realtimepublishers.com®

The Definitive Guide™ To

Securing Windows in the Enterprise

SCRIPTLOGIC

Don Jones

Copyright Statement

[**Editor's Note:** This eBook chapter was downloaded from Content Central. To download other chapters from this eBook, please visit http://cc.realtimepublishers.com/portal.aspx?pubid=335.]

Chapter 2: Securing Clients

Client computers are often neglected when it comes to security. Everyone tends to focus on servers, and, let's face it, servers are definitely easier to secure. In addition, servers exist in data centers or other protected locations and are tended to by trained administrators. Client computers, in contrast, sit on the desks and in the carrying bags of mere users, and are subjected to every imaginable stress: physical security threats, spyware, viruses, airports, hotels, and so on.

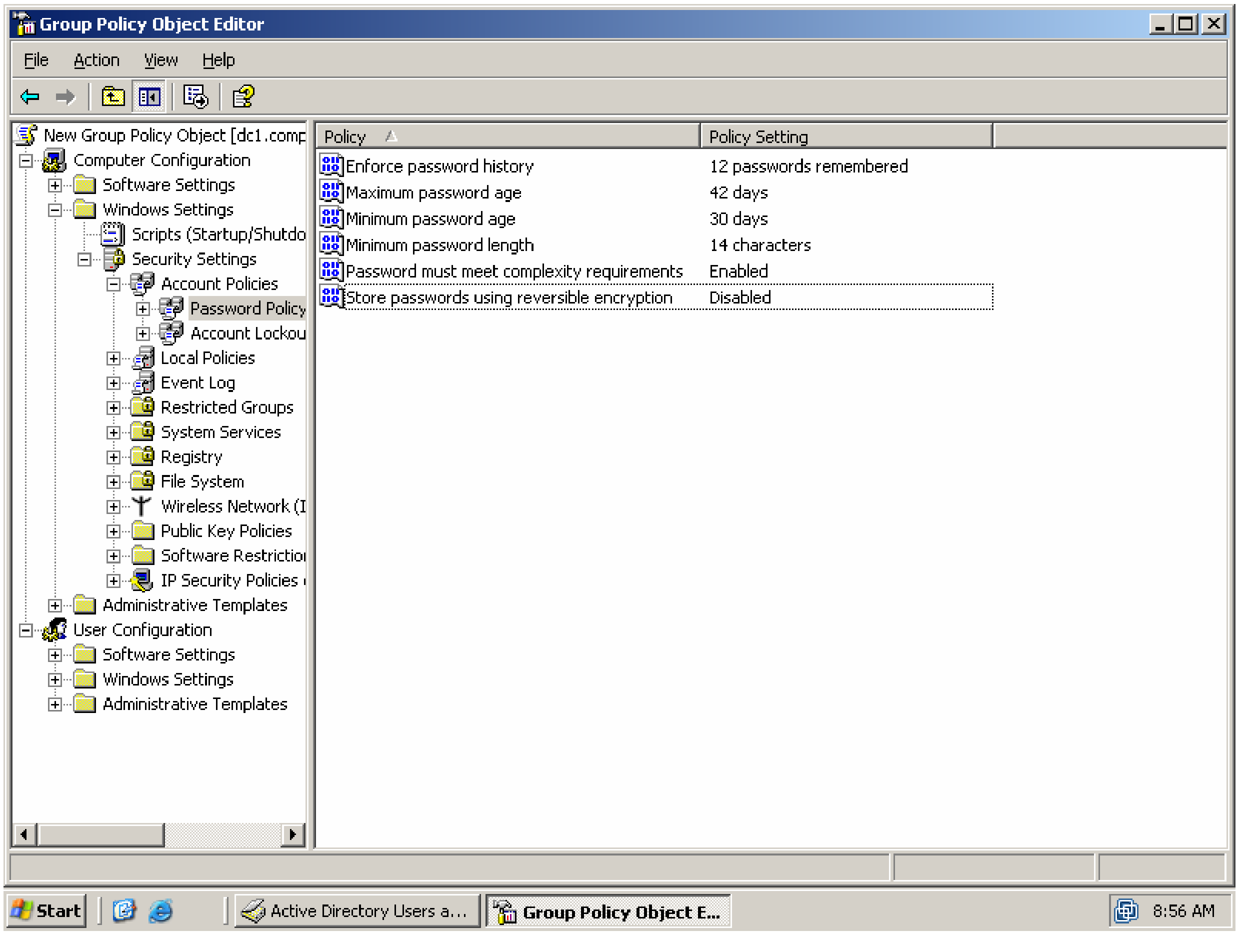
The reality is that client computers can hold just as much critical information as servers. On their client computers, users store local copies of files (the *only* copy of those files, in some cases), use Windows' Offline Files features to retain copies of server-based data, and so forth. The amount of corporate information stored in users' mailboxes, for example, is staggering—as much as 70 percent, according to a recent survey by VERITAS. Corporate confidential data is more likely to be compromised from a client computer than from a server, yet client computers typically have the least amount of security and the poorest, from a security viewpoint, configurations. This chapter will highlight some of the major security concerns affecting client computers, and give you ideas about how to address them.

Local Accounts and Passwords

Local user accounts exist on every Windows computer except domain controllers, and client computers' local accounts are one of the most-overlooked security issues in any enterprise. For example, every computer has a local Administrator account, which has complete and total control over nearly everything on that computer—including the profile contents for domain users who utilize the computer. Simply gaining access to the local Administrator account can therefore provide access to a great deal of domain information, even though the local Administrator account doesn't have direct access to anything in the domain.

> If the local Administrator account is compromised, a keystroke logger could be installed, enabling the hacker to compromise credentials of other users that may have access to sensitive data on the servers. There are software utilities, such as PestPatrol, available that can scan for keystroke logging tools.

Some organizations will take the time to configure local account policies, governing the maximum age, minimum length, and other restrictions for the local accounts. This process is simple, as Windows Group Policy allows you to do so through Active Directory (AD). Figure 2.1 shows an open Group Policy Object (GPO) that is linked to an organizational unit (OU); every computer within this OU will be affected by the password policy configured in the GPO.



Policy	Policy Setting
Enforce password history	12 passwords remembered
Maximum password age	42 days
Minimum password age	30 days
Minimum password length	14 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Figure 2.1: Configuring password policy in a GPO.

However, local accounts aren’t used all that often in many environments. If an account—such as Administrator—isn’t used, then its password will never be changed and it remains a security liability. Perhaps the most common way of dealing with this local account security issue is to simply ignore it, creating one of the biggest issues in client computer security. Many organizations take half the time on local account management than they spend managing their domain accounts, yet those local accounts can have access to just as much sensitive data.

Local computer accounts don’t have direct rights to resources stored in a domain. But when domain information is copied to a local computer, local accounts—especially the Administrator account—can gain access to it, essentially bypassing domain security (from a business viewpoint, at least) now that the file is under the computer’s local security.

One way to quickly deal with the issue is to write a short script. The following VBScript, for example, can be used to change the local Administrator password on a remote computer:

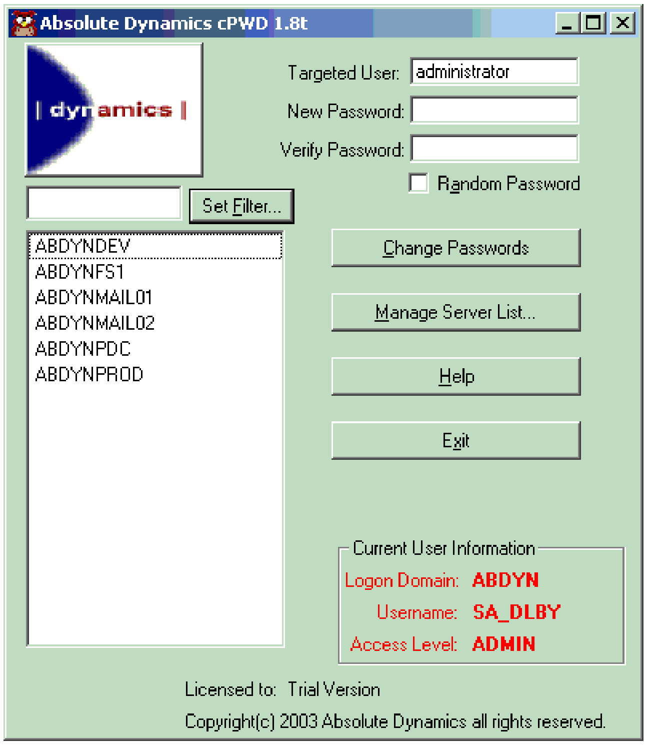
```
sComputer = "client1"
Set oUser = GetObject("WinNT://" & sComputer & "/Administrator,
user")
oUser.SetPassword "N3wP@ssw0rd!"
oUser.SetInfo
```

Naturally, this isn't a terribly useful tool because it only changes one computer at a time. A more powerful version of this script would read all of the computers from a file, listing one computer per line, and change their local Administrator accounts:

```
Set oFSO = CreateObject("Scripting.FileSystemObject")
Set oTS = oFSO.OpenTextFile("C:\Computers.txt")
Do Until oTS.AtEndOfStream
 sComputer = oTS.ReadLine
 Set oUser = GetObject("WinNT://" & sComputer & _
  "/Administrator,  user")
 oUser.SetPassword "N3wP@ssw0rd!"
 oUser.SetInfo
Loop
oTS.Close
```

However, this solution is still not ideal. It requires that you maintain a huge list of client names—a task that makes it easy to miss one. In addition, any computer that isn't available (turned on) when you run the script won't be updated—in fact, this script will crash on the first unavailable computer. It's possible to change the script so that it will log unreachable computers, and you can even have it read computer names from AD. However, even this solution doesn't address all the shortcomings. AD too often contains old computer accounts, and might not contain the name of *every* computer in your environment (standalone lab computers, for example). Smart organizations will rename the local Administrator account, but might not have done so consistently on every computer. In this situation, you need to change the password of an account whose name you don't even know—a difficult task!

Commercial tools can do a better job in many cases. For example, Absolute Dynamics' cPWD can change passwords on multiple computers, and even target computers on which the Administrator account has been renamed. As Figure 2.2 shows, multiple computers have been targeted to have their local Administrator password changed.



Targeted User: administrator
New Password:
Verify Password:
☐ Random Password

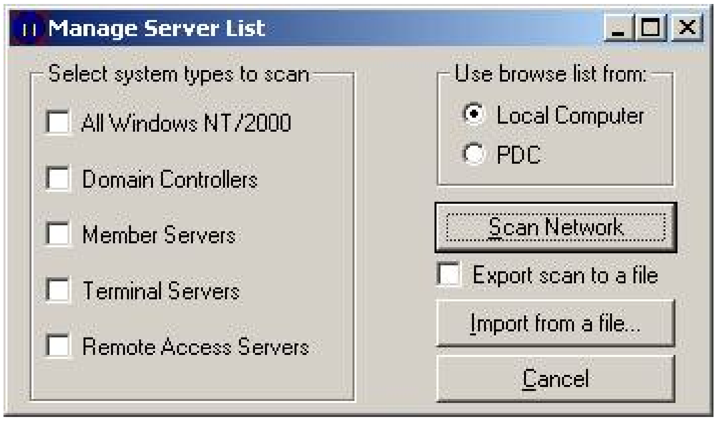
ABDYNDEV
ABDYNFS1
ABDYNMAIL01
ABDYNMAIL02
ABDYNPDC
ABDYNPROD

Current User Information
Logon Domain: ABDYN
Username: SA_DLBY
Access Level: ADMIN

Licensed to: Trial Version
Copyright(c) 2003 Absolute Dynamics all rights reserved.

Figure 2.2: cPWD makes changing local accounts easier.

Simply entering *A* for the account name will target the local Administrator account by its security identifier (SID), regardless of the account’s actual name. The tool is designed to target a list of computers, but has the capability to dynamically generate that list, as Figure 2.3 shows.



Select system types to scan
☐ All Windows NT/2000
☐ Domain Controllers
☐ Member Servers
☐ Terminal Servers
☐ Remote Access Servers

Use browse list from:
● Local Computer
○ PDC

☐ Export scan to a file

Figure 2.3: Dynamically targeting computers to change local account passwords.

This scan is performed through the browse master, meaning it will pick up only those computers that are online at the time. Computers that are offline will be missed, and you’ll need to pick up those separately—perhaps by running the scan several times each month to get as many computers as possible.

> ☞ Like so many security issues that affect client computers, local account passwords are a problem on member and standalone servers, too, and the same solutions can be used to help solve the problem.

Service Management

Services are another area in which client computers can present security difficulties. Client computers come with several pre-enabled services, many of which can be disabled entirely. Even those services you choose to leave running, however, present security risks when configured to run as an over-privileged account or when configured to run as an account whose password is never changed. Of course, Windows doesn't make it easy to keep service accounts properly configured, so you'll need you use some creativity.

Unnecessary Services

Every service in Windows is necessary to *someone*—Microsoft didn't include any services that do nothing all the time in every environment. By unnecessary services, I'm referring to services that provide features or capabilities that *many* environments don't utilize. Why disable these services? History tells us that eventually a bug will be discovered in one of these services that will allow attackers to perform any number of heinous acts on the computer. By disabling services that you're not utilizing, you'll help prevent these services from becoming an attack vector in the future.

Disabling a service is easy. Simply right-click My Computer, select Manage, then open the Services node in the left-hand tree view. You can double-click any service to change its startup type to Disabled, and you'll be able to stop the service if its running. Once set to Disabled, a service can't be started unless its startup type is first changed to Automatic or Manual.

☞ For even more security, uninstall the service if possible. For example, rather than just disabling Internet Information Services (IIS), uninstall it from the Add/Remove Windows Components utility in the Control Panel (accessed through Add/Remove Programs). Most built-in services can't be removed in this fashion, but some can, and by removing the software you'll eliminate the potential for someone to re-enable and start the service.

The following list of services—some of which are disabled by default—I recommend disabling (and, if possible, removing):

✎ A few of the services exist only on server computers; to ensure network security, they are included in this list for your reference.

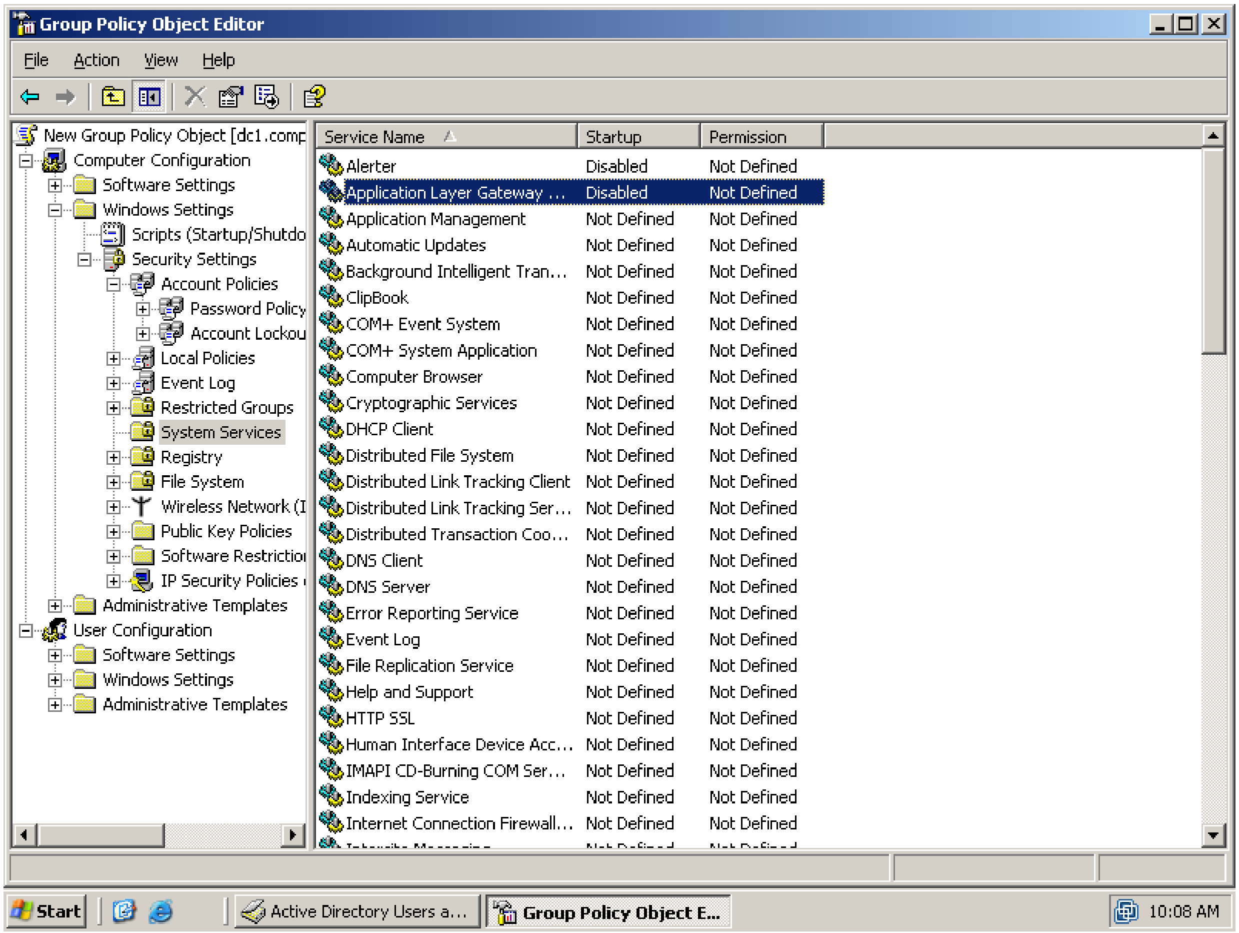
- Alerter—This service allows the computer to send and display certain types of alerts; primarily used with older software from the Windows NT days.
- Application Layer Gateway Service—This service is not required after Windows XP SP2 is installed.
- ClipBook—This service is an extension of the Windows Clipboard functionality and is disabled by default.
- Computer Browser—This service maintains a listing of network computers and resources; servers will typically provide this functionality, and clients shouldn't typically run this service. If you have a good DNS infrastructure and your users aren't accustomed to "browsing" the "network neighborhood," disable this service on all machines.
- Error Reporting Service—This service provides a pop-up dialog box that offers to transmit errors and application crashes to Microsoft; it is unnecessary.

- FTP Publishing—This service is part of IIS. It is generally not appropriate for a client computer to be hosting an FTP site, so this service can be disabled and uninstalled.
- Human Interface Device Access—Usually disabled by default anyway, this service is necessary only for certain complex keyboards and other interface devices.
- IIS Admin—Part of IIS and rarely needed on client computers, this service can be disabled and uninstalled.
- Indexing Service—This service provides indexing of files on the local drive for faster searching; it is rarely used by most users and is therefore a good candidate for disabling.
- IPSec Services—This service is necessary only if you're using IPSec or L2TP Virtual Private Networks (VPNs).
- Message Queuing—This service is necessary only for applications that utilize Microsoft Message Queue (MSMQ) services.
- Messenger—This service is *not* MSN Messenger or Windows Messenger; it is a separate service used with the NET SEND command and can almost always be disabled.
- MS Software Shadow Copy Provider—Microsoft Backup tries to use this service; the service is not usually necessary if you aren't using Backup.
- Net Logon—This service is not usually required on a standalone system; it is required to log on to a domain controller.
- Network DDE—This service is not required by most systems.
- Network DDE DSDM—This service is not required by most systems.
- Network Location Awareness—This service is not required after Windows XP SP2 is installed.
- Network Provisioning Service—This service is used with domain controllers and XML configuration files; it is not required for standalone computers, but might be needed in a domain environment.
- Peer Name Resolution Protocol—This service is disabled (or removed) after Windows XP SP2 is installed; rarely needed and used primarily by IPv6.
- Peer Networking—This service is disabled (or removed) after Windows XP SP2 is installed; rarely needed and used primarily by IPv6.
- Peer Networking Group Authentication—This service is disabled (or removed) after Windows XP SP2 is installed; rarely needed and used primarily by IPv6.
- Peer Networking Identity Manager—This service is disabled (or removed) after Windows XP SP2 is installed; rarely needed and used primarily by IPv6.
- Performance Logs and Alerts—This service is rarely used on client computers and can be disabled; enable it if you specifically need to create performance logs and alerts.
- Portable Media Serial Number Service—This service is generally used only by Windows Media Player's Digital Rights Management and can often be disabled with no ill effects.

- Remote Desktop Help Session Manager—If you don’t use Windows XP’s Remote Assistance feature, this service can be disabled.
- Remote Registry Service—This service provides remote access to the registry; if you don’t need that (keeping in mind that Windows Management Instrumentation—WMI—provides an alternative method for remotely accessing the registry), disable this service.
- Routing and Remote Access—This service is usually disabled by default because client computers don’t typically accept incoming connections.
- Secondary Logon—If you don’t utilize the “Run As” command to run applications under alternate credentials, disable this service.
- Security Center—This service monitors Automatic Updates, the Windows Firewall, and other features; disabling this service simply removes the ability for Windows to alert you when, say, your virus definitions are out of date (something your antivirus software will likely do for you on its own anyway).
- Server—This service is used for file and print sharing; if your client computers don’t share files and printers, disable this service. Doing so doesn’t stop users from connecting to shared files or printers on servers.
- Simple Mail Transport Protocol (SMTP)—This service is part of IIS and should usually be removed if you’re not using the machine as a mail server.
- Simple TCP/IP Services—This service is a rarely used minor TCP/IP service; it can usually be disabled.
- Smart Card—Not using smart cards? Disable this service.
- SNMP Service—If you’re not using SNMP, disable this service.
- SNMP Trap Service—Disable this service if you’re not using SNMP.
- SSDP Discovery Service—This service is used as part of Universal Plug-n-Play and detects and configures UPnP devices on a home network; it is rarely used in a corporate environment. MSN Messenger does rely on this service on certain types of networks to get outside the firewall.
- TCP/IP NetBIOS Helper Service—If you’re not using WINS, you can disable this service.
- TCP/IP Printer Server—This service provides TCP/IP-based print sharing and can usually be disabled on client computers.

- Telnet—This service is usually not appropriate for client computers and can be disabled.
- Uninterruptible Power Supply—It's rare for a client computer to have a smart UPS—one that can shut down the computer if the UPS is on battery power and is running low; thus, this service can usually be disabled.
- Volume Shadow Copy—This service can generally be disabled on a client computer.
- WebClient—This service can be disabled and isn't currently used by anything that I'm aware of on client computers.
- World Wide Web Publishing—Again, part of IIS, this service is not generally appropriate for a client.

So how do you go about enforcing your disabled service decisions across your enterprise? Group Policy is a start. As Figure 2.4 shows, you can use a GPO to enforce the startup type for any of the built-in services.



Service Name	Startup	Permission
Alerter	Disabled	Not Defined
Application Layer Gateway ...	Disabled	Not Defined
Application Management	Not Defined	Not Defined
Automatic Updates	Not Defined	Not Defined
Background Intelligent Tran...	Not Defined	Not Defined
ClipBook	Not Defined	Not Defined
COM+ Event System	Not Defined	Not Defined
COM+ System Application	Not Defined	Not Defined
Computer Browser	Not Defined	Not Defined
Cryptographic Services	Not Defined	Not Defined
DHCP Client	Not Defined	Not Defined
Distributed File System	Not Defined	Not Defined
Distributed Link Tracking Client	Not Defined	Not Defined
Distributed Link Tracking Ser...	Not Defined	Not Defined
Distributed Transaction Coo...	Not Defined	Not Defined
DNS Client	Not Defined	Not Defined
DNS Server	Not Defined	Not Defined
Error Reporting Service	Not Defined	Not Defined
Event Log	Not Defined	Not Defined
File Replication Service	Not Defined	Not Defined
Help and Support	Not Defined	Not Defined
HTTP SSL	Not Defined	Not Defined
Human Interface Device Acc...	Not Defined	Not Defined
IMAPI CD-Burning COM Ser...	Not Defined	Not Defined
Indexing Service	Not Defined	Not Defined
Internet Connection Firewall...	Not Defined	Not Defined

Figure 2.4: Disabling services through Group Policy.

☞ Several services' names changed in Windows XP SP2; be sure you've got the proper GPO templates on your domain controllers so that the list shown will reflect the version of Windows XP you're using in your environment.

Service Logons and Passwords

Although Group Policy lets you decide which services will be allowed to run, it does nothing for helping you manage two important aspects of services:

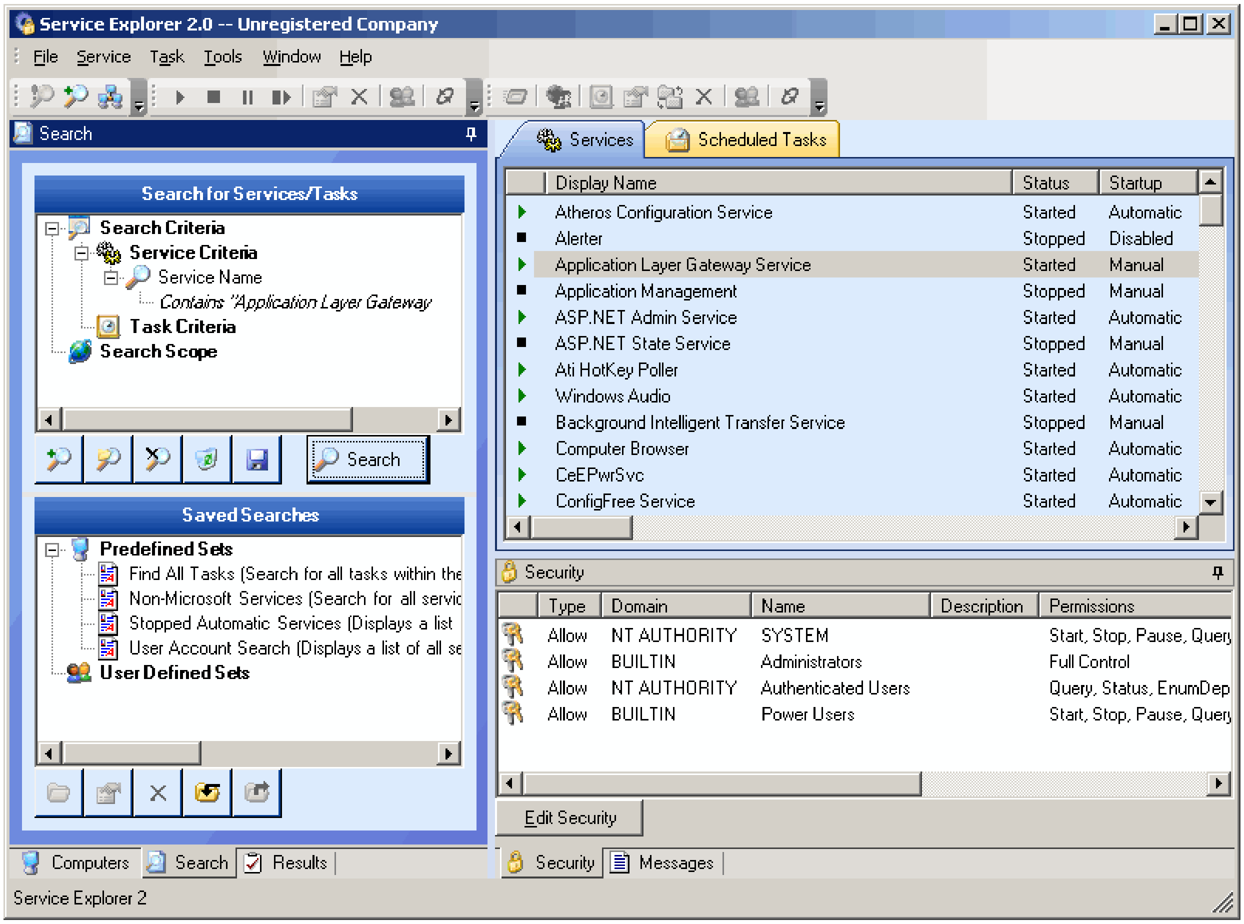
- The account they will run under
- The password for that account

Many services, for example, are configured to run under the all-powerful Local System account; such is especially true on server computers on which additional services for SQL Server, Exchange Server, and other add-on applications are running. Even on client computers, however, you might want to alter the account that a service is using to reduce its permissions to a more reasonable level. More importantly, any service *not* running as Local System will be logging on using a password, and that password will need to be changed on a regular and fairly frequent basis, just like any user password.

✎ If your company must remain compliant—for example, with the Sarbanes Oxley Act—and your company policy is to change user passwords every 45 days, you must include the often-neglected service accounts if you are to maintain regulatory compliance.

Changing a service's password involves two steps: Changing the password of the user account (which, if it's a local account, can be a time-consuming task without some kind of tool to help out), then telling the service itself to use the new password. That latter step can be exceedingly painful, especially if the service is installed on many computers.

Obviously, this area is where many administrators will write (or download) a script of some kind to do the job. Although this solution is okay, it typically assumes that you know which computers are running the service in question. To be on the safe side, you really need a tool that can first *find* all computers running the service, then reconfigure the service's password. ScriptLogic Service Explorer, which Figure 2.5 shows, has a search function that will search entire domains or workgroups for specified services, then allow you to configure those services en masse.


Service Explorer 2.0 -- Unregistered Company
File Service Task Tools Window Help
Search
Search for Services/Tasks
Search Criteria
Service Criteria
Service Name
Contains "Application Layer Gateway
Task Criteria
Search Scope
Search
Saved Searches
Predefined Sets
Find All Tasks (Search for all tasks within the
Non-Microsoft Services (Search for all servic
Stopped Automatic Services (Displays a list
User Account Search (Displays a list of all se
User Defined Sets
Computers
Search
Results
Services
Scheduled Tasks
Security
Edit Security
Security
Messages
Service Explorer 2

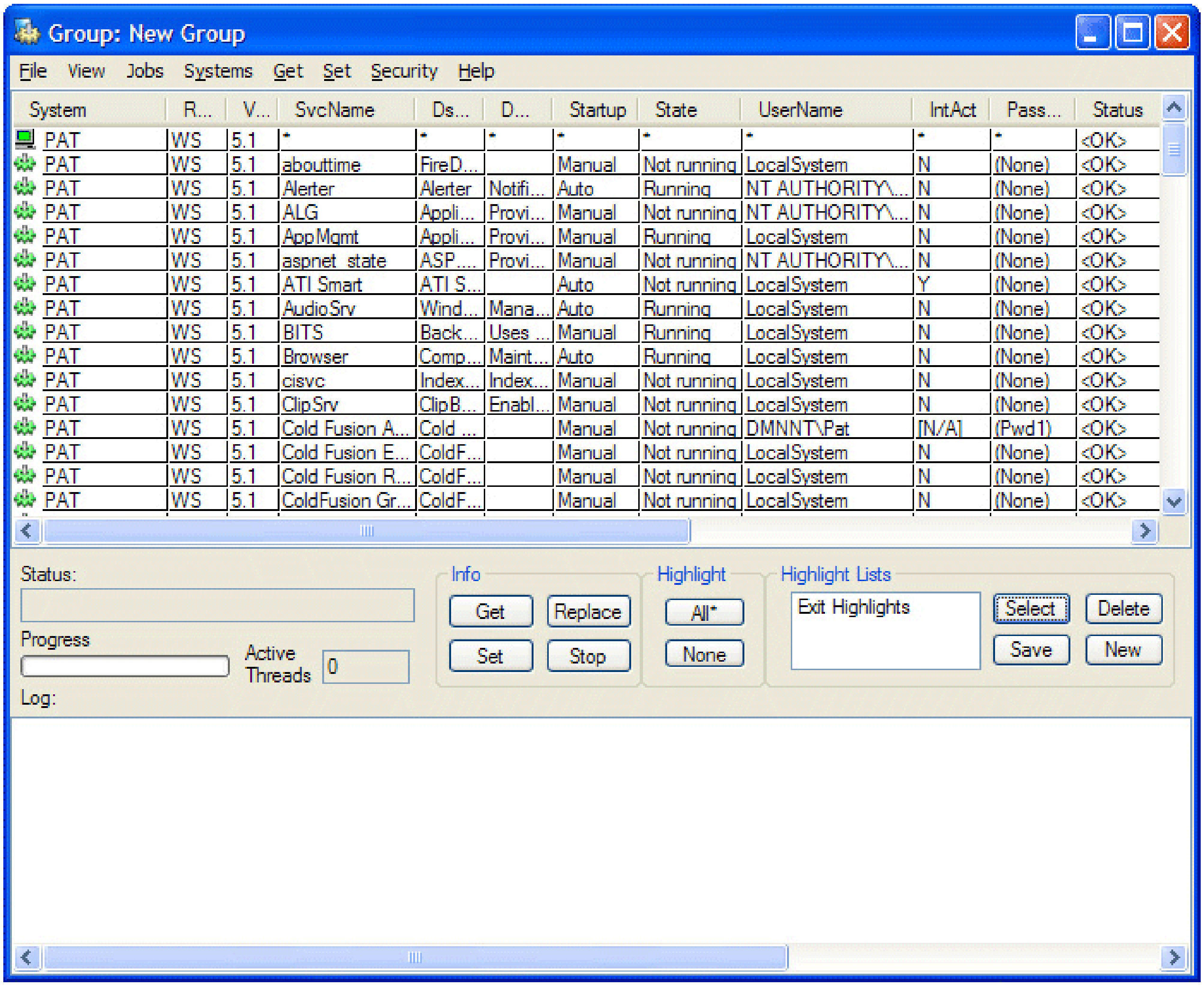
Display Name	Status	Startup
Atheros Configuration Service	Started	Automatic
Alerter	Stopped	Disabled
Application Layer Gateway Service	Started	Manual
Application Management	Stopped	Manual
ASP.NET Admin Service	Started	Automatic
ASP.NET State Service	Stopped	Manual
Ati HotKey Poller	Started	Automatic
Windows Audio	Started	Automatic
Background Intelligent Transfer Service	Stopped	Manual
Computer Browser	Started	Automatic
CeEPwrSvc	Started	Automatic
ConfigFree Service	Started	Automatic

Type	Domain	Name	Description	Permissions
Allow	NT AUTHORITY	SYSTEM		Start, Stop, Pause, Query
Allow	BUILTIN	Administrators		Full Control
Allow	NT AUTHORITY	Authenticated Users		Query, Status, EnumDep
Allow	BUILTIN	Power Users		Start, Stop, Pause, Query

Figure 2.5: Searching for the Application Layer Gateway Service.

Service Explorer has several helpful built-in searches, as well, such as one that looks for non-Microsoft services and another that displays all services that use a particular user account to log on. This type of search is useful when you're changing a password: Find every service actually using the account in question!

A similar tool, Lieberman Software's Service Account Manager, works similarly. As Figure 2.6 shows, Service Account Manager provides a single view of all services on a given machine. It can also locate machines running a particular service, and when updating a service's logon password, it can update the locally cached credentials for the service, allowing it to log on and continue running even if the computer temporarily loses connectivity with a domain controller (for services logging in under a domain account).



System	R...	V...	SvcName	Ds...	D...	Startup	State	UserName	IntAct	Pass...	Status
PAT	WS	5.1	*	*	*	*	*	*	*	*	<OK>
PAT	WS	5.1	abouttime	FireD...		Manual	Not running	LocalSystem	N	(None)	<OK>
PAT	WS	5.1	Alerter	Alerter	Notifi...	Auto	Running	NT AUTHORITY\...	N	(None)	<OK>
PAT	WS	5.1	ALG	Appli...	Provi...	Manual	Not running	NT AUTHORITY\...	N	(None)	<OK>
PAT	WS	5.1	AppMgmt	Appli...	Provi...	Manual	Running	LocalSystem	N	(None)	<OK>
PAT	WS	5.1	aspnet_state	ASP....	Provi...	Manual	Not running	NT AUTHORITY\...	N	(None)	<OK>
PAT	WS	5.1	ATI Smart	ATI S...		Auto	Not running	LocalSystem	Y	(None)	<OK>
PAT	WS	5.1	AudioSrv	Wind...	Mana...	Auto	Running	LocalSystem	N	(None)	<OK>
PAT	WS	5.1	BITS	Back...	Uses ...	Manual	Running	LocalSystem	N	(None)	<OK>
PAT	WS	5.1	Browser	Comp...	Maint...	Auto	Running	LocalSystem	N	(None)	<OK>
PAT	WS	5.1	cisvc	Index...	Index...	Manual	Not running	LocalSystem	N	(None)	<OK>
PAT	WS	5.1	ClipSrv	ClipB...	Enabl...	Manual	Not running	LocalSystem	N	(None)	<OK>
PAT	WS	5.1	Cold Fusion A...	Cold ...		Manual	Not running	DMNNT\Pat	[N/A]	(Pwd1)	<OK>
PAT	WS	5.1	Cold Fusion E...	ColdF...		Manual	Not running	LocalSystem	N	(None)	<OK>
PAT	WS	5.1	Cold Fusion R...	ColdF...		Manual	Not running	LocalSystem	N	(None)	<OK>
PAT	WS	5.1	ColdFusion Gr...	ColdF...		Manual	Not running	LocalSystem	N	(None)	<OK>

Active Threads: 0

Exit Highlights

Figure 2.6: Service Account Manager provides centralized service management.

The bottom line is that managing services is perhaps one of the most-overlooked client security problems, and there are tools that can help you solve the problem very, very easily. Getting your services locked down and your service logon passwords under control is a great step toward a more secure Windows enterprise.

Local Firewalls

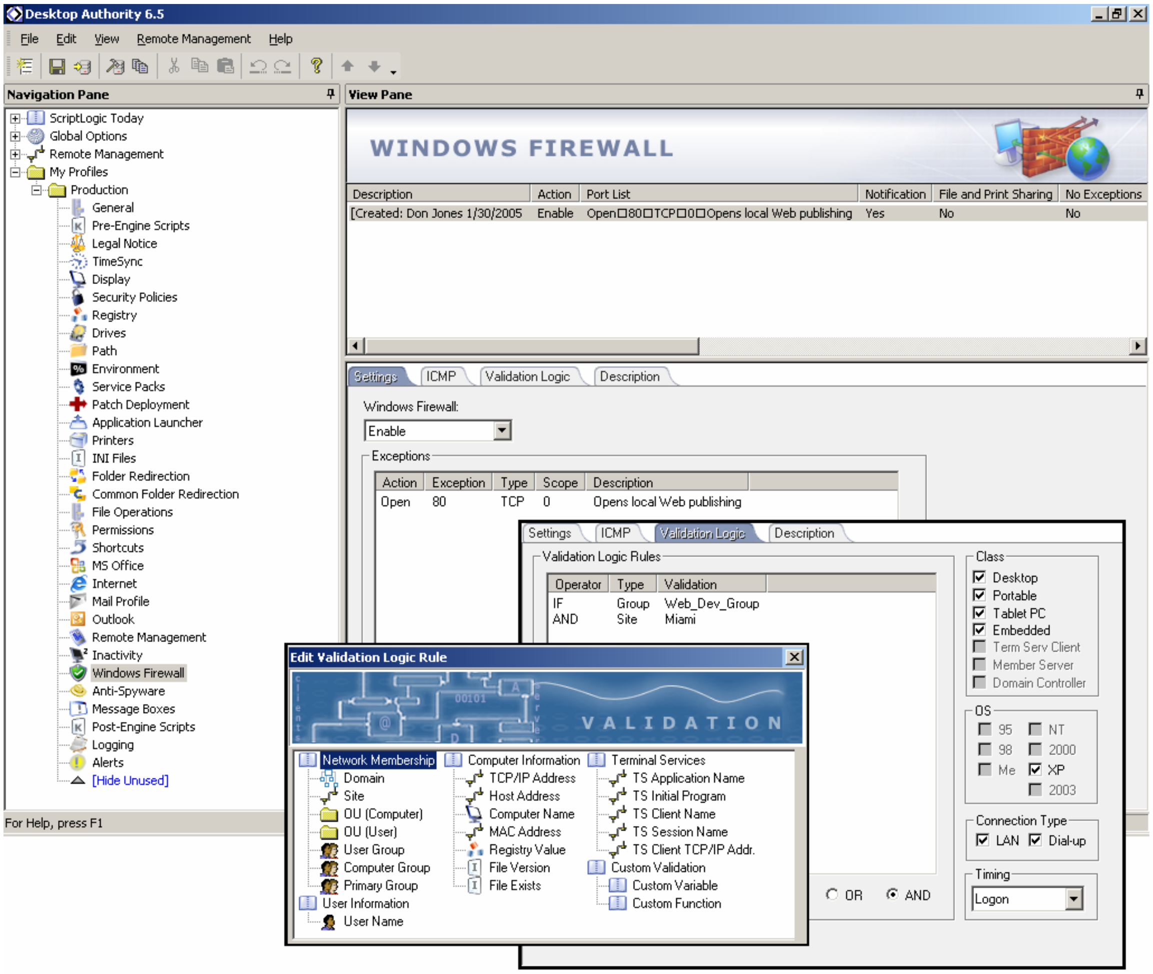
I'll risk starting a firestorm of debate with this statement: Every Windows client computer should have a local firewall. Now that I've said it, let me defend myself, because I know the topic of local firewalls is one that creates a lot of tension in the Windows administrative community.

Some administrators hate local firewalls, and for good reason. They definitely increase the administrative burden client computers represent. You'll need to be more concerned with what client computers are doing so that you can configure the firewall appropriately. I don't think that "additional administrative burden," however, is a good excuse for lax security. The fact is that most attacks target client computer vulnerabilities; because you can never tell what vulnerabilities might be lurking in Windows or your other corporate software, a firewall provides a good, solid line of defense. Keep in mind that most attacks come from *within* your network, so don't think that the corporate firewall is a perfect defense that obviates the need for a per-client defensive mechanism.

Microsoft's Windows Firewall, installed in Windows XP SP2, is a decent client-side firewall; other client-side firewalls are available from several companies. Windows Firewall has the benefit of being centrally configured through Group Policy: You can turn it on and off, configure port exceptions to allow incoming traffic, and so forth. Because most client computers don't need to accept incoming connections (excepting, of course, replies to network traffic that originated on the client; replies are allowed by default), you can often just configure the firewall to be on and leave it at that.

☞ If your domain controllers aren't showing the Windows Firewall Group Policy settings, you can add them by downloading the appropriate SP2 ADM files from http://www.microsoft.com/downloads/details.aspx?FamilyID=92759d4b-7112-4b6c-ad4a-bbf3802a5c9b&displaylang=en#filelist.

My complaint about Group Policy is that it is not quite granular enough in its application. GPOs can be linked to OUs, domains, or sites; the application of a particular GPO can be blocked at any of those levels, as well. With Windows XP and Windows Server 2003 (WS2K3) systems, application can be made a bit more granular through the use of WMI filters. However, you can't easily, for example, apply a GPO only to members of a certain group who have a particular software application running on their computer. ScriptLogic Desktop Authority, however, can apply Windows Firewall settings at that kind of granularity. For example, Figure 2.7 shows, I've created a Desktop Authority setting that enables the Windows Firewall and creates a port exception allowing incoming traffic on TCP port 80 (strictly as a demonstration; few client computers would actually need such an exception).



Description	Action	Port List	Notification	File and Print Sharing	No Exceptions
[Created: Don Jones 1/30/2005	Enable	Open□80□TCP□0□Opens local Web publishing	Yes	No	No

Windows Firewall: Enable

Exceptions

Action	Exception	Type	Scope	Description
Open	80	TCP	0	Opens local Web publishing

Validation Logic Rules

Operator	Type	Validation
IF	Group	Web_Dev_Group
AND	Site	Miami

○ OR ● AND

Class
☑ Desktop
☑ Portable
☑ Tablet PC
☑ Embedded
□ Term Serv Client
□ Member Server
□ Domain Controller

OS
□ 95 □ NT
□ 98 □ 2000
□ Me ☑ XP
□ 2003

Connection Type
☑ LAN ☑ Dial-up

Timing
Logon

Figure 2.7: Configuring a firewall setting in Desktop Authority.

I can restrict application of this setting to only those computers that are *not* members of the Administrator PCs group. In other words, administrators' PCs won't have this policy applied; a perfectly reasonable requirement in many environments in which administrators run software that ordinary users never will. A great many rules can be applied to the setting, such as the type of machine (desktop, laptop, tablet PC, and so forth), the OS, the type of connection, and so forth.

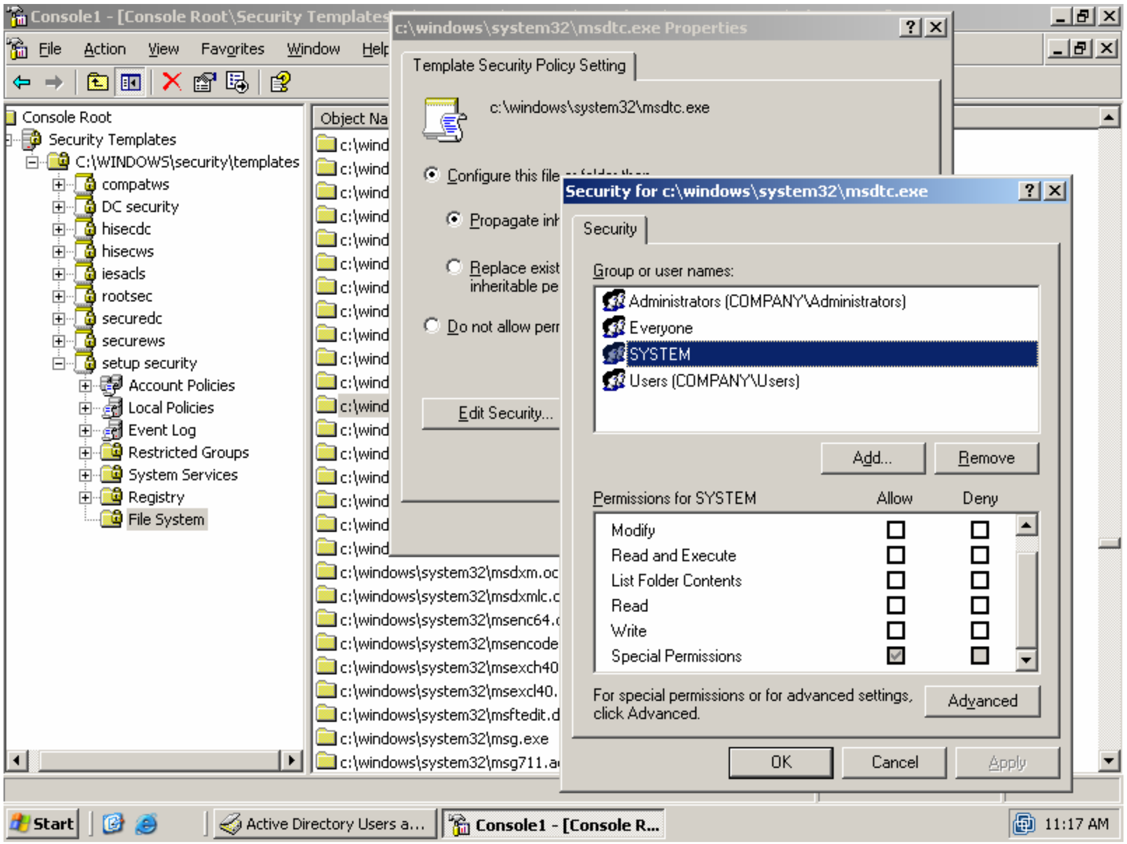
> Although Windows Firewall was first introduced in Windows XP SP2 and you will most commonly use it on client computers, WS2K3 SP1 also contains the Windows Firewall and makes it available on server computers.

NTFS Permissions

Consistent file permissions are crucial to enterprise security. As I've already mentioned, client computers often contain many confidential files, but client computers are often perceived as being less critical from a file permissions viewpoint. This position is dangerous: Imagine the damage that could be caused if someone swiped a company laptop in an airport waiting lounge, for example.

> Companies dealing with regulatory compliance issues—such as the Health Insurance Portability and Accountability Act (HIPAA), for example—should be very concerned about the security of files on client computers. Some organizations might want to keep files from being stored on client computers—a topic I'll address in the next few sections. However, sometimes allowing users to keep local copies of files—especially on laptops—is unavoidable. In those situations, having the correct file permissions in place is critical to maintaining your compliance.

Windows security templates can be used to create a consistent NTFS permissions structure. For example, the Setup Security.inf security template—shown opened in the Security Templates console in Figure 2.8—applies the starting security permissions for the entire OS.


Console1 - [Console Root\Security Templates
File
Action
View
Favorites
Window
Help
Console Root
Security Templates
C:\WINDOWS\security\templates
compatws
DC security
hisecdc
hisecws
iesacls
rootsec
securedc
securews
setup security
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Object Na
c:\wind
c:\windows\system32\msdxm.oc
c:\windows\system32\msdxmlc.c
c:\windows\system32\msenc64.c
c:\windows\system32\msencode
c:\windows\system32\msexch40
c:\windows\system32\msexcl40.
c:\windows\system32\msftedit.d
c:\windows\system32\msg.exe
c:\windows\system32\msg711.a
c:\windows\system32\msdtc.exe Properties
Template Security Policy Setting
Edit Security...
Security
Add...
Remove
Advanced
OK
Cancel
Apply
Start
Active Directory Users a...
Console1 - [Console R...
11:17 AM

c:\windows\system32\msdtc.exe

● Configure this file or folder then

● Propagate inh

○ Replace exist inheritable pe

○ Do not allow perr

Security for c:\windows\system32\msdtc.exe

Group or user names:

- Administrators (COMPANY\Administrators)
- Everyone
- SYSTEM
- Users (COMPANY\Users)

Permissions for SYSTEM	Allow	Deny
Modify	□	□
Read and Execute	□	□
List Folder Contents	□	□
Read	□	□
Write	□	□
Special Permissions	☑	□

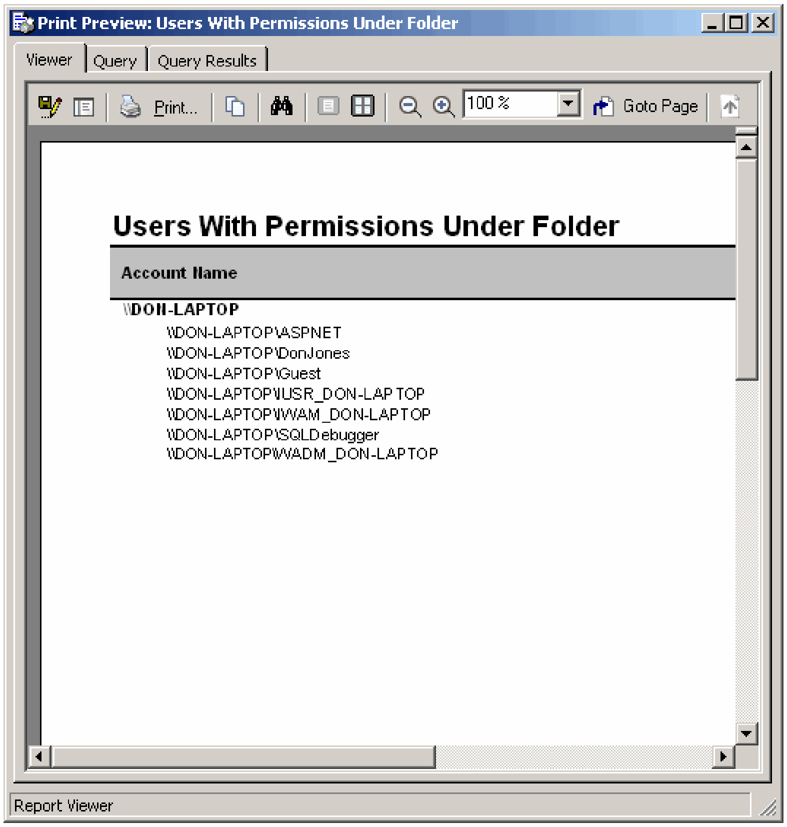
For special permissions or for advanced settings, click Advanced.

Figure 2.8: Using security templates to manage NTFS permissions.

You can create your own security templates, import them into a GPO, and apply them to a domain, site, or OU. Templates are a decent way to configure consistent NTFS permissions for a particular folder structure across a large number of computers. However, templates are far from a perfect solution. For example, they require all targeted computers to have an identical folder structure (at least within the folder structure you're defining in the template), which isn't always the case. Further, templates provide no reporting capability, which would allow you to easily verify the NTFS permissions applied to a given file or folder.

Third-party tools can, however, provide a robust level of reporting and help manage security more easily. BindView Corporation makes a suite of products designed to help organizations better meet regulatory and industry standards, including security permissions and auditing settings on files.

ScriptLogic Enterprise Security Reporter helps you effectively manage security and can also provide robust reports for client-level security. Although Enterprise Security Reporter is intended primarily for reporting on server-based security, many of its functions can be useful for client-based security as well. In a compliance environment, you might even be required to provide these types of reports for your client computers. The tool starts by loading security information from targeted computers into a SQL Server database, which allows you to then instantly obtain security reports, such as reports on which users have specific permissions under a given folder hierarchy. Figure 2.9 shows a sample report, listing the users that have permissions under a specified folder. This type of report is excellent for compliance management, because it lets you quickly verify that only the proper users have permissions on folders known to contain confidential information.



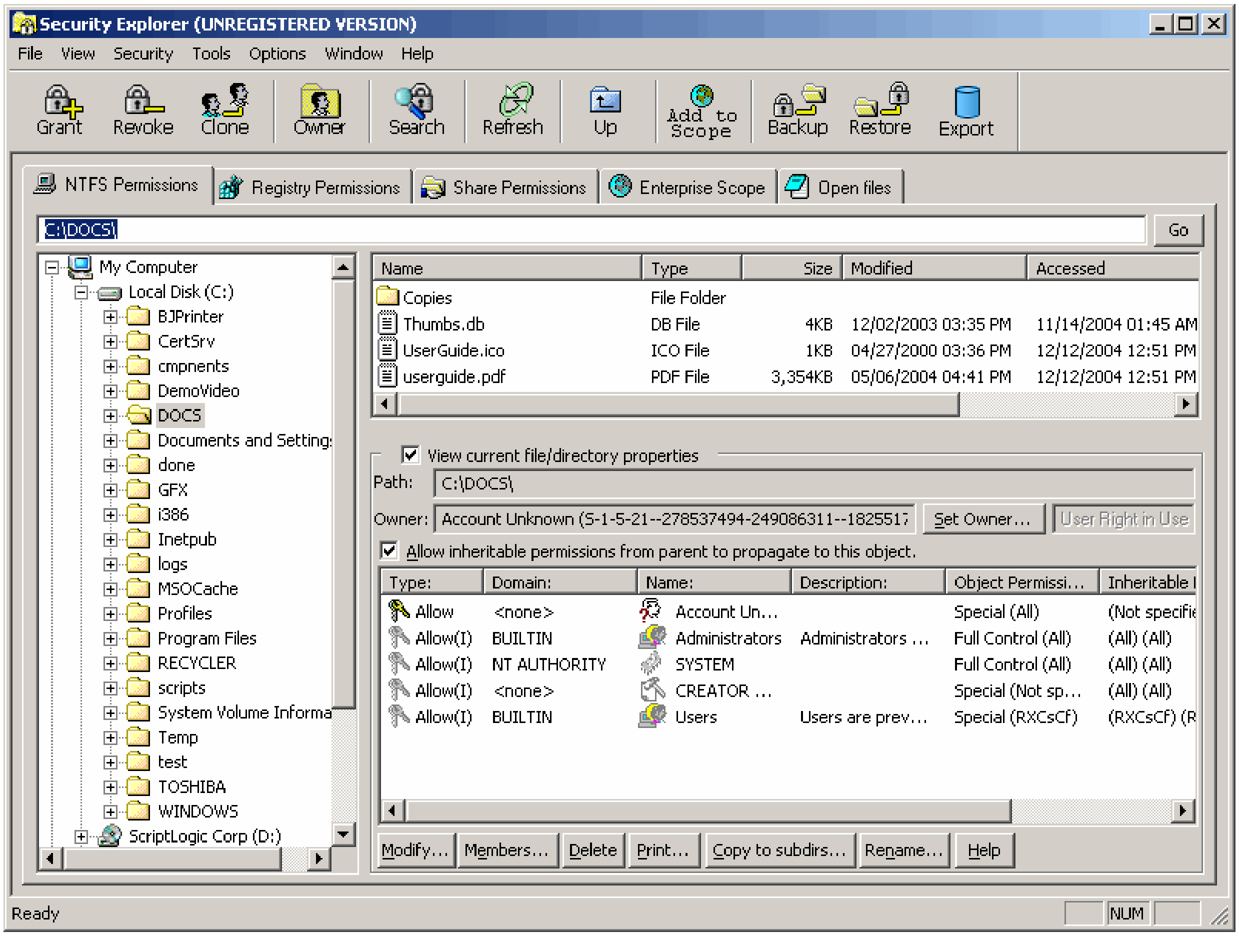
Users With Permissions Under Folder

Account Name

\\DON-LAPTOP
\\DON-LAPTOP\ASPNET
\\DON-LAPTOP\DonJones
\\DON-LAPTOP\Guest
\\DON-LAPTOP\IUSR_DON-LAPTOP
\\DON-LAPTOP\IWAM_DON-LAPTOP
\\DON-LAPTOP\SQLDebugger
\\DON-LAPTOP\WADM_DON-LAPTOP

Figure 2.9: Viewing permissions assigned to a specified folder.

For a more interactive security tool, ScriptLogic Security Explorer allows you to create *scopes*, which are collections of targeted security elements—including, for example, folders. Figure 2.10 shows Security Explorer examining the permissions on a folder that has been added to a scope; this folder might be an application data folder, for example.


Security Explorer (UNREGISTERED VERSION)
File View Security Tools Options Window Help
Grant Revoke Clone Owner Search Refresh Up Add to Scope Backup Restore Export
NTFS Permissions Registry Permissions Share Permissions Enterprise Scope Open files
Go
Modify… Members… Delete Print… Copy to subdirs… Rename… Help
Ready
NUM

C:\DOCS\

- My Computer
  - Local Disk (C:)
    - BJPrinter
    - CertSrv
    - cmpnents
    - DemoVideo
    - DOCS
    - Documents and Setting:
    - done
    - GFX
    - i386
    - Inetpub
    - logs
    - MSOCache
    - Profiles
    - Program Files
    - RECYCLER
    - scripts
    - System Volume Informa
    - Temp
    - test
    - TOSHIBA
    - WINDOWS
  - ScriptLogic Corp (D:)

Name	Type	Size	Modified	Accessed
Copies	File Folder			
Thumbs.db	DB File	4KB	12/02/2003 03:35 PM	11/14/2004 01:45 AM
UserGuide.ico	ICO File	1KB	04/27/2000 03:36 PM	12/12/2004 12:51 PM
userguide.pdf	PDF File	3,354KB	05/06/2004 04:41 PM	12/12/2004 12:51 PM

☑ View current file/directory properties

Path: C:\DOCS\

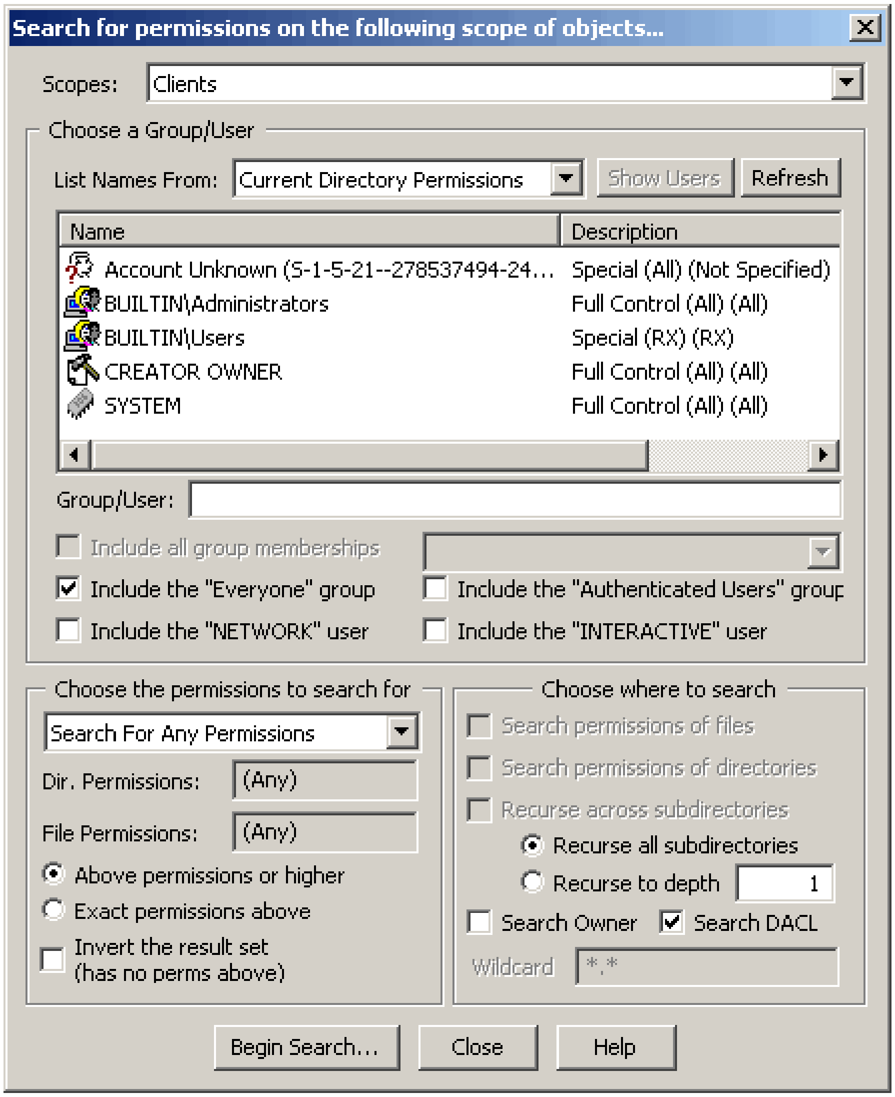
Owner: Account Unknown (S-1-5-21--278537494-249086311--1825517 Set Owner… User Right in Use

☑ Allow inheritable permissions from parent to propagate to this object.

Type:	Domain:	Name:	Description:	Object Permissi…	Inheritable I
Allow	<none>	Account Un…		Special (All)	(Not specifie
Allow(I)	BUILTIN	Administrators	Administrators …	Full Control (All)	(All) (All)
Allow(I)	NT AUTHORITY	SYSTEM		Full Control (All)	(All) (All)
Allow(I)	<none>	CREATOR …		Special (Not sp…	(All) (All)
Allow(I)	BUILTIN	Users	Users are prev…	Special (RXCsCf)	(RXCsCf) (R

Figure 2.10: Viewing security permissions through Security Explorer.

Once you have a scope established, you can conduct searches on it, modify its permissions, and so forth. For example, in Figure 2.11, I'm conducting a search on a scope named Clients. I might look for anything within the scope that assigns permissions to the Everyone group, or for permissions assigned to a particular user or group. I can search permissions on files, folders, and subfolders within the scope, and I can restrict the search to a particular set of permissions. By using this powerful search mechanism, I can quickly locate undesirable permissions, then use Security Explorer to remove or modify them.



Search for permissions on the following scope of objects...

Scopes: Clients

Choose a Group/User

List Names From: Current Directory Permissions

Name	Description
Account Unknown (S-1-5-21--278537494-24...	Special (All) (Not Specified)
BUILTIN\Administrators	Full Control (All) (All)
BUILTIN\Users	Special (RX) (RX)
CREATOR OWNER	Full Control (All) (All)
SYSTEM	Full Control (All) (All)

Group/User:

□ Include all group memberships
☑ Include the "Everyone" group
□ Include the "Authenticated Users" group
□ Include the "NETWORK" user
□ Include the "INTERACTIVE" user

Choose the permissions to search for

Search For Any Permissions

Dir. Permissions: (Any)

File Permissions: (Any)

● Above permissions or higher
○ Exact permissions above
□ Invert the result set (has no perms above)

Choose where to search

□ Search permissions of files
□ Search permissions of directories
□ Recurse across subdirectories
● Recurse all subdirectories
○ Recurse to depth 1
□ Search Owner
☑ Search DACL

Wildcard *.*

Figure 2.11: Searching a scope in Security Explorer.

These tools can all help you maintain more consistent permissions. Of course, don't forget about freely available tools for managing permissions, such as Windows' built-in Cacls.exe command-line tool and the more flexible Windows resource kit tool, XCacls.exe. Although less suitable for administration of multiple computers, these tools can allow you to quickly reconfigure security permissions in a folder hierarchy on a single machine, and they can be used in a batch file to make it easier to make changes across multiple machines at once.

However, bear in mind that maintaining consistent permissions across multiple client computers will *always* be difficult. A better idea, if possible, is to simply get the files *off* of the client computers entirely.

Folder Redirection

The idea behind folder redirection is simple, and is illustrated in Figure 2.12. Users access what appears to be a local folder, but that access is *redirected* to a server-based folder. Users typically never realize that the files are located on a server rather than their local computers. The benefit is that files can be centrally secured and audited on the server, eliminating the need to worry about consistent security on the client. The client doesn't actually contain the files, and therefore doesn't need special security considerations. Files can also be more easily backed up and restored on the server than on a client.

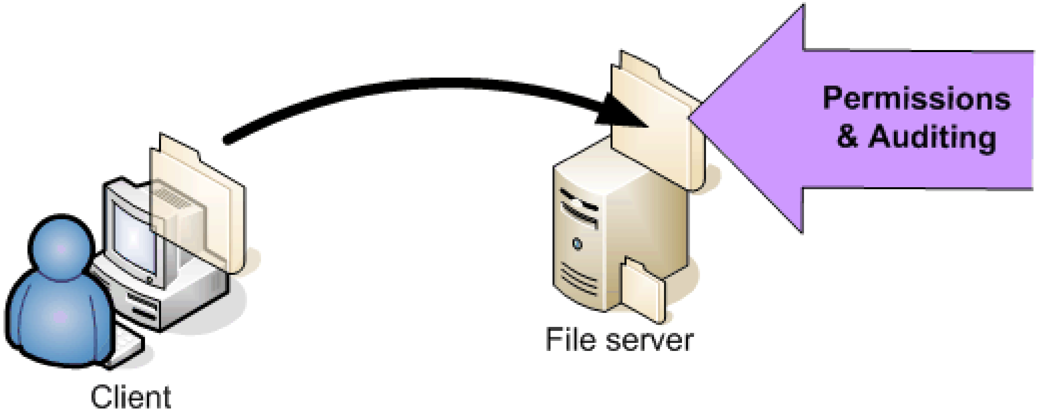


Figure 2.12: Folder redirection keeps folders and files centrally located.

✎ There is a downside to folder redirection for portable computers because users think they have all the files locally and don't realize folder redirection is in effect. When they disconnect from the network, their files "vanish." Using Windows' Offline Files feature can help mitigate this problem.

Folder redirection for certain special folders—most commonly, users' profile folder, which contains the My Documents folder—can be accomplished through Group Policy. Larger organizations often need to redirect folders based on the user so that different users' redirected folders can be housed on various file servers, providing sufficient storage for everyone. Group Policy accomplishes this task most easily if you can have file servers that correspond with AD OUs. In this case, you create a unique GPO for each OU and redirect that OU's users (or rather, those users' folders) to a particular server. Otherwise, you might need to use a technology such as Windows Distributed File System (DFS), which can provide a non-server-centric view of the network, allowing users' folders to be redirected to an arbitrary server, as Figure 2.13 illustrates.

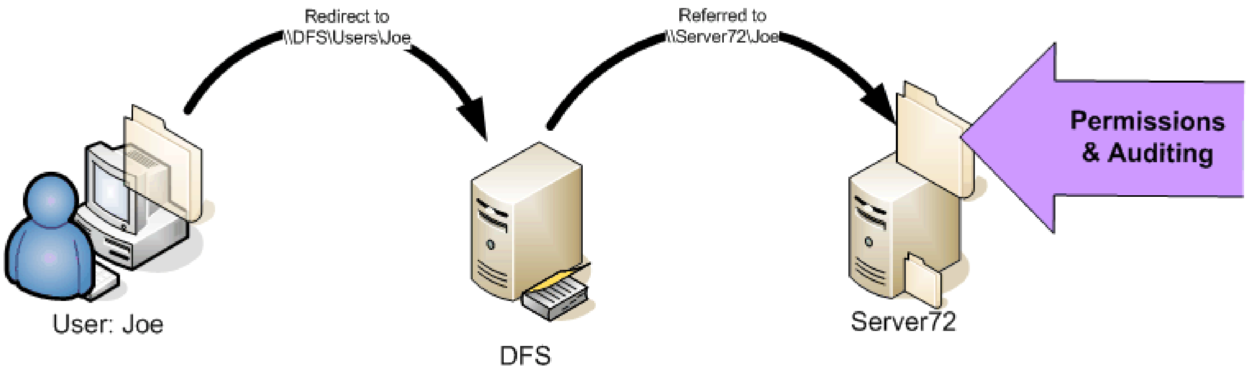
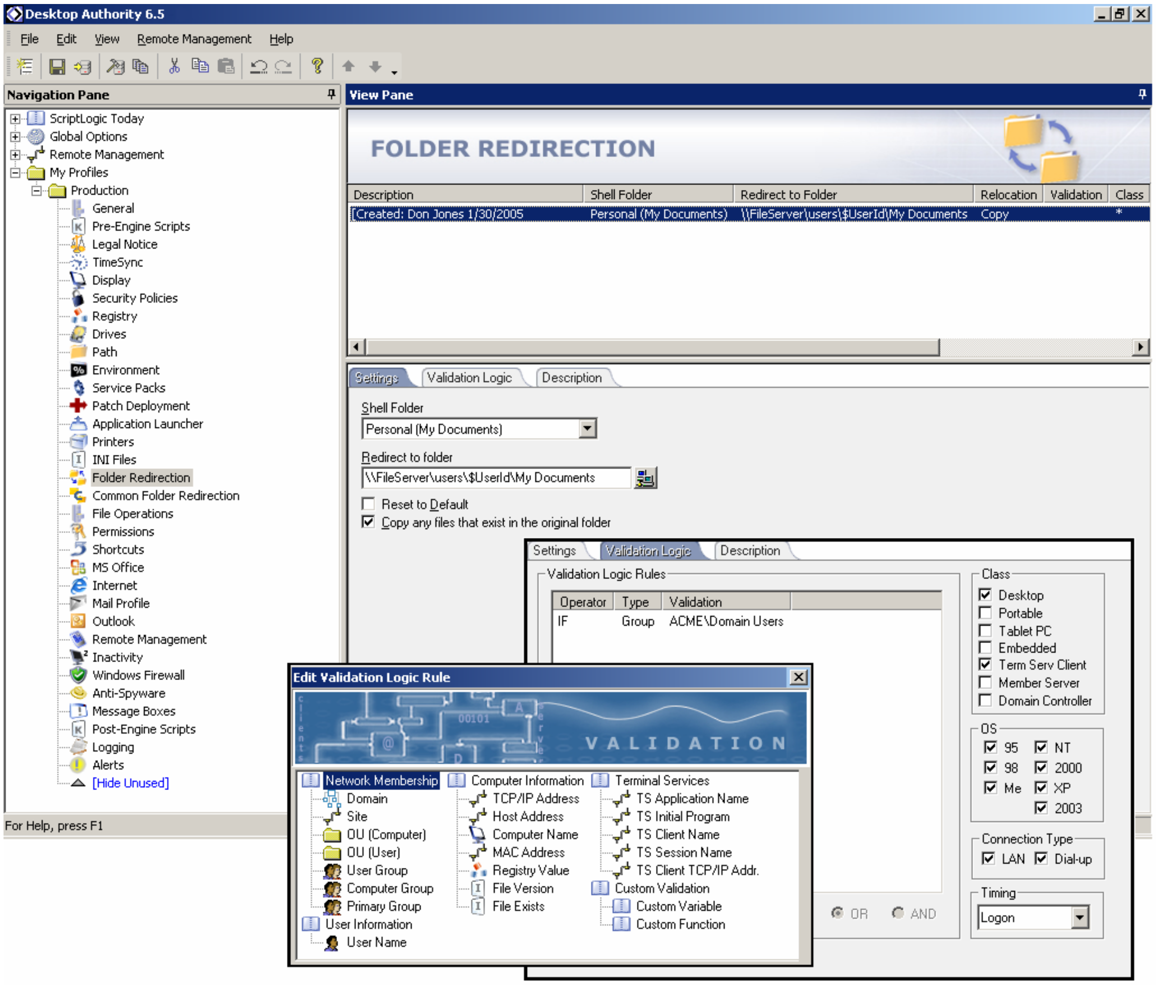


Figure 2.13: Using DFS along with folder redirection.

Another technique is to use a desktop configuration tool such as ScriptLogic Desktop Authority. As Figure 2.14 shows, this tool can redirect many different shell folders to an arbitrary location. It can also copy any files that already exist locally in the to-be-redirected-folder to the new location, ensuring a transparent cutover to the redirection scheme. Desktop Authority 6.05 can redirect the following folders:

- Start menu folder
- Programs folder
- Startup folder
- Desktop folder
- Favorites (Internet Explorer bookmarks) folder
- Personal (My Documents) folder
- My Pictures folder
- Cookies folder
- History folder
- Recent golder
- Send To folder
- Temporary Internet Files folder



Description	Shell Folder	Redirect to Folder	Relocation	Validation	Class
[Created: Don Jones 1/30/2005	Personal (My Documents)	\\FileServer\users\$UserId\My Documents	Copy		*

Shell Folder: Personal (My Documents)

Redirect to folder: \\FileServer\users\$UserId\My Documents

☐ Reset to Default

☑ Copy any files that exist in the original folder

Validation Logic Rules

Operator	Type	Validation
IF	Group	ACME\Domain Users

○ OR ○ AND

Class: ☑ Desktop ☐ Portable ☐ Tablet PC ☐ Embedded ☑ Term Serv Client ☐ Member Server ☐ Domain Controller

OS: ☑ 95 ☑ NT ☑ 98 ☑ 2000 ☑ Me ☑ XP ☑ 2003

Connection Type: ☑ LAN ☑ Dial-up

Timing: Logon

Figure 2.14: Redirecting the My Documents folder.

Desktop Authority also provides for more granular application of settings than Group Policy offers. For example, this setting might be applied to all desktop computers, but not to portable computers (for whom redirection can be problematic because the computer isn't always on the network).

☞ A single Desktop Authority profile—roughly analogous to a GPO—can contain multiple *elements;* each element can, for example, redirect a single shell folder. Desktop Authority can also redirect the so-called *common* folders—including common Application Data—that are shared by all users of a computer.

Folder redirection is a crucial security tactic, allowing you to maintain ease-of-use for your users while consolidating files onto more easily secured and easily audited file servers. Folder redirection can also help enforce system configurations. For example, if all users' desktop folders are redirected to a single shared location, and users are not given write permissions to that location, then all users will have a consistent, locked desktop configuration. Such a configuration can make it more difficult for users to introduce external software—such as viruses—by locking down some portion of the file system where Web browsers and other applications try to save files.

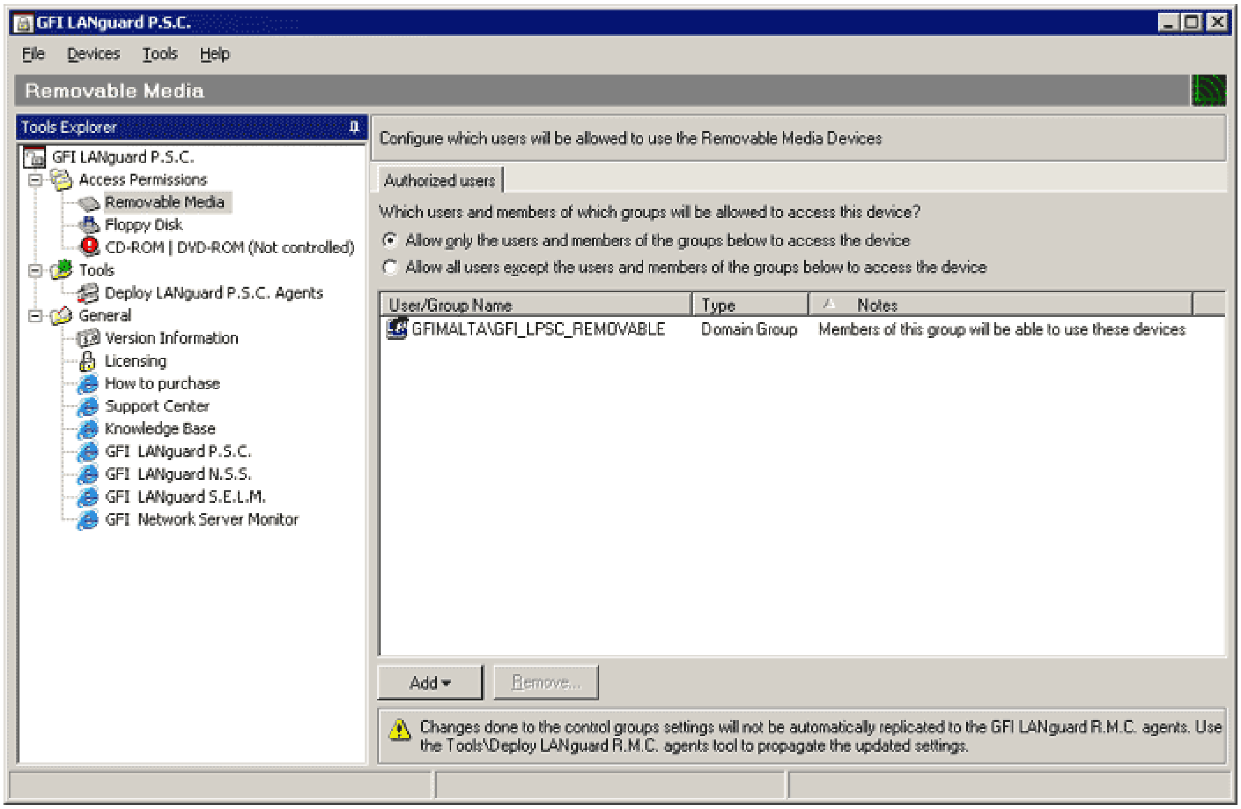
Removable Storage

Organizations have long sought to lock down removable media, a key means of introducing unwanted software into the environment and for removing confidential information from the environment. In the past, organizations might order computers without floppy drives or might restrict the use of optical media burners. However, removable media today is ubiquitous, with FireWire/IEEE1394 and USB devices making it easier for users to take data in and out of the environment without notice. Third-party tools currently provide the only reliable means of locking down these external, removable storage options.

> ✎ Why bother locking down USB flash drives, for example? Because most removable media support only the FAT, FAT32, or CDFS file systems, none of which support security permissions. Thus, removable media not only represents an opportunity to introduce unwanted software and to remove confidential data but also ensures that any data removed from the environment will be completely unsecured. Although some removable media offers security options such as encryption, there is no centralized means of enforcing the use of such features, making it less likely that users will do so.

SecureWave Sanctuary is designed for device access control. Devices are categorized—digital cameras (which have onboard storage), optical burners, smart card readers, flash drives, and so forth—and, by default, disabled. You can “white list” allowed devices, such as scanners or modems, and leave all other devices disabled. Users are unable to install the devices under Windows, meaning they are unable to use disallowed devices to bring data in or out of the environment. Device access can be granted on a temporary, per-user basis if necessary. You can even allow optical drives to function, but provide a list of allowable media, ensuring that users can run authorized software but not introduce new software into the environment.

Another similar package is GFiLANguard Portable Storage Control (PSC), which focuses exclusively on portable storage such as USB flash drives. It addresses almost all forms of portable storage, including flash drives, MP3 players and smartphones, digital cameras, CDs, floppies, and so forth. As Figure 2.15 shows, device permissions can be mapped to AD groups, helping to minimize security management overhead. For example, you might create groups that represent allowed devices, then simply add users to the groups on an as-needed basis.



Configure which users will be allowed to use the Removable Media Devices

Which users and members of which groups will be allowed to access this device?

● Allow only the users and members of the groups below to access the device

○ Allow all users except the users and members of the groups below to access the device

User/Group Name	Type	Notes
GFIMALTA\GFI_LPSC_REMOVABLE	Domain Group	Members of this group will be able to use these devices

⚠ Changes done to the control groups settings will not be automatically replicated to the GFI LANguard R.M.C. agents. Use the Tools\Deploy LANguard R.M.C. agents tool to propagate the updated settings.

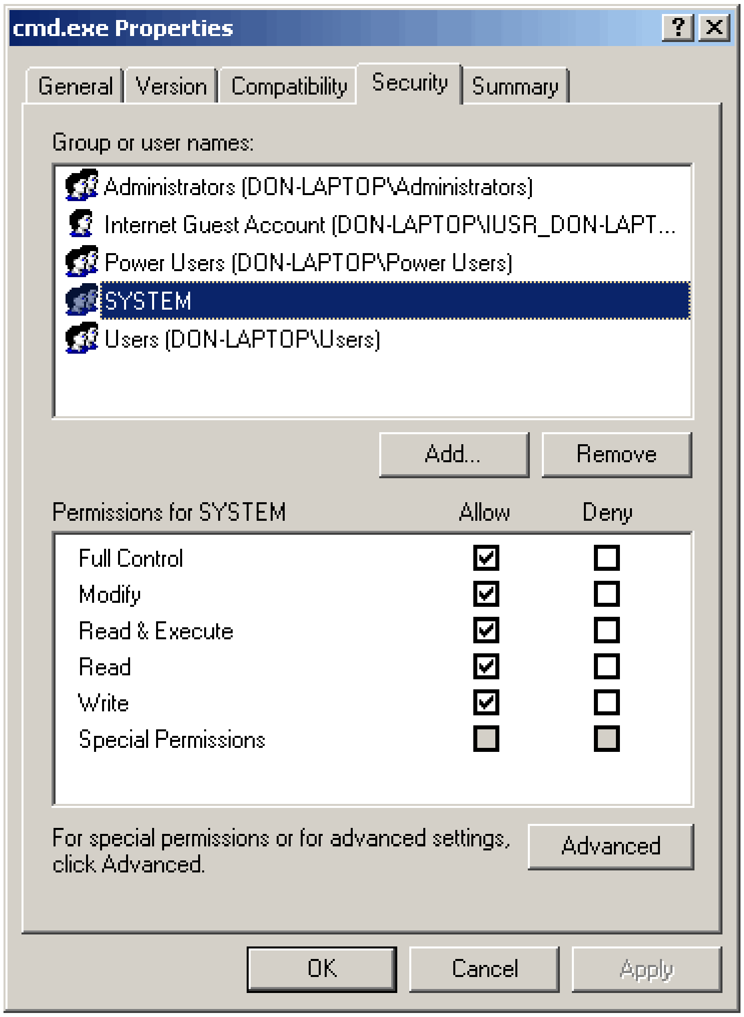
Figure 2.15: Restricting access to devices.

☞ Don’t forget all the ways in which data can leave a computer or enter it. Your network is one obvious way, but that’s something you can control. Any portable device with memory—such as a digital camera—is a possibility. Also keep in mind Bluetooth- and infrared-accessible devices, such as PDAs and smart phones, and be sure to control them appropriately.

Controlling access to removable storage will help make your environment more secure by reducing the ways in which information can leave your network and reducing the ways in which unwanted software can enter your network.

Local System Permissions

Local system permissions are the final area covered in this chapter. Consider Cmd.exe, a file that is usually located in C:\Windows\System32. Figure 2.16 shows the file permissions on Cmd.exe on a Windows XP Professional computer that has been upgraded to SP2.



Group or user names:

- Administrators (DON-LAPTOP\Administrators)
- Internet Guest Account (DON-LAPTOP\IUSR_DON-LAPT...
- Power Users (DON-LAPTOP\Power Users)
- SYSTEM
- Users (DON-LAPTOP\Users)

Permissions for SYSTEM	Allow	Deny
Full Control	☑	□
Modify	☑	□
Read & Execute	☑	□
Read	☑	□
Write	☑	□
Special Permissions	□	□

For special permissions or for advanced settings, click Advanced.

Figure 2.16: Default permissions on Cmd.exe.

Notice that the SYSTEM account has Full Control. Why would the system itself need to open a new command-line window? I typically remove the SYSTEM account from this and many other files in the file system.

Also notice that the Internet Guest Account has permissions to run Cmd.exe. Anonymous users have the ability to open a command-line window and execute commands. Spend some time investigating the default permissions on the many files and folders lurking around in Windows and to apply more sensible defaults. Some other files you might want to investigate include:

- Command.com
- Ftp.exe
- Tftp.exe
- Telnet.exe
- WScript.exe
- CScript.exe
- Net.exe

> ✎ Don't try to *delete* these files; most are under Windows File Protection and will be replaced eventually (by a service pack, if nothing else). Instead, modify the permissions on these files so that only appropriate users—real users, not SYSTEM—can execute them.

The idea is that these types of all-powerful utilities can create significant havoc if an attacker gains access to them. Reduce the likelihood of that happening by removing access from any account that doesn't absolutely need to have it.

Summary

Client computers represent a significant security risk in many organizations simply because they're rarely as controlled or as well-configured as servers. This chapter has introduced you to some of the major client vulnerabilities and given you some tips on how to lock them down appropriately. One way to get a better handle on client security is to think about the entire life cycle data takes in your organization—from the server, across the network, to the client, to portable devices, and so forth. Thinking about that life cycle will help you better implement appropriate levels of security at each point in the cycle.

The next chapter will focus on a topic that affects both clients and servers—the software built-in to Windows that presents major vulnerabilities. Often called "middleware," applications such as Internet Explorer (IE), Windows Media Player, and other applications have a reputation for security problems. I'll show you some ways in which those problems can be addressed and mitigated.

Content Central

Content Central is your complete source for IT learning. Whether you need the most current information for managing your Windows enterprise, implementing security measures on your network, or deploying new enterprise software solutions, Content Central offers the latest instruction on the topics that are most important to the IT professional. Browse our extensive collection of eBooks and video guides and start building your own personal IT library today!

Download Additional eBook Chapters!

If you found this eBook chapter to be informative, please visit Content Central and download other eBook chapters from this publication. If you are not already a registered user of Content Central, please take a moment to register in order to gain free access to this and many other great IT eBooks and video guides. Please visit: http://www.realtimepublishers.com/contentcentral/.