, abstracting the complexities of domain structure, inheritance, accumulation, and security lists.

Full Armor Network Configurator provides tools for the easy setup, deployment, and administration of policies. Full Armor Network Configurator manages policies for users and groups from a centralized location, providing tools to help a novice administrator determine which policies to establish, which groups and users to assign, and abstracts the administrator from needing to know where and how to copy policy files to enable deployment.

In working with large corporate customers, the Full Armor team developed a five step deployment guide that has been implemented into the software, and is taught in the Managed PC Certification training class. It has been found that companies who follow these steps can implement Enterprise Policy Management faster and more effectively.

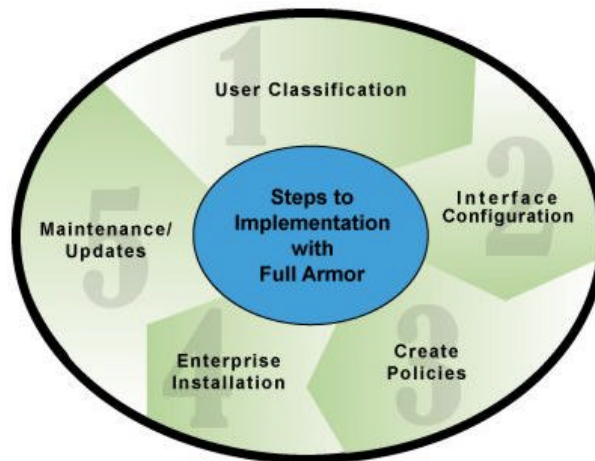


Figure 8: Full Armor has developed, as part of the Managed PC Certification training course and FULL ARMOR NETWORK CONFIGURATOR software, a five step process for Enterprise Policy Management

The steps to implement Enterprise Policy Management are briefly described as follows:

Step 1: User and Computer Classifications

In the computing environment there are many different types of users with different computing requirements and standards. Furthermore, there are many different types of computing platforms and locations. How do you take each unique user and computer into account when developing policies? Where do you begin? Classifying and grouping various user groups and computers is the first step in implementing Enterprise Policy Management. Full Armor utilizes and extends the GartnerGroup classifications of user and computer types to help classify users into the correct category.

The classifications for user type are:

- **High Performance Workers** - dependent on technology for performing mission critical tasks (e.g., trader, financial analyst, development engineers);
- **Knowledge Workers** - add value and communicate information (e.g., product manager, marketing manager, technical consultant, supervisory manager);
- **Structured Task Workers** - perform repetitive tasks as part of a workflow (e.g., accounting) ;
- **Data Entry Workers** -input data into computer systems (e.g., clerk).

The classifications for computer type are:

- **Corporate Desktop** – a desktop PC that is stationary and is located at a corporate office with on-site dispatched support;
- **Remote Desktop** – a desktop PC that is stationary and is located at a corporate office that does not have dispatched support locally;
- **Mobile Workers** - spend more than 50% of the time on the road;
- **Telecommuter** – workers who spend more than 50% of the time from a fixed location outside of corporate offices;
- **Kiosk or Demo PC** – a computer dedicated to demonstration or kiosk operations;

These categories represent a good starting point for standardization using policies. From these categories, additional policies can be created and refined.

Step 2: Interface Configuration and Lock-Down

Based on the type of user and type of computer, Full Armor provides templates that administrators can use to lock-down and/or configure the PC:

User Type	Full Armor Enterprise Policy
High Performance	Basic including System protection Installed Application Protection, and Undo32 (recovery tools)
Knowledge	Advanced including all aspects of Basic plus additional restrictions for Application installations, defined workspace, and optional Soft-NetPC configuration (disable floppy and CD-ROM)
Structured Task	AppStation which locks down the PC and configures the look and feel of the desktop for a limited set of applications and very tightly defined workspace
Data Entry	TaskStation which completely locks down the PC and configures the PC to boot into a single program, often implemented with a browser interface

Computer Type	Full Armor Enterprise Policy
Corporate Desktop	Basic including System protection Installed Application Protection, and Undo32 (recovery tools)
Remote Desktop	Advanced including all aspects of Basic plus additional restrictions for Application installations, defined workspace, and optional Soft-NetPC configuration (disable floppy and CD-ROM)
Mobile and Telecommuter PCs	Firewall which locks down the PC and configures the look and feel of the desktop for a limited set of applications and very tightly defined workspace
Kiosk and Demo PCs	TaskStation which completely locks down the PC and configures the PC to boot into a single program interface.

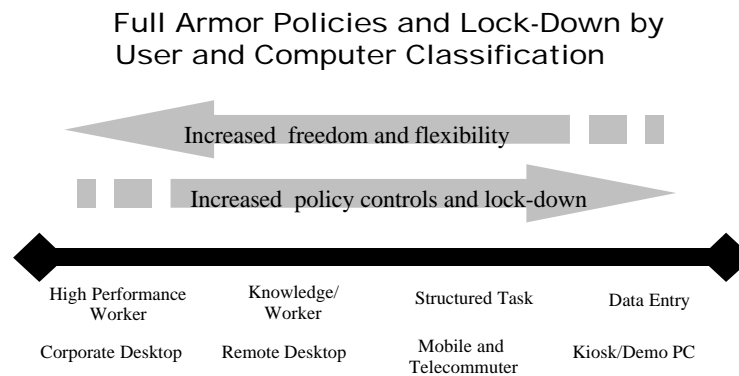


Figure 9: Full Armor provides a classification system and templates for easily creating and assigning policies based on user and computer type. Using these policies, the correct level of control and freedom can be assigned to reduce costs while maximizing user capabilities. Full Armor provides, as part of the Managed PC Certification course, an interview questionnaire to assist in classifying users into these categories.

Step 3: Creating Policies

Using Full Armor Network Configurator, policies are created for Organizations, Groups, Users, or Computers. These policies utilize the templates provided, which divide users and computers into initial classifications. The IS professional can then further define and classify users, and create additional policies for individual organizations, groups, users, or computers.

Step 4: Enterprise Installation

To enable each PC to have a similar policy management system with maximum flexibility and control, the Full Armor Zero Administration client is deployed enterprise-wide. This is done easily through a login script, batch file, or third party software installer.

Once Full Armor Zero Administration is deployed, policy setup, deployment, and administration is automatic through Full Armor Network Configurator, with downloads of the latest policies maintained based on login and updates over the network. These policy downloads can be flexibly managed for mobile and telecommuters to avoid login delays and traffic.

Step 5: Maintenance / Updates

Full Armor Network Configurator can be used to modify and update policies as the computing standards and user organizations change. The policies are automatically placed, and update the client via the network login process. Policies are maintained and deployed centrally and automatically.

The Full Armor Zero Administration client can be maintained and updated in the same manner as it is deployed when updates occur. For technology refresh, Full Armor has a utility that allows administrators to temporarily turn off the protection, update/install the client applications, and turn the protection back on.

Full Armor Zero Administration supports DMI v2.0 and WBEM allowing remote viewing, monitoring and control of each desktop's policies for easy troubleshooting and repair.

Full Armor Network Configurator, Managed PC Certification training, and implementation services make Enterprise Policy Management easy. Setup, deployment, and administration is simplified and automated.

Full Armor Summary

Full Armor and Enterprise Policy Management

According to industry estimates, the annual Total Cost of Ownership (TCO) of a corporate PC is between \$5,000 and \$13,200. Corporations and their system administrators are challenged to find a way to reduce these costs, by eliminating costly technical support calls, end-user downtime, and changes to system configuration settings. Full Armor meets this challenge by providing enterprise level software and services to establish and maintain PC system and software configurations. Full Armor software proactively enforces PC standards, maintains Y2K compliance, and lowers the Total Cost of Ownership. According to GartnerGroup, a Full Armor Managed PC can deliver \$1,210 in TCO savings per PC every year.

Keeping PCs Up and Running

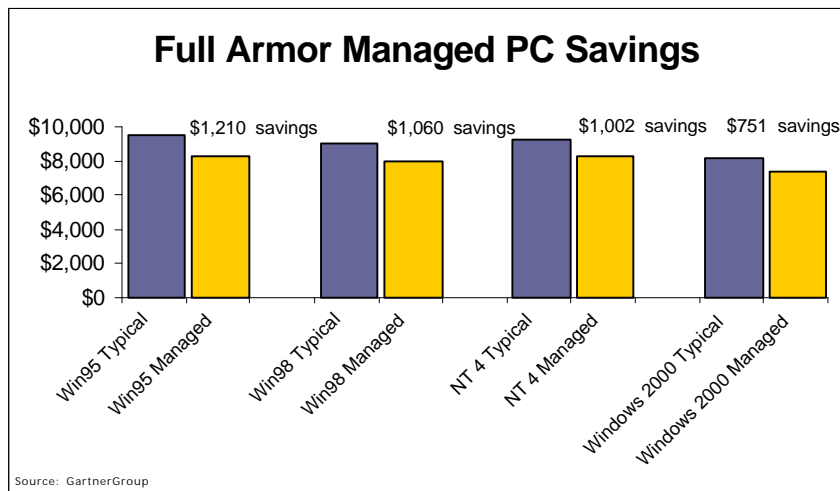
- Customizable lockdown based on user types and rules
- Framework for balancing end user needs vs. IT manageability
- Lowers TCO - Support and Downtime

Maintain Y2K Compliance

- Enforces approved configurations
- Eliminates application regression

Enterprise Policy Management Made Easy

- Easy setup, deployment, administration and extension of Microsoft's policies
- Heterogeneous management and control
- Certification training
- "Jumpstart" support services



Author's Biography

Thomas Pisello is currently serving on the advisory board of Full Armor Corp.

Thomas Pisello is a co-founder of Spiral-Up, a provider of Resource Capital to high technology start-up companies, with services which include business development, marketing, and public relations.

Prior to Spiral-Up, Mr. Pisello served as Managing VP for the GartnerGroup. Mr. Pisello led a team transforming the traditional GartnerGroup research, models, and methodologies into automated decision support tools for Information Technology (IT) strategy development and management. At GartnerGroup, Mr. Pisello was recognized as one of the thought leaders in the areas of Total Cost of Ownership (TCO) and Return on IT Investments. Mr. Pisello was involved in software M&A activities, helping review, evaluate and acquire software companies.

Mr. Pisello joined GartnerGroup when the company he founded in 1994, Interpose, was acquired by GartnerGroup in February of 1998. Prior to the acquisition, Interpose grew with Mr. Pisello as CEO, to a profitable organization pioneering consulting tools for IT financial analysis and decision support. At Interpose, Mr. Pisello worked strategically in sales and marketing programs for Microsoft, Compaq, Dell, Novell, Entex, Inacom and many other IT vendors and service providers.

Prior to Interpose, Mr. Pisello held a number of key management and software engineering positions, serving as a Product Line Director for Seagate Software (formerly Conner Peripherals), Conner Peripherals, Archive, and Maynard Electronics where he helped develop storage and network management solutions for distributed computing environments.

Mr. Pisello holds a BSEE from the State University of New York at Buffalo, and a Management degree from Rollins College, Winter Park, FL. He holds five software patents, serves on several advisory boards for software start-up companies, and has written books (The Economics of Distributed Computing, Pisello and Kirwin, 1999), articles, and presented on various financial, management, and Information Technology topics.
