Department of Energy

CIAC

Computer Incident Advisory Capability

UCRL-ID-147617

Connecting to the Internet Securely; Windows 2000

CIAC-2321

William J. Orvis

Kathryn Call

John Dias

March 2002

Lawrence Livermore National Laboratory

DISCLAIMER

The information within this paper may change without notice. Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties with regard to this information. In no event shall the author be liable for any damages whatsoever arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.

This work was performed under the auspices of the U.S. Department of Energy by University of California Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48 between the U.S. Department of Energy (DOE) and The Regents of the University of California (University) for the operation of UC LLNL. The rights of the Federal Government are reserved under Contract 48 subject to the restrictions agreed upon by the DOE and University as allowed under DOE Acquisition Letter 97-1.

TABLE OF CONTENTS

1 OVERVIEW

As the threat to computer systems increases with the increasing use of computers as a tool in daily business activities, the need to securely configure those systems becomes more important. There are far too many intruders with access to the Internet and the skills and time to spend compromising systems to not spend the time necessary to securely configure a system. Hand-in-hand with the increased need for security are an increased number of items that need to be securely configured. Windows 2000 has about seven hundred security related policy settings, up from seventy two in Windows NT.

While Windows 2000 systems are an extension of the Windows NT 4 architecture, there are considerable differences between these two systems, especially in terms of system and security administration.

Operational policy, system security, and file security are other areas where Windows 2000 has expanded considerably beyond the domain model of Windows NT 4. The Windows NT 4 Domain model consists of domains of workstations that, with a single login, share resources and are administered together. The database of user settings and credentials resides in the domain server. Domains can trust other domains to expand the sharing of resources between users of multiple domains. On Windows 2000, the domains still exist but multiple domains that share trust are combined into Domain Trees and Domain Forests depending on how the logical namespace is divided. These trees and forests are combined under a new object called Active Directory. Domains themselves are broken down into Organizational Units. As such, there are more levels at which security policies can be set and for which information sharing can be controlled.

Keep in mind that Active Directory, while it is in a superior position in a domain hierarchy, is not a super domain. It is a very different thing. Active Directory is essentially just a database for company wide information. It is a place where you go to get information rather than having that information pushed to you. That database can include user authentication information and any users authenticated at the Active Directory level have access to all the domains below them. And while security policy information can be set at the Active Directory level, it cannot be pushed onto user workstations from there. Pushing of settings and software can only be done from the Domain and OU levels.

The design of an Active Directory is not a trivial operation and should not be done without careful consideration and planning. The biggest problem with an active directory is that it must be designed and implemented from the top down. After a root Active Directory Domain is created, it is not possible to rename it or graft it onto a higher level Domain. The only way to do that is to define a new Root Domain with new subdomains below it and then to migrate all the workstations from the old Domains to the new ones. Information for designing an Active Directory Domain is not in this document.

Each domain under Active Directory must share a single namespace. That is, the name of every machine in a domain must share the same right hand side of the domain name. For

example, a1.physics.llnl.gov and b2.physics.llnl.gov can both reside in the physics.llnl.gov domain.

Root domains and their logical subdomains form a Domain Tree. Each Domain Tree shares a contiguous namespace. For example, if the root domain is llnl.gov, subdomains could be engineering.llnl.gov, physics.lnl.gov, and chemistry.lnl.gov. However comp.argonne.gov could not be a subdomain. Engineering could be further subdivided into the subdomains mechanical.engineering.llnl.gov, electrical.engineering.llnl.gov, and computer.engineering.llnl.gov.

Alternately, mechanical, electrical, and computer could be Organizational Units (OU) within the engineering domain. An Organizational Unit is a container in a domain for user and machine accounts, and services. Computers within the mechanical engineering OU share the engineering.llnl.gov namespace, not the mechanical.engineering.llnl.gov namespace as they would in a subdomain. The same is true for the other engineering OUs. Administration of an Organizational Unit is much like administration of a domain without having to create a separate domain. Administration of Organizational Units can be delegated to other administrators to spread the administration job without giving these administrators access to the entire domain.

This hierarchy of domains/subdomains/organizational units forms an equivalent hierarchy of security domains or containers where security settings on a container (stored in the container's database) are applied to all objects within a container. Security settings at outer domains filter down to the interior subdomains, organizational units, and eventually to the individual workstations.

Operational policies and security settings are placed on domains, subdomains, or organizational units using Group Policy. Local Security Policy is used to make settings that are unique to an individual system. When you attempt to get access to something on a system, Group Policy is applied first and then Local Group Policy. Thus, Local Group Policy can increase the security on an object but not decrease it.

With the increased granularity in security settings comes a lot more things to set. Combine this with the hierarchy of security domains and an administrator has a huge number of items to analyze and set. Luckily, with this increase in settings comes a group of editors for setting these values, including templates of settings that can be applied with a single command. All of these settings are accomplished with plug-ins to the Microsoft Management Console.

The Microsoft Management Console (MMC) was introduced in Windows NT 4 as the manager of the Internet Information Server and as the console of the Security Configuration and Analysis manager. The MMC is simply a program that supplies the visual interface for various snap-ins that are used to manage a system. For example, Group Policy is an MMC snap-in console for managing Group Policy. Some snap-ins can only show settings while others can change settings on a system. The snap-ins that you will use to configure a Windows 2000 system are:

- Security Configuration and Analysis

- Group Policy
- Local Security Policy

Other tools for configuring a system are:

- reg.exe – A command line tool which can be used to set policy from within a script.
- hfnetchk.exe – A tool to detect and list the state of patches on a system.
- secedit.exe – A command line tool for applying security templates from a script.
- regedit32.exe – A general purpose tool for editing the registry.
- Critical Update Notification – A service that automatically checks for the existence new security patches.
- Windows Update – A web based service for installing security patches.

2 REMOTE MANAGEMENT CONSIDERATIONS IN WINDOWS 2000

Windows 2000 has several new remote management capabilities that security managers need to be aware of. These include Domain level security policies set with Group Policy, Automatic system installation and upgrades, and automatic software installation and upgrades. From a management point of view, these capabilities considerably reduce the amount of time necessary to setup and maintain a large number of systems. From a security point of view, these capabilities create single points of failure that can be used to compromise or take down the whole network.

For example, if a virus infected application is placed on the domain server as an application to be installed on all systems, the update manager will dutifully infect every computer in the network. If a backdoor program were added to the system installer, every new system would be installed with the backdoor in place. If a mistake is made in a group policy, that same mistake now exists on every machine in the domain.

The result is, keep the domain server and management station extremely secure and be very careful with applications to be pushed to every system. Security policy settings at the higher levels should be more global in nature, and should be very straight forward so that the implications are well understood. More restrictive and complicated policies should be done at a lower level, such as at the OU, where the implications are better understood because the administrators better understand the machines they are directly maintaining.

2.1 DOMAIN SECURITY SETTINGS WITH GROUP POLICY

Using the Group Policy Editor snap-in of the MMC, security policies can be set that apply to the whole domain. Be careful which policies you set at this level as they must be of the one-size-fits-all type. Any policies that are different for different Organizational Units should not be set at the domain level.

Some examples of policies that are reasonable to be set at the domain level are,

- Minimum password length
- Password complexity

- Login banner

Some examples of policies that probably should not be set at the domain level are,

- Login script
- Machines login is allowed from
- User rights

Different organizational units likely have different requirements for the login script. Setting it at the domain level requires that the single domain level script do everything that every Organizational Unit wants. User rights determine what the different types of users can do. Users in a development group need significantly different user rights than a customer service group.

2.2 AUTOMATIC SYSTEM INSTALLATION

Using a service called Remote Installation Services (RIS), you can install, over the network, Windows 2000 and any preconfigured applications on a computer with a newly formatted hard drive. To make this work, you must have preconfigured the windows installation and added any installable applications. The easiest way to do this is to configure a standard system the way you want it, with all applications in place, and then use the sysprep utility to create an installable image of that system.

The installable image is placed on the RIS server. A remote computer with a newly formatted hard drive is booted with the RIS client floppy which installs the Client Installation Wizard. The Wizard then connects to the server and controls the installation of the system image.

Great care must be taken here to insure that the system image you create and install on every new computer is secure. Unless you run to the system and pull its network connection, it will be on the network as soon as the system installation is done. If the installed system is not secure and there are no other protections (firewall, etc.) there is a risk that the system will be attacked in its insecure state. We (CIAC) have seen new systems attacked and compromised within minutes of their being placed on the network, as if the intruders were just waiting for a new system to appear.

2.3 DESKTOP MIRRORING AND SOFTWARE INSTALLINATION

The IntelliMirror service is used to install applications on a user's system. In addition, it can also be used to setup a network where a user's software, data, and desktop settings follow him around the network and are available on whatever computer he logs into.

2.3.1 Automatic Software Installation

Automatic software installation part of IntelliMirror comes in two flavors: assigned or published. With *assigned* software, registry changes are made on a user's system to make the software appear to be on the system. The software name appears in the start menu and the association between document file extensions and the application exists. The application is not actually installed on the computer until the first time it is used. The first

time the application is used, either by clicking it in the Start menu or double clicking an associated document file, the application is downloaded from the server and installed. Thereafter, the application runs directly from the user's system. If the user deletes or uninstalls the application, it is reinstalled the next time he tries to use it.

Published applications are not automatically installed, but are available for the user to install using the Add/Remove Programs control panel. When a user chooses to add an application, it is downloaded over the network and installed.

2.3.2 Automatic Patching and Upgrades

Automatic upgrades are handled in much the same way as automatic software installation. That is, the upgrade file is assigned to each computer and installed the first time the upgraded application is used. If the upgrade is on the system, it is installed the next time the system is started.

While not as risky as full system installations. Automatic system patching and upgrades could also be used to make a system unsecure or unstable. Keep in mind that when doing automatic system upgrades, you are installing the upgrade or patch on all the systems in a domain or OU. Be careful that the patch you are installing is appropriate for all the systems it is being installed on and that it does not open up other vulnerabilities.

2.3.3 User Desktop and Files

Another feature of IntelliMirror is its ability to make a user's applications, files, and desktop settings follow him around the network. Whatever machine he logs into is reconfigured, within reason, to be like his home machine, with all applications, data, and settings in place.

3 SECURITY SYSTEMS IN WINDOWS 2000

In this section, we will look at the details of the Windows 2000 systems and managers that you can use to secure a system.

3.1 SECURITY CONFIGURATION WITH MMC

Most of the security configuration in Windows 2000 is done with Microsoft Management Console (MMC) snap-ins. If you open the Administrative Tools folder within the Control Panel folder all of the control panels found there are actually links to Microsoft Common Console (.MSC) documents which are the configuration "console" files for the MMC. These consoles specify which snap-ins to load when starting the MMC. The following consoles are the most common ones used for security management.

- *Security Configuration and Analysis* `%SystemRoot%\system32\secconf.msc`
- *Security Templates* `%SystemRoot%\security\templates`
- *Group Policy* `%SystemRoot%\system32\gpedit.msc`
- *Local Security Policy* `%SystemRoot%\system32\secpol.msc`

If you want to modify or create a new console, open the console with MMC using the /a switch. The /a switch puts the MMC into *author* mode, allowing you to make changes to the console file. You can then add other snap-ins to the console to keep your often used ones together. For example, when developing a template strategy, it is useful to add the *Security Templates* snap-in to the *Security Configuration and Analysis* console. In that way you can quickly move between the template editor and the system analyzer within a single console.

3.1.1 How Security Settings Flow

Before you can use the security configuration consoles, you need to understand how the security settings flow between group policies, local policies, local settings, security settings databases, and security templates. Because of the way information flows between these different objects, settings you may think you have made may be changed without you knowing it.

When a group policy setting is made on a domain controller, that policy is automatically pushed to the connected client systems whenever they login and again every ninety minutes or so. Those settings overwrite the local policy settings on the client computer. When a machine starts up or a user logs in, the policy settings override any local settings in the registry. They don't change the local settings, they are simply used in place of the local settings if they exist.

There are three, main, policy editor consoles used with Windows 2000: *Security Configuration and Analysis*, *Group Policy*, and *Local Security Policy*. When run on a client machine, both the *Group Policy* and *Local Security Policy* consoles save the system configuration information in the database,

```
%SystemRoot%\security\Database\secedit.sdb
```

Whenever you make a change in a system's local policy, that change is made in both the system's registry and in the database. Note, however, that the *Group Policy* and *Local Security Policy* consoles do NOT read the registry when displaying the current settings, they only read the database.

> **Warning:** There is a problem here in that the *Group Policy* and *Local Security Policy* editors could indicate that a system has some required settings and the actual settings could be completely different. If a user changes some registry settings using RegEdit or by double clicking a .reg file, he could change security settings in the registry and these two consoles would not know it. Before trusting the results of the consoles, perform a system shutdown and reboot to force the database to be updated.

The *Security Configuration and Analysis* console works differently. While it does save security settings in a database, when you run the analyzer function, it examines and displays the real registry settings. If you don't run the analyzer function, the data you see is from the database which was created the last time you ran analyze. The database is,

```
%SystemRoot%\security\Database\secanalysis.sdb
```

The main drawback of the *Security Configuration and Analysis* console is that you cannot make individual registry changes with it, you can only apply all the settings in a template.

Now, all of this may seem confusing, but consider the following example. There are two registry values in the WinLogon key that create the login banners, one for the banner caption and one for the banner body.

Key:

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\WinLogon
```

Values:

```
LegalNoticeCaption = “The caption text.”
LegalNoticeText = “The body of the banner.”
```

Here, HKLM stands for HKEY_LOCAL_MACHINE.

In the absence of any policy settings, these two keys define the title and contents of the banner. On Windows 2000, there is a second pair of values in a different registry key.

Key:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system
```

Values:

```
LegalNoticeCaption = “The local policy caption text.”
LegalNoticeText = “The local policy body of the banner.”
```

These are the local policy registry keys. Whenever someone logs into the system, if either of these keys contains a string value, that value takes precedence over the values in the WinLogon key. That is, any defined values in the `Policies` keys override similar values in the system’s or application’s keys. In this way, a local policy overrides a local setting.

If a group policy is set for a domain, whenever the group policy values are pushed out to a system, those values actually overwrite the values in the `Policies` keys. In this way, the group policy overwrites local policy, which overrides local settings.

These registry values determine what is actually displayed in the login banner. If you start the *Local Security Policy* editor and open Local Policies/Security Options in the tree view, you see the two policies listed below,

```
Message title for users attempting to log on
Message text for users attempting to log on
```

The values displayed for these policies are the values from the database, not from the registry. If you change any of these values, the change is applied to the database and to the values in the `Policies` registry key. However, there is nothing to prevent Active Directory or a user with regedit (the registry editor) from changing those keys after they have been set with the security consoles. See Appendix F for the location of all the registry settings used by Group Policy.

We have seen the values in the database change to the values in the registry without us actually doing it, so there is a system process that compares the database to the registry and makes changes as needed. This process appears to run at boot time and every so often during the day.

Basically, what we are saying here is to not depend on the *Local Security Policy* or the *Group Policy* consoles to tell you what the current policy is on a system. You must use the *Security Configuration and Analysis* console and perform an analysis of your system before you can declare the state of the settings on that system.

3.1.2 Using the Security Configuration and Analysis Console

The *Security Configuration and Analysis* console is the primary console document for configuring the security of a system. This console has two capabilities. First, it analyzes a system's security settings and compares them to a template. Any settings that do not match the template are marked. Second, it applies all the security settings in a template to a system, making hundreds of settings in a single pass.

The *Security Configuration and Analysis* console makes security settings in the following areas:

- Account Policies
- Local Policies
- Event Log
- Restricted Groups
- System Services
- Registry
- File System

An explanation of each of the individual policy settings is in Appendix E. The Account Policies area consists of two subareas:

- Password Policy
- Account Lockout Policy
- Kerberos Policy

The Password Policy subarea consists of settings of password length, complexity and age. The Account Lockout subarea sets the number of failed logins that will lock out an account, the duration of the lockout, and the time to reset the account. The Kerberos policy is available if you are using Kerberos authentication. It contains several timeouts for the ticket granting service.

The Local Policies area consists of three subareas:

- Audit Policy
- User Rights Assignment
- Security Options

The audit policies include login/logoff, policy changes, and privilege use. Auditing of file access is done on a directory by directory basis. User rights are the privileged things a

user is allowed to do, such as login remotely or shutdown a machine. Security Options gets just about everything else that cannot be classified in the previous subareas.

The Event Log area contains all the settings for the Application, Security, and System event logs. The settings include the size of the logs and access to them.

The Restricted Groups area allows you to make two settings on the security-sensitive groups. You can set the members of a group and you can set what groups a group is a member of. The restricted groups are,

- Administrators
- Backup Operators
- Guests
- Power Users
- Replicator
- Users

The System Services area allows you to set which services are allowed to run in a system and when they are to run (at boot or when needed). In a single computer, system services are configured using the Services control panel. Using the System Services policy, you can override any of the control panel settings.

The Registry area sets access to different parts of the system registry. Different keys within the registry can have their access restricted to certain individuals in the same manner that you restrict access to files.

The File System area allows you to set the access security on files or directories.

3.1.3 Using the Analyzer

The console maintains two tables in the database, one containing the state of the system the last time the system was analyzed and a second containing a template. To analyze a system, choose Security Configuration and Analysis in the tree view and choose the Analyze Computer Now action. When the analysis process is complete, all settings that are defined in the database and that match the actual setting have a green check on the setting's icon. Those that are defined in the database and that do not match the actual setting get a red x on the icon. Those settings that are not configured in the database show a plain icon.

3.1.4 Configuring From a Template

To configure a system using the settings in the template, choose Security Configuration and Analysis in the tree view and choose the Configure Computer Now action. All of the settings in the current template are made on the computer system.

3.1.5 Managing Templates

To load a template, choose Security Configuration and Analysis in the tree view and choose the Import Template action. The template you choose is added to the template currently in the database. Items defined in the new template replace those previously in the database. However, items that are defined in the database but that are not defined in the new template are retained in the database. Choosing the Export Template action writes the current template into a template file.

If you want the database to contain only the imported template, you must first create a new database and then import the template. You create a new database using the Open database action and specifying a database name that does not exist. As part of the database creation process, the console asks for a template.

The templates themselves are text files and can be opened and edited. While changing values in a template is not straightforward, deleting sections is. If you want a template that contains only the file access parts of an existing template, it is not difficult to figure out which part of the template deals with files and to delete the others. Watch out for string definitions in the templates as the strings are used in the templates themselves and should not be deleted.

To change a template using the Security Configuration and Analysis console, select the security setting you want to change and either double click it or choose the Security action. The Analyzed Security Policy Setting dialog box opens. The contents of the dialog box depend on the type of security setting you are making. Your first choice is to determine if you want to include this setting in the template. Check the “Define this policy in the database.” check box if you want to include this option in the template. After that you set whatever setting you want the security setting to have and click OK. The setting is now in the template database and is compared to the current value of the security setting. The setting is not applied to the actual security setting until you choose to configure the computer from the template.

This console is often combined with the *Security Templates* console, which is a security template editor and which contains eight built-in templates designed to provide different levels of security for workstations or servers. The templates are stored in the following directory.

```
%SystemRoot%\security\templates
```

The included templates have three levels of security,

- Basic
- Compatible
- Secure
- Highly Secure
- Dedicated Domain Controller

The templates come in versions for a workstation, server, and domain server.

The basic templates apply the Windows 2000 default security settings to all security areas except those pertaining to user rights. The basic templates are available primarily to undo the application of one of the more secure templates. They do not modify the user rights areas because these areas are often modified by the installation of applications and to reset them to the default would likely break the applications.

The compatible templates decrease the security of the Users group to the point where they can run applications not certified for Windows 2000. These settings are equivalent to the Users setting in Windows NT 4. The default way to run non certified applications in Windows 2000 is to put the users in the Power Users group.

The secure templates implement the recommended security settings for all areas except files, folders, and registry keys.

The highly secure templates make security settings for network communications that limit network communications to other Windows 2000 computers. Computers with the highly secure settings will not be able to communicate with computers running Windows 95, 98, or NT.

The dedicated domain controller template increases the security on a domain controller which does not run any server based applications. The default configuration of a Windows 2000 domain controller is reduced to allow server based applications to run. If you do not run any server based applications on the domain controller, you can increase its security with this template.

3.1.6 Using the Local Security Policy Console

The Local Security Policy console sets security policy on the local machine. That is, it sets values in the Policies registry key.

There are four areas managed with the Local Security Policy console,

- Account Policies
- Local Policies
- Public Key Policies
- IP Security Policies on Local Machine

Account policies and local policies are the same as are in the Security Analysis and Configuration console. Public key policies contains a subarea Encrypted Data Recovery Agents. Values in that subarea contain encryption certificates used for encrypting data.

The IP Security Policies on Local Machine area contains security rules for communicating with other machines. That is, which machines require encrypted connections and what to do if a machine asks for an encrypted connection.

The console can import or export a template, and can use the same templates as are used by the Security Configuration and Analysis console. The biggest difference between the Security Configuration and Analysis and the Local Security Policy consoles is that when

a template is imported, it is immediately applied to the registry. Also, while it can use the same templates as are used by the Security Configuration and Analysis console, it only applies those parts that are in the four areas listed above.

In addition to using templates, you can set individual values using this console without having to apply a whole template. To set or change policies, select the item you want to change and choose the change you want to make from the Action menu.

3.1.7 Using the Group Policy Console

The Group Policy console sets group policy on a domain server and local group policy on a workstation. The Group Policy has two main areas.

- Computer Configuration
- User Configuration

Within both areas are three subareas, however the contents of the subareas are different depending on which of the major areas is selected.

- Software Settings
- Windows Settings
- Administrative Templates

Under Computer Configuration/Software settings, there are no default values on a workstation. Under Computer Configuration/Windows Settings are,

- Scripts
- Security Settings

The scripts subarea contains a place where you can specify startup and shutdown scripts. The Security Settings area is identical to that in the Local Security Policy console.

The Administrative templates area does not really contain templates but individual settings that are pushed out to a workstation. The area contains four subareas,

- Windows Components
- System
- Network
- Printers

The Windows Components subarea contains settings for applications installed along with Windows 2000 such as Internet Explorer and Netmeeting. The System subarea contains settings for logon, Disk Quotas, DNS Clients, Group Policy, and Windows file protection. The Network subarea contains settings for Offline files and Network and dialup connections.

Under the User Configuration/Software settings, there are no default values on a workstation. Under Windows Settings, there are three subareas,

- Internet Explorer Maintenance
- Scripts

- Security Settings

Internet Explorer Maintenance contains settings for the default user's Internet Explorer's settings. The Scripts area contains a place for setting logon and logoff scripts and the Security settings area contains no values for a workstation.

The Administrative Templates area contains settings for,

- Windows Components
- Start Menu & Taskbar
- Desktop
- Control Panel
- Network
- System

The settings contained here include those that allow you to control the user's desktop, start menu, and what settings the user can make in the control panel. For the most part, these are administrative control rather than security items.

3.2 KERBEROS

The default authentication and access control mechanism for a pure, Windows 2000 network is Kerberos version 5. Other authentication mechanisms are available for mixed environments with older versions of Windows such as LanManager (LM), NT LanManager (NTLM), and NTLM v2. The LM protocol is only needed for older systems and should be avoided if possible because the authentication handshake and password are not encrypted.

3.3 SMARTCARDS

As an alternative to Kerberos, smartcards can be used for user authentication and access control. Use of smartcards does require more hardware, including the cards themselves for each user and a card reader at each machine.

3.4 PUBLIC KEY CRYPTOGRAPHY

Public key cryptography is the foundation for many of the security services available on Windows 2000, including Kerberos, smartcards, IPSec, VPN, and others.

3.5 IPSEC

IPSec (IP Security) is an extension of the IP networking protocol that adds encryption and authentication to network packet traffic. The security is added at a low level in the protocol stack so that applications do not need to know anything about it. As far as they are concerned, packets are sent and received with clear data. It is the low-level security systems that do the encryption and decryption of packets to protect them while they are traversing the Internet.

3.6 IPFILTERING

IP Filtering is a setting in Windows 2000 networking where you can explicitly set which IP protocols and ports are going to accept incoming packets. For IP Filtering to work, you must specify every port on your computer that is going to be open to receive incoming packets. Much of the effectiveness of IP Filtering is in preventing accidental port openings as disabling or removing unneeded services already blocks most ports.

3.7 ENCRYPTING FILE SYSTEM

An encrypting file system is available on Windows 2000. With it, you may encrypt a single file, a whole directory or a whole disk drive. Protected files are encrypted with an encryption key that is encrypted with the user's key and, optionally, a recovery key and kept with the file. When a file is accessed, the key is decrypted and used to decrypt the file "on the fly". That is, files are not decrypted to disk, but are decrypted sector by sector as the sector is needed. When the file is written back to disk, the sectors are encrypted before writing. Keep in mind, that if you Save As a file to an unencrypted directory the file will not be encrypted. Only if it is saved back to the original encrypted file name or into an encrypted directory is it encrypted before saving it to disk.

In general, you should encrypt whole directories so that temporary files created by applications and written to disk are also encrypted. You should also consider encrypting any temp directories on a system as they are also used by applications for temporary file storage.

3.8 VPN

Virtual Private Networking is essentially a way to make a remote workstation appear to be on an internal company network. It does this by creating an encrypted, virtual pipe from the workstation to a machine on the internal network where the pipe is decrypted and the packets are placed on the internal network. As far as the remote machine and the internal machines are concerned, the remote machine appears to be directly connected to the internal network.

VPN is primarily used by people using their laptops on travel to access company records or people working at home who must access internal company records. Care must be taken with laptops that implement a VPN connection to an internal network that the VPN connection is not setup to automatically connect with a stored password. If that was the case, a stolen machine would give the thief access to the internal company network by simply turning it on.

4 SECURING A WINDOWS 2000 WORKSTATION

Windows 2000 Workstation is optimized for a desktop workstation. That is, foreground applications have higher priority and there are not so many server type functions available.

The best way to install Windows 2000 is on a freshly formatted hard drive. This type of installation eliminates all legacy settings and applications that may be reducing the efficiency of the system. Reformatting a hard drive also re-writes and realigns all the tracks on the drive that may have moved slightly because of heat and ageing of the drive. A problem with such an installation is that all your applications and settings are lost and must be reinstalled or reentered.

The next best way to install Windows 2000 is a clean install into an existing disk partition. You do this by placing it in a different directory from the existing Windows system (for example, /winnt2 instead of /winnt). You still loose most of your settings and you must reinstall all of your applications but most of the application data files (such as e-mail files, address books, and favorites lists) are not lost.

Lastly, you can perform an upgrade of an existing Windows system to Windows 2000. This type of upgrade preserves all of your settings and applications, including your file permissions for the system and other directories. If you are upgrading from Windows NT 4, the Windows 2000 installer does not normally change your existing security settings to what might be optimal for Windows 2000.

4.1 INSTALLING WINDOWS 2000

The basic installation of Windows 2000 onto a clean hard drive or a clean installation onto an existing system is relatively straight forward. You simply boot the installation program and follow the instructions.

1. **Disconnect the system from the Internet if it is connected.**
   The process of installing a new system opens several security holes that must be closed before the system can be put on the network.

2. **Start the Windows installer.**
   Place the Windows installation CD into the drive and reboot. If your system does boot the installation CD, you must start the installer using the installation floppies.

3. **Follow the directions for a new installation.**

4. **Set the installation partition.**
   When the system asks you what partition to install windows into, you have the choice of deleting, creating, or using the existing partitions. If you want a clean installation onto a formatted disk, delete the partition where you want to install the system and then recreate it. Recreating the partition causes it to be formatted. Note that formatting the partition deletes everything on it.

5. **Set the file system in the partition to NTFS.**
   The NTFS file system is required in order to apply protections to the files and directories. There is no file system protection for a FAT or FAT32 file system.

6. **Choose the location for the windows directory.**
   If you are installing onto a clean disk, accept the default directory name (/winnt). If you are doing a clean install onto an existing disk, choose a different name for the directory (such as /winnt2). Later, you can delete the old windows directory.

7. **Use a strong Administrator password.**
   Make sure the administrator's password is a strong password with adequate length (8 characters) and complexity (mix of text, numbers, and punctuation).

8. **Follow the directions to complete the installation.**

4.2 UPGRADING NT TO WINDOWS 2000

Upgrading an existing Windows NT 4 system to Windows 2000 proceeds much like an installation onto an existing partition, with the difference that you install into the existing windows directory.

1. **Disconnect the system from the Internet if it is connected.**
   The process of installing a new system opens several security holes that must be closed before the system can be put on the network.

2. **Start the Windows installer.**
   You can do this by booting the system with the old system, inserting the Windows 2000 installation CD and choosing to upgrade the existing system. You can also boot the system as before using the installation CD or floppies and choosing to upgrade the existing system.

3. **Set the file system in the partition to NTFS.**
   The NTFS file system is required in order to apply protections to the files and directories. There is no file system protection for a FAT or FAT32 file system.

4. **Choose to upgrade the existing Windows directory.**

5. **Follow the directions to complete the installation.**

4.3 POST INSTALL SECURITY SETTINGS

After installing Windows 2000, you must make several updates before the system can be safely put onto the Internet. These updates include installing the latest service pack and any post service pack security updates.

If possible, copy the service pack and updates onto a CD and use that for installation. In this way, the security holes are closed before a system is placed on the Internet. If it is not possible to get a CD of the service pack, you can place the system on the Internet, download, and install the service pack directly from the Microsoft Windows Update website (windowsupdate.microsoft.com). Note that there is a link to the Windows Update website on the Start menu. Because the system is not completely patched yet, connection to the Windows Update website and patching of the system must be done immediately

after connecting the system to the Internet. If the system is going to be left for some time before the installation of the service pack and patches are complete, you should disconnect it from the Internet.

1. **Connect the system to the Internet.**
   Plug the network cable into the computer and set the Networking properties for your system on your local subnet. You must set the computer name, IP address, gateway, and nameservers, or you can specify a DHCP server where your system can get that data.

Warning: If you are not immediately going to install the service pack and patches, pull the network cable out of the back of the computer to remove it from the Internet. Reinsert the network cable only when you are ready to continue.

2. **Connect to the Windows Update website.**
   (http://windowsupdate.microsoft.com) and click Product Updates.
   When you connect to the Product Updates page on the Windows Update website, the server will ask to install a Java program on your system to evaluate what updates you need. When asked, allow that program to be installed and run.

3. **Install the latest service pack.**
   From the list of required updates, select the latest service pack and install it. Some of the updates can be installed together but others must be installed separately and the system rebooted to complete the install before installing something else.

4. **Reboot your system when told to do so.**

5. **Install other updates.**
   Connect to the Windows update website again and select any required updates and patches. Download and install them. Make a note of the date of the most recent update package. You may need to do steps 4 and 5 several times before you get all of the updates installed.

6. **Upgrade Internet Explorer.**
   Even if you are not going to be using Internet Explorer as your web browser, several programs and system utilities use it, so update it to the latest version. The latest version of Internet Explorer can also be installed from the Windows Update website. In general, you should do a custom installation of Internet Explorer so you can limit the other applications installed along with it. Of special concern is the Outlook Express mail client. If you are not using Outlook Express as your mail client, make sure it isn't installed by the Internet Explorer installer.

7. **Reboot the system when told to do so.**

8. **Run Windows Update again.**
   Connect to the Windows update Product Updates website again and check that all required patches have been installed.

9. **Reboot the system when told to do so.**

At this point, your system is reasonably safe. Next, you need to check for any recent fixes that have not yet made it to the Windows Update website.

1. **Go to the Windows Security Site (http://www.microsoft.com/security/).**

2. **Select Security Bulletins.**

3. **Filter the bulletins by operating system and service pack.**
   Sort the bulletins by Windows 2000 Professional and the service pack (2) you just installed. See if there are any important security concerns for the system with dates after the date of the latest update package that you installed above.

4. **Download and install any hotfixes noted in the bulletins.**

Note: Most hot fixes require a reboot after each installation. To install multiple hotfixes and only have to reboot once at the end, download and use the qchain program from the Microsoft website. By running qchain after running all of your installation programs, you can run several installers and only do a reboot after the last installation. See Appendix B more information on qchain.

5. **Download the HFNETCHK.EXE program.**
   The HFNETCHK.EXE program is available in the Windows Security Toolkit on the Microsoft website

   http://www.microsoft.com/technet/security/tools/content.asp

   This program downloads a list of security patches and information on how to determine if they have been installed.

6. **Run HFNETCHK.EXE**
   Run HHNETCHK.EXE (See Appendix A) when asked to allow the download of an XML file from Microsoft, click yes. Make note of any missing hotfixes. Note that hotfixes marked as a "Warning" are those where the program cannot determine if they are installed or not. You must know if they were included in the updates.

Note: HFNETCHK.EXE can be run on one machine but gather patch information for all machines on a Windows domain (you must run it as the domain administrator). See Appendix A for more information on hfnetchk.

7. **Install any required hotfixes.**
   Find the hot fix bulletins on the security page, download, and install them.

8. **Reboot the system again just for good measure.**
   Many Windows installations need to change files that are in use and can't be

replaced while the system is running. These files are placed in a special queue and are replaced at system startup (this is why Windows is always telling you to reboot the system).

4.3.1 NTFS File Systems

The NTFS file system is usually specified during installation of the system. If you are doing an upgrade of an existing system you may have a FAT or FAT32 file system. The NTFS file system is needed in order to be able to do file and folder level access permissions. To check a disk to see what type of file system it contains, open My Computer, right click on a disk drive and select properties. On the general tab of the properties dialog box it should say File system: NTFS. If it does not, you need to run the convert utility to convert the file system to NTFS. The convert utility will convert a FAT or FAT32 file system to NTFS without having to reformat the drive. While it should not damage any files on the drive, it is a good idea to backup any critical files just in case. To run the convert utility, open a command window and type the following command:

```
convert drive: /fs:ntfs
```

where *drive* is the drive letter of the drive you want to convert. If it cannot lock the drive because it is in use, it will do the conversion the next time you reboot your system.

4.3.2 Security Configuration and Analysis

Run the Security Configuration and Analysis console in the Control Panels/Administrative Tools directory and use it to apply the CIAC template to your system. Using this tool sets most of your required security settings. The list of settings in the CIAC template is in Appendix E.

1. **Start the Security Configuration and Analysis console.**
   Look for it in Control Panel/Administrative tools. You must run the tool as local Administrator on the machine you are going to configure or as the Domain Administrator.

2. **Open the CIAC template.**
   Select Security Configuration and Analysis in the tree view and choose the Import Template Action. Find the CIACWorkstation or CIACDomainController templates, depending on which kind of a machine you are configuring. And open it.

3. **Analyze the system.**
   With Security configuration and Analysis selected, choose the Analyze Computer Now action. All the objects in the template will be checked and compared to the actual settings on the system.

4. **Examine the proposed changes.**
   Examine any objects listed in the console that have a red X on them as they do not

match the template and will be changed. Make sure the proposed changes are consistent with the planned use of the system.

5. **Apply the settings in the template.**
   With Security Configuration and Analysis selected, Choose the Configure Computer Now action. When this is done, your computers settings should match those in the template. Running Analyze Computer Now again should show no differences between the computer settings and the template.

4.3.3 Disable Unneeded Network Services

Any network service that is running on a system can provide a hole that an intruder can use to break in and take control of your system. Thus, any network services that you are not using should be disabled or uninstalled from your system. Of primary importance is the Internet Information Server (IIS) which provides a web, mail, and news server for the network. Most workstations do not need any of these services so the IIS can be uninstalled if it was installed by the system installer.

To see what services are running on a system, open the Control Panel and double click on Administrative Tools, and then double click on Services. From the services control panel, you can start or stop a service, set when a service starts, or disable it. For service startup you can pick one of the three options.

- Automatic – The service starts when the system boots.
- Manual – A program can start the service when it needs it.
- Disabled – A service cannot be startup.

Alternately, from the Security Configuration and Analysis console, choose the System Services area to see all the running system services plus you can see which were set by the template and which are still at their default values.

4.3.4 Disable or Delete Unnecessary Accounts

The unnecessary accounts consist primarily of the Guest account and any of the Anonymous login accounts created for the IIS server or other services. The first account to get rid of is Guest. At the minimum, it should be disabled. To further protect a system, replace the Everyone group with the Authenticated Users group everywhere in the file system. The Authenticated Users group is the same as Everyone but without Guest and without Anonymous.

If you are using the IIS, you probably have a guest like account called IUSR_machinename where machinename is the name of the machine you are working on. This account is used for the initial connection of a person to a web server. Everyone who connects to a web server on a machine first becomes IUSR_machinename. Ater that, if he attempts to download web files from a protected directory he must authenticate and become a real user of the system. If you plan to allow anonymous access to a web server, be sure the IUSR_machinename account has access to all the files you want him to have

access to and to no other files. If you are not using a web server on your machine, remove this account.

Another anonymous account is the IWAM_machinename account. This is created by the Web Application Manager for the same reason as the IUSR_machinename account is created for IIS. Web applications are services that are accessed through the Web server but that run as a separate process. The IWAM_machinename account is used for the initial connection to the process.

4.3.5 Set Directory Protection

The default directory protections set in Windows 2000 are relatively secure, compared to previous versions of Windows. If you do a clean installation of Windows 2000 all the directory permissions will be set to these default values. If you upgrade from Windows NT 4, the installer will keep your previous permissions and you will need to adjust them to raise the security of your system.

Templates containing the default directory permissions for Windows 2000 are in the following files,

`%SystemRoot%\inf\defltwk.inf` - Workstations
`%SystemRoot%\inf\defltsv.inf` – Stand Alone Server
`%SystemRoot%\inf\defltdc.inf` – Domain Controller

Either of these files can be opened by the Security Configuration and Analysis console and used to analyze your system. Do not apply these templates as they contain many more settings than the file system settings. To set only the file system options, copy the template and edit is with a plain text editor such as Notepad. Remove all the sections that do not have to do with the filesystem. Be careful you don't delete any strings defined in the template for use in the template. You then start the Security Configuration and Analysis console, create a new database with the Open database command and then import the new template. You must create a new database because any settings that are not set in the template are remembered from previous templates you have applied to this system.

4.3.6 Restrict Remote Access to the Registry

This item is set in the Registry area of the CIAC template in Appendix E. The registry key is,

```
HKLM\System\CurrentControlSet\Control\SecurePipeServers\Winreg
```

Set the access control to this key to Administrators full control only. Allow no one else access to this key.

However, some services need access to this key in order to operate. For example, the Spooler and Replicator services need access. You can either add the account name that the service runs under to the access list of the `Winreg` key or define the `AllowedPaths`

key under the `Winreg` key and add a machine value containing the paths to the keys to bypass security on. This key is not created by the CIAC Template. Create the key,

```
HKLM\System\CurrentControlSet\Control\SecurePipeServers
      \Winreg\AllowedPaths
```

Name: `machine`
Type: `REG_MULTI_SZ`
Value:
```
System\CurrentControlSet\Control\ProductOptions
System\CurrentControlSet\Control\Print\Printers
System\CurrentControlSet\control\Server Applications
System\CurrentControlSet\Services\Eventlog
Software\Microsoft\Windows NT\CurrentVersion
```

See the Microsoft Knowledge Base article Q155363 for more information.

4.3.7 Set Protections on Registry Keys

These settings are in the Registry section of the CIAC template.

4.3.8 Restrict Anonymous Access to the LSA

The LSA is the Local Security Authority and contains information about current users and accounts. You should restrict Anonymous access to this key so intruders cannot gain information about a system they could then use to attack that system. To restrict access to the LSA, add the following value to the LSA key.

```
HKLM\System\CurrentControlSet\Control\LSA\
```

Name: `RestrictAnonymous`
Type: `REG_DWORD`
Value: `1`

4.3.9 Strong Password Policy

These settings are part of the local Account Policy. This password policy is set in the CIAC template. The password policy needs to be strengthened to insure that passwords cannot be guessed by an intruder. Do this by setting the following policies:

- Minimum length: 8
- Password history: 10
- Maximum password age: 180 days
- Password complexity: Enabled

Password history prevents a user from reusing an old password. Password complexity requires that a password not contain the account name and that it contains characters from three of the following groups.

- Lower case letters
- Upper case letters
- Numbers

- Symbols

4.3.10 Set the Account Lockout Policy

These settings are part of the local Account Policy. This account lockout policy is set in the CIAC template. The lockout policy prevents an intruder from using a dictionary attack on a system by locking out an account after a certain number of login failures. A dictionary attack attempts to log on to a users account by trying all of the passwords in a dictionary of passwords, one at a time.

Set the following account lockout policies:

- Account lockout duration: 30 minutes
- Account lockout threshold: 5 invalid logins
- Reset account lockout counter after: 30 minutes

With these settings, an account is locked out after 5 login failures but will be automatically reset after 30 minutes. Note that the Administrator's account cannot be locked out.

4.3.11 Configure the Administrator's Account

Because the Administrator account is available on all Windows systems, it is a well known attack point for intruders. It is useful to change the name of the Administrator account (not root or Admin) to something else to make it more difficult for an intruder to attack a system.

You should also enable account lockout for the Administrator account for network logins. Do this with the passprop.exe utility from the Server resource kit. The command to enable administrative lockouts is,

```
passprop /adminlockout
```

Note that this does not lockout the Administrator account from console logins. To reverse this setting, use the `/noadminlockout` switch.

4.3.12 Remove any Unnecessary File Shares

File shares consist of two types; those created by the user and administrative shares created by the system. Unlike Windows NT 4, administrative shares cannot be permanently deleted. While you can delete them for the current session, they return the next time the system reboots or the *server* service is stopped and restarted. Administrative shares are only accessible (read) by the local Administrators, Backup Operators, and Server Operators.

Shares are administered with the Computer Management MMC console in the System Tools\Shared Folders\Shares area. Shares starting with a $ are administrative shares. In this console, you can add or delete user created shares and set permissions on those shares. Remove any user shares that are not needed.

You can also see the current shares on a system using the following command in a command window.

```
net shares
```

You can also delete shares at the command prompt by typing,

```
net shares sharename /delete
```

Where `sharename` is the name of the share you want to delete.

4.3.13 Set Appropriate Protections on Necessary Shares

Protecting required shares can be accomplished in two places. You can either place protections on the share, or on the files and folders within the share. It is not necessary to place protections in both places. It is common practice to set the permissions on a share to everyone full access and to then set restrictive access controls on the shared folder itself.

To set permissions on a share, right click the shared folder and choose sharing to display the sharing dialog box. Click the permissions button to see the current access controls on the folder. Change those permissions as necessary. To set permissions on the shared folder, right click on the folder, choose properties and select the security tab. In the properties dialog box, set the access controls on the folder.

The share permissions on administrative shares are read for local Administrator, Backup Operator, and Server Operator and cannot be changed.

4.3.14 Install Antivirus Software

With the large number of viruses available today, antivirus software is a must. When using antivirus software, be sure of the following items.

- The antivirus software and virus definitions are up-to-date. Current packages update weekly over the Internet.
- Active virus protection is operating. Active virus protection checks every file when it is accessed and every e-mail message when it is downloaded.
- Scan critical files at startup (boot sector, root directory, system files).
- Scan all files on a weekly basis.

5 SECURING A WINDOWS 2000 DOMAIN SERVER

Installation of a Windows 2000 Server or Domain Server proceeds much like that for a Windows 2000 workstation, with the following exceptions.

- Installation of the Internet Information Server (IIS) software.
- Patching and security settings for IIS.
- Policy configuration using the server policy settings.

5.1 INSTALLATION OF INTERNET INFORMATION SERVER (IIS) SOFTWARE

If this server is going to serve up files using network services such as web, ftp, net news, and e-mail, you are going to have to install the Internet Information Server (IIS). Normally, the IIS is installed automatically with every server installation unless you have explicitly indicated that you do not want it installed. You can also install it later by opening the Add/Remove Programs control panel and clicking Add/Remove Windows Components. The IIS installation is one of the listed options.

When you are installing the IIS on a server, click the details box and only select those options that you are going to use. If you are not going to need the FTP service, don't install it. If you have already installed it, uninstall it in the same control panel. Generally, you will need the Internet Information Server Snap-in plus any servers you want to install. The snap-in is used to manage the server.

Do not install the FrontPage extensions, documentation, and sample applications on your working server. FrontPage extensions, documentation and sample applications are for web page development and should only be placed on a web development machine that is only accessible to the web developers. When new web pages are ready to be published onto the main server, they should be copied onto the server using a protected connection such as VPN or SFTP (Secure FTP, a part of SSH), or using a program such as ROBOCOPY, which is available in the resource kit. RoboCopy uses the LanManager connection to copy files and so should be run through an IPSec secured connection to the server. RoboCopy is useful for pushing over files because the files it pushes can be selected so it does not push over the sample or FrontPage files and only files that have changed are copied to the server.

5.2 POST INSTALL SECURITY SETTINGS

5.2.1 Patching IIS

After the IIS server is installed, you should connect to WindowsUpdate (http://windowsupdate.microsoft.com), or to wherever you maintain your security patches, and install all required security patches.

5.2.2 Set Appropriate Web Directory Permissions

Set permissions for the various files within your web application to give yourself the most protection. It is easiest to partition the web space into folders that separate the executable content such as programs and scripts from the static content such as web pages and images. In this way, you can set the permissions at the folder level and the files in the folder will inherit the permissions.

Remove the Everyone group from all the web directories. Create a WebUser group and put any users who are going to have access to this website in that group. If this is going to

be an anonymous web server (no login required), put the IUSR_machinename user into the WebUser group. Give the WebUser read only access to the directories containing static files and execute access for directories containing scripts and executables.

In addition, give the Administrator and System users full control to these directories. On your development machine, create a WebDevelopers group to contain the usernames of the people who are going to be allowed to create and modify web pages and give that group Full Access to all of the web pages.

Warning: On development systems where the Front Page server extensions are installed, do not change the permissions of the directories that start with _vti (for example, _vti_bin) as it is the file permissions on these directories that controls who can remotely administer the web. If you give the IUSR_machinename user execute access to the auth.dll file in the _vti_bin\auth directory, anyone who can connect to your webserver will be able to change your web pages without being required to login.

Warning: Beware when reinstalling web services such as the Front Page extensions. The FrontPage installer assumes you are going to be developing an anonymous website and gives everyone read access to the whole site when it is installed. Be sure to go back and check file permissions after reinstalling any web related software.

Because this happens so often, you should create a Security Configuration and Analysis template that sets the appropriate access control on all the directories in your website. After reinstalling web software you can check for any changes using the Analyze now action and reset the access control using the Configure now action.

5.2.3 Set Access Controls on IIS Log Files

The IIS-generated log files are in the following directory,

```
%systemroot%\system32\LogFiles
```

Set the access permissions to that directory to the following, to prevent intruders from deleting the web files to hide their activities.

- Administrators (Full Control)
- System (Full Control)
- WebUser (Read Write Create)

5.2.4 Turn on Web Logging

Turn on web logging using the Internet Information Services MMC console. Select the site you are setting and click properties. In the dialog box that appears, click the Web Site

tab and check Enable Logging. Click the Active Log Format drop down list and select W3C Extended Log File Format. Select the following properties to log.

- Client IP Address
- User Name
- Method
- URI Stem
- HTTP Status
- Win32 Error
- User Agent
- Server IP Address
- Server Port

5.2.5 Turn on Secure Sockets Layer Encryption

If this is not going to be an anonymous website, that is, you are going to require your users to login, you need to protect the communications. If you are using basic authentication, which is what you must use if your users are remotely accessing your web server and you are using Windows file protections to control access, you should protect the whole session. This is because the username and password are sent to the server with every web request after the initial login and they are only protected with a simple hash that is easily broken.

If your web application is doing the login and then controlling the later connections with a cookie, you need only encrypt the login pages.

To turn on SSL encryption, you first need a server certificate which you can buy from vendors like VeriSign or create yourself using a certificate generator. Note that to use a self generated server certificate, all your users must set their browsers to trust your root certificate. The certificate request is generated and the resulting key is installed using the Key Manager console.

After the certificate is installed, SSL is activated using the Internet Information Server console. Select the file or directory you want to protect and choose properties. Choose the Directory Security tab and click the Edit button under Secure Communications. Check Require Secure Channel when accessing this resource to turn on SSL. Click Encryption Settings and check Require 128 bit Encryption to require high security instead of 40 bit encryption.

> **Note:** Using SSL is supposed to significantly slow down web communications, but our experience indicates that it is not noticeable.

5.2.6 Remove All Sample Applications

Sample applications should only be allowed on the web development server which can only be accessed by the web developers. Remove all sample applications from the

production servers. These samples need to be deleted off the hard drive and the Virtual directory removed from the website.

Some common samples installed automatically by web server installers are as follows:

```
C:\inetpub\iissamples
C:\inetpub\iissamples\sdk
C:\inetpub\AdminScripts
C:\Program Files\Common Files\System\msadc\Samples
```

5.2.7 Remove the IISADMPWD Virtual Directory

This directory allows you to change Windows NT passwords using the web.

Open the Internet Information Server console and find IISADMPWD in the list of virtual directories. Click on that one and click Delete. You can also remove the files which are in the following directory.

```
%SystemRoot%\System32\inetsrv\iisadmpwd
```

5.2.8 Remove the IISADM Virtual Directory

This directory allows you to configure the web server using web pages.

Open the Internet Information Server console and find IISADM in the list of virtual directories. Click on that one and click Delete. You can also remove the files which are in the following directory.

```
%SystemRoot%\System32\inetsrv\iisadm
```

5.2.9 Remove Unused Script Mappings

The IIS is configured to support several common file extensions. The server operates by specifying which .DLL file to use to process each file type. Any extensions that you are not using should be removed.

Open Internet Services Manager console, click on the Default Web server and choose properties. Click Home Directory and Configuration to open the App Mappings window. Select any file extensions that you are not using and click Delete. Most modern servers use Active Server Pages and web pages with server-side includes. All the others can probably be removed. The index server extensions are tied to several vulnerabilities and should be removed.

Extension	Description
.asp, .asa	Active Server Pages
.htr	Web-based Password Reset

.ida, .idq, .htw	Index Server
.idc	Internet Database Connector (obsolete use ADO from Active Server Pages)
.shtm, .stm, .shtml	Web pages containing server-side includes

5.2.10 Disable RDS Support

The RDS Data Factory is probably the most attacked facility in the IIS server. It is used to allow special Active-X controls on web pages to directly connect to a database through a web server without having to reload the whole page. If it is not being used, it should be removed. If it is being used, you should make sure it is well patched and up to date.

To disable it, open the default website and find the MSADC virtual directory. Click on it and click delete. You can also delete the files themselves which are in the following directory.

```
%SystemDisk%\Program Files\Common Files\system\msadc
```

6 MAINTAINING SECURITY CONFIGURATIONS

Now that you have your system configured and secure, how do you keep it that way. As fast as we apply security patches, intruders find other ways into out systems. The following tools are available to help keep your systems configured and secure.

- WindowsUpdate
- HFNETCHK
- Critical Update Notification
- Microsoft Security Bulletins

6.1 USING WINDOWS UPDATE

WindowsUpdate is actually a website that you connect your system to.

```
http://windowsupdate.microsoft.com
```

In the web page that opens, click on Product Updates to begin the process. A java applet is downloaded to your system along with a database of required updates. The Java applet will examine your system and give you a list of all the updates installed on your system and any new updates that you might need. The updates are divided into six classes.

- Critical Updates
- Picks of the Month
- Advanced Security Updates
- Recommended Updates

- Additional Windows Features
- Device Drivers

Generally, you should always install any critical updates that are listed. Consider the other updates only if your application needs them. To install any updates, simply check them, click install, and follow the directions.

6.2 USING HFNETCHK

HFNETCHK is another tool for examining a system and listing any needed updates and security patches. It is useful to a system manager because it can examine all the machines in a domain from a single location.

Download HFNETCHK from the following location.

```
http://www.microsoft.com/technet/security/tools/hfnetchk.asp
```

When you run the tool, it downloads the latest database of required patches and hot fixes from Microsoft. If you execute it without any options, it scans the system you are running it on. If you use the -r switch followed by an IP address range it will scan all the computers in that range. Note that the computers in the range must be in your domain and you must be logged in as the domain admin to access the systems. The result is a list of Microsoft technet article numbers and security bulletin numbers that you can then access to get more information about the patch. Note that patches listed with a warning are those that it does not know how to detect. You will have to determine by other means (such as computer logs or notes) if the patch is in place.

Appendix A shows the results of a run of the HFNETCHK tool.

6.3 USING CRITICAL UPDATE NOTIFICATION

Critical Update Notification is a tool you install in Windows 2000 that watches the Microsoft security website for new critical updates. If a new critical update is available , the tool displays a dialog box giving you the option to go to the windowsupdate website to install the critical update.

The critical update notification tool is included with Windows 2000 and is installed by default. The tool is also available from the windowsupdate website

```
http://windowsupdate.microsoft.com
```

6.4 USING MICROSOFT SECURITY BULLETINS

Microsoft security bulletins are available on the Microsoft website at the following address.

```
http://www.microsoft.com/technet/security/current.asp
```

You can also subscribe to the bulletins and have them delivered by e-mail at that same site.

6.5 MICROSOFT PERSONAL SECURITY ADVISOR

http://www.microsoft.com/technet/security/tools/mpsa.asp

6.6 MICROSOFT SECURITY CHECKLISTS

http://www.microsoft.com/technet/security/tools/tools.asp

7 REFERENCES

The following reference materials contain a considerable amount of information about the setup and management of Windows 2000. System managers

Microsoft, *Windows 2000 Professional Resource Kit*, Microsoft Press, (2000)

Microsoft, *Windows 2000 Server Resource Kit*, Microsoft Press, (2000)

Microsoft Windows Security Website
`http://www.microsoft.com/security`

NSA, NSA Windows 2000 Configuration Guides, National Security Agency, ()
`http://nsa2.www.conxion.com/win2k/index.html`

NIST System Administration Guidance for Securing Microsoft Windows 2000 Professional System, Special Publication 800-43, National Institute of Standards and Technology, (2002)
`http://csrc.nist.gov/itsec/guidance_W2Kpro.html`

CIAC Bulletin J-043g: Creating Login Banners
`http://www.ciac.org/ciac/bulletins/j-043.shtml`

APPENDIX A – USING HFNETCHK UPDATE MANAGER

A sample run of the HFNETCHK tool.

```
H:\hfnetchk tool>hfnetchk

Microsoft Network Security Hotfix Checker, 3.1
Developed for Microsoft by Shavlik Technologies, LLC
info@shavlik.com (www.shavlik.com)

 ** Attempting to download the XML from
http://download.microsoft.com/download/
ml/security/1.0/NT5/EN-US/mssecure.cab. **

 ** File was successfully downloaded. **

 ** Attempting to load H:\Projects\hfnetchk tool\mssecure.xml. **

Using XML data version = 1.0.1.152  Last modified on 10/11/2001.

Scanning BEATRICE
.........................
Done scanning BEATRICE
----------------------------
BEATRICE
----------------------------


        WINDOWS 2000 SP2


                WARNING         MS01-022        Q296441
                Patch NOT Found MS01-041        Q298012
```

APPENDIX B - - USING QCHAIN

Windows installers for security patches often cannot replace files that are in use. To replace these files, they schedule a startup job that replaces the file at boot time and require a reboot when the installer completes. This is why Windows installers are always requiring reboots. If you try to install multiple patches, the startup job for one patch may overwrite the startup job for a previous patch. The Qchain program is available on the Microsoft website to chain several patches together and apply them without having to reboot between each patch.

```
http://support.microsoft.com/support/kb/articles/Q296/8/61.asp
```

APPENDIX C – DOE LOGIN BANNER

Login banners are required on all U.S. Department of Energy computers. CIAC Bulletin J-043g: *Creating Login Banners* contains the current banner and instructions for installing it on different operating systems. On Windows systems, the banner and its title are installed in the following registry key.

`HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon`

Name: `LegalNoticeCaption`

Type: `REG_SZ`

Value: `NOTICE TO USERS`

Name: `LegalNoticeText`

Type: `REG_SZ`

Value: See notice below.

The same values can be inserted in the Policies registry key, whose values override those in the winlogon key.

`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\system`

Following is the text of the banner.

NOTICE TO USERS

This is a Federal computer system and is the property of the United States Government. It is for authorized use only. **Users (authorized or unauthorized) have no explicit or implicit expectation of privacy.**

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. **By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel.**

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

APPENDIX D – INCLUDED SECURITY CONFIGURATION MANAGER TEMPLATES

The Windows 2000 operating system contains several built-in templates that work with the Security Configuration and Analysis console. These templates define different levels of security for a Windows system.

DEFAULT INSTALLATION TEMPLATES

These templates define the default configuration of a newly installed Windows 2000 system.

`%SystemRoot%\INF\defltwk.inf` - Workstation
`%SystemRoot%\INF\defltsv.inf` - Stand alone server
`%SystemRoot%\INF\defltdc.inf` - Domain Controller

SECURITY TEMPLATES

The security templates come in three different levels, basic, secure, high-security, dedicated domain controller, and compatibility. These templates are all in the default location for the Security Configuration and Analysis console.

`%SystemRoot%\security\templates`

Basic Security Templates

The basic security templates are primarily for reversing the application of the higher security templates. They set all the security settings to the Windows 2000 default values except for user rights.

`basicwk.inf`- Workstation
`basicsv.inf` - Stand alone server
`basicdc.inf` - Domain Controller

Secure Templates

The Secure templates implement the recommended security settings for everything but files, folders, and registry keys. The default configuration for files, folders, and registry keys is considered to be secure.

`securews.inf`- Workstation or Server
`securedc.inf` - Domain Controller

High Security Templates

The High-security templates add settings for secure Windows 2000 network communications to the Secure templates. These settings are only usable in a pure Windows 2000 network as older versions of Windows will not be able to communicate with this system.

`hisecws.inf`- Workstation or Server

`hisecdc.inf` - Domain Controller

Compatible Template

The compatible template is primarily for upgrades of Windows 2000 from Windows NT. Widows 2000 Users have stricter security settings than Users in Windows NT so Windows 2000 Users may not be able to run some legacy applications that have not been certified to run under Windows 2000. The Windows 2000 Power Users are comparable to the Windows NT Users. If you do not want your normal users to be in the Power Users group in order to run legacy applications, you can apply the compatibility template which decreases the security of the Users group to the point where they should be able to run legacy applications.

`compatws.inf`- Compatible Workstation

Setup Security Template

The Setup Security template contains the default configuration settings placed on this system when it was installed. This gives you a chance to get back to the installation configuration. Some application installers change directory permissions and user rights and this template may reverse those settings. Be careful with the application of this template as it may make some applications unexecutable.

`setup security.inf`- Setup Security Settings

Dedicated domain Controller Template

Use the Dedicated Domain Controller template on domain controllers that do not run other server based applications. The security settings on Domain Controllers are designed to allow the Administrator run server based applications on the domain controller. This causes the security of the local Users group to be less than ideal. Apply this template on Domain Controllers that do not run other server based applications.

`dedicadc.inf` - Dedicated Domain Controller

APPENDIX E – CIAC SECURITY CONFIGURATION AND ANALYSIS TEMPLATE

This appendix describes all the settings that you can make in the Security Configuration and Analysis MMC console. The title of each table refers to the location in the Security Configuration and Analysis console where the setting exists. We also include the suggested CIAC setting for each of these items. Items marked "Not Defined" are not set in the CIAC templates. DC = Domain Controller, AD = Active Directory, Empty means the option is defined but contains no values.

ACCOUNT POLICIES/PASSWORD POLICY

Policy	Description	Workstation Setting	DC Setting
Enforce password history	The number of passwords the system remembers to prevent a user from reusing an old password too soon.	10	10
Maximum password age	The maximum age of a password after which it must be changed. Reduce this to 90 days if the passwords are sent in the clear over the network, such as with the old LanManager protocol.	180 days	180 days
Minimum password age	The minimum amount of time a user must wait before changing a password again. This is to prevent a user from defeating the password history by changing the password multiple times.	0 days	0 days
Minimum password length	The minimum length for a password.	8 characters	8 characters
Passwords must meet complexity requirements	Require a password to not include the account name and to contain characters from at least three of the following character sets: lower case letters, upper case letters, numbers, and symbols.	Enabled	Enabled
Store password using reversible encryption for all users in the domain	Stores passwords in the clear for applications that need them for authentication.	Disabled	Disabled

ACCOUNT POLICIES/ACCOUNT LOCKOUT POLICY

Policy	Description	Workstation Setting	DC Setting
Account lockout duration	The length of time an account is locked out because of login failures. A locked out account will be reenabled after this time.	30 minutes	30 minutes
Account lockout threshold	The number of login failures that triggers a lockout. This is to prevent someone from trying to b This does not apply to the Administrator account, which cannot be locked out. Network logins to the administrator account can be set to lock out. See key???	5 invalid logon attempts	5 invalid logon attempts
Reset account lockout counter after	The count of login failures is reset to zero after this amount of time.	30 minutes	30 Minutes

ACCOUNT POLICIES/KERBEROS POLICY

These only apply if you are using Kerberos authentication.

Policy	Description	Workstation Setting	DC Setting
Enforce user logon restrictions	Requires the KDC to validate every request for a session ticket.	Disabled	Enabled
Maximum lifetime for service ticket	The maximum time that a session ticket may be used to access a service. Must be greater than 10 minutes and less than the Maximum lifetime for a user ticket.	600 minutes	600 minutes
Maximum lifetime for user ticket	The Maximum lifetime for a user's ticket granting ticket may be used.	10 hours	10 hours
Maximum lifetime for user ticket renewal	The period over which a user's ticket granting ticket may be renewed.	7 days	7 days
Maximum tolerance for computer clock synchronization	The maximum difference between a server's clock and a user's clock that will be tolerated. This is to prevent "replay attacks" where an attempt is made to reuse an old ticket by setting back the clock on a workstation.	5 minutes	5 minutes

LOCAL POLICIES/AUDIT POLICY

Policy	Description	Workstation Setting	DC Setting
Audit account logon events	Audit success or failure of logons to other systems where this system was used to authenticate the user. This only has meaning on a domain controller.	No Auditing	Success, Failure on a DC.
Audit account management	Audit the success or failure of account management actions, such as creating, changing or deleting a new account, changing a password, etc.	Success, Failure	Success, Failure
Audit directory service access	Audits the success or failure of access to an Active Directory object. This only has meaning on an Active Directory domain controller.	No Auditing	Success, Failure if this is an AD DC.
Audit logon events	Audit success or failure of logons to this system. Includes both console and network logons.	Success, Failure	Success, Failure
Audit object access	Audit success or failure of accesses to system objects such as files, folders, printers, etc. as long as the object has its own access control setting.	Success, Failure	Success, Failure
Audit policy change	Audit success or failure of changes to the user rights, audit, or trust policies on this machine.	Success, Failure	Success, Failure
Audit privilege use	Audit the success or failure of a user exercising a user right except Backup and Restore. See also "Audit use of Backup and Restore privilege."	Success, Failure	Success, Failure
Audit process tracking	Audit process startup, shutdown, handle duplication, and indirect object access. This is primarily a debugging tool.	No Auditing	No Auditing
Audit system events	Audit system startup, shutdown, and changes to the auditing system.	Success, Failure	Success, Failure

LOCAL POLICIES/USER RIGHTS ASSIGNMENT

Policy	Description	Workstation Setting	DC Setting
Access this computer from the network	Users who may make network logins to this computer. If this is an IIS server, the IIS guest account (IUSR_*machinename*) must be here even if you are going to force an authenticated login.	Backup Operators, Power Users, Users, Administrators	Backup Operators, Power Users, Users, Administrators
Act as part of the operating system	Allows a process to authenticate as any user, giving it access to all of a users resources. Normally only needed by low level resources.	Empty	Empty
Add workstations to domain	Users who may create computer accounts in a domain. Only valid on a domain controller.	Empty	Authenticated Users
Back up files and directories	Users who may circumvent file protections to backup a system. Gives read access to the whole system. See also Restore Files and Directories.	Backup Operators, Administrators	Backup Operators, Administrators
Bypass traverse checking	Users who may bypass traverse file access checking. Allows a user to pass over a directory for which he does not have access to read files in a subdirectory for which he does have access.	Backup Operators, Power Users, Users, Administrators	Administrators, Authenticated Users
Change the system time	Users who may change the system clock.	Administrators, Power Users	Administrators, Server Operators
Create a pagefile	Users with the ability to create or change a pagefile.	Administrators	Administrators
Create a token object	Accounts that can be used to create access tokens. This should only be used by low level system processes.	Empty	Empty
Create permanent shared objects	Accounts that can create a directory object in the Windows 2000 object manager. This should only be used by low level system objects.	Empty	Empty
Debug programs	Users who can attach a debugger to any process. Software developers may need this.	Administrators	Administrators
Deny access to this computer from the network	Users who may not access this computer from the network. Supercedes “Access this computer	Empty	Empty

	from the network." if a user appears in both.		
Deny logon as a batch job	Users who may not login as a batch job. Supercedes "Log on as a batch job." if a user appears in both.	Empty	Empty
Deny logon as a service	Users who may not register a process as a service. Supercedes "Log on as a service." if a user appears in both.	Empty	Empty
Deny logon locally	Users who may not login locally. Supercedes "Login locally." if a user appears in both.	Empty	Empty
Enable computer and user accounts to be trusted for delegation	Users who may use another user's delegated credentials.	Empty	Administrators
Force shutdown from a remote system	Users who may remotely shutdown a computer.	Administrators	Administrators, Server Operators
Generate security audits	Users who may generate entries in the system security log. This right is normally only used by low level system processes.	None	None
Increase quotas	Users who may increase the processor quota of a process	Administrators	Administrators
Increase scheduling priority	Users who may change the execution priority of a process.	Administrators	Administrators
Load and unload device drivers	Users who may dynamically load and unload device drivers.	Administrators	Administrators
Lock pages in memory	Obsolete, not used.	None	None
Log on as a batch job	Users who may login as a batch job. Used by processes like the task scheduler to run a batch job as a user. See also "Deny log on as a batch job."	Not defined	Not defined
Log on as a service	Users who may register a process as a service. See also "Deny log on as a service."	Not defined	Not defined
Log on locally	Users who can log on locally. This includes logons at the console and the guest accounts (such as IUSR_*machinename*) who must authenticate as a real user to get expanded access.	Backup Operators, Power Users, Users, Administrators	Backup Operators, Account Operators, Print Operators, Administrators

Manage auditing and security log	Users who may specify auditing on system objects such as files, directories, and Active Directory objects. Software developers may need this.	Administrators	Administrators
Modify firmware environment values	Users who may modify system wide environment variables.	Administrators	Administrators
Profile single process	Users who may use process profiling tools to measure the performance of non system processes. Software developers may need this.	Administrators, Power Users	Administrators
Profile system performance	Users who may use process profiling tools to measure the performance of system processes.	Administrators	Administrators
Remove computer from docking station	Users who may undock a laptop from a docking station. Domain controllers should not be undockable.	Power Users, Users, Administrators	None
Replace a process level token	Users who can replace the access token of a running process. This right is normally only used by low level system processes.	Empty	Empty
Restore files and directories	Users who can circumvent local file and directory protections to restore files from a backup. See also “Back up files and directories.”	Backup Operators, Administrators	Backup Operators, Server Operators, Administrators
Shut down the system	Users who, while logged on locally, can shut down the system. See also, “Force shutdown from a remote system.”	Backup Operators, Power Users, Users, Administrators	Backup Operators, Account Operators, Server Operators, Print Operators, Administrators
Synchronize directory service data	Unused	Not defined	Not defined
Take ownership of files or other objects	Users who can take ownership of secured objects, such as files, directories, processes, printers, etc.	Administrators	Administrators

LOCAL POLICIES/SECURITY OPTIONS

Policy	Description	Workstation Setting	DC Setting
Additional restrictions for anonymous connections	Determines additional restrictions that are placed on anonymous connections. Options are: • **None. Rely on default permissions.** • **Do not allow enumeration of SAM accounts and shares.** Replaces "Everyone" with "Authenticated Users" in the security permissions for resources. • **No access without explicit anonymous permissions.** Removes anonymous user from "Everyone" and "Network." Anonymous accounts must be given explicit access to objects. Everyone = Authenticated Users + Guest + Anonymous	Do not allow enumeration of SAM accounts and shares	Do not allow enumeration of SAM accounts and shares
Allow server operators to schedule tasks (domain controllers only)	Allows server operators to submit At jobs for later execution.	Not defined	Not defined
Allow system to be shut down without having to log on	Enables the Shut Down command on the login window. On most systems, users who can access the login screen also have access to the plug so it is better to allow them to do a controlled shutdown than to simply pull the plug.	Enabled	Enabled
Allowed to eject removable NTFS media	Users who may eject removable NTFS media.	Administrators and Interactive User	Administrators
Amount of idle time required before disconnecting session	Amount of idle time before a SMB connection (Windows networking) connection is automatically disconnected.	15 minutes	15 minutes
Audit the access of global system objects	Adds system access control lists to system objects such as events, semaphores, and drivers so access to	Disabled	Disabled

	these objects can be audited.		
Audit use of Backup and Restore privilege	Adds Backup and Restore privilege use to “Audit Privilege Use”. Enables “Audit Privilege Use.”	Disabled	Disabled
Automatically log off users when logon time expires	Domain user accounts with explicit login hours are logged off if they are outside those hours. If this is disabled, a login that is made during a users normal hours is allowed to continue outside of those hours.	Enabled	Enabled
Automatically log off users when logon time expires (local)	Local user accounts with explicit login hours are logged off if they are outside those hours. If this is disabled, a login that is made during a users normal hours is allowed to continue outside of those hours.	Enabled	Enabled
Clear virtual memory pagefile when system shuts down	Clear the systems pagefile (swap) when the system shuts down to insure that there is no sensitive data accessible on the disk.	Enabled	Enabled
Digitally sign client communication (always)	Always digitally sign SMB (Windows Networking) client (you are the client connecting to a server) communications. Prevents man-in-the-middle attacks. Both ends of the communication must support the signing.	Disabled	Disabled
Digitally sign client communication (when possible)	Digitally sign SMB (Windows Networking) communications when possible. Prevents man-in-the-middle attacks. Both ends of the communication must support the signing. Enable this one to be able to connect to servers that require digital signatures.	Enabled	Enabled
Digitally sign server communication (always)	Always sign SMB (Windows Networking) server (you are the server) communications. Prevents man-in-the-middle attacks. Both ends of the communication must support the signing. Clients who do not have digital signing enabled will not be able to connect.	Disabled	Disabled
Digitally sign server communication	Sign SMB (Windows Networking) server (from you to a server) communications when possible.	Disabled	Enabled

(when possible)	Prevents man-in-the-middle attacks. Both ends of the communication must support the signing.		
Disable CTRL+ALT+DEL requirement for logon	Disables the requirement to press Ctrl-Alt-Del to get the login window. Enabling this makes a machine susceptible to password capture programs. Beware of reverse logic.	Disable	Disable
Do not display last user name in logon screen	Does not display the last user to login in the login dialog box. Should be enabled on publicly accessible, multi-user machines.	Disabled	Disabled
LAN Manager Authentication Level	Set the authentication for network authentication. Older systems (Win95) require LanManager (LM) logins. Windows NT 4 prior to SP4 require LM or NTLM logins. This should be set as high as possible while still allowing all required systems to communicate. The allowed settings are: • **Send LM & NTLM responses:** Clients use LM and NTLM authentication, and never use NTLMv2. DCs accept LM, NTLM, and NTLMv2 autheitication. • **Send LM & NTLM - use NTLMv2 session security if negotiated:** Clients use LM and NTLM authentication and use NTLMv2 session security if the server supports it. DCs accept LM, NTLM, and NTLMv2 authentication. • **Send NTLM response only:** Clients use NTLM authentication only and use NTLMv2 session security if the server supports it. DCs accept LM, NTLM, and NTLMv2 authentication. • **Send NTLMv2 response only:** Clients use NTLMv2	Send LM & NTLM responses	Send LM & NTLM responses

	authentication only and use NTLMv2 session security if the server supports it. DCs accept LM, NTLM, and NTLMv2 authentication. • **Send NTLMv2 response only\refuse LM:** Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. DCs refuse LM and accept only NTLM and NTLMv2 authentication. • **Send NTLMv2 response only\refuse LM & NTLM:** Clients use NTLMv2 authentication only and use NTLMv2 session security if the server supports it. DCs refuse LM and NTLM, and accept only NTLMv2 authentication.		
Message text for users attempting to log on	The body (text) of the logon banner seen before viewing the login dialog box. See Appendix C DOE Login Banner.	DOE login banner text. See Appendix C DOE Login Banner.	DOE login banner text. See Appendix C DOE Login Banner
Message title for users attempting to log on	The title (text) of the logon banner dialog box. See Appendix C DOE Login Banner.	Notice To Users	Notice To Users
Number of previous logons to cache (in case domain controller is not available)	User credentials from this many previous logons are cached and used in the event that a domain controller is not available.	10 logons	10 logons
Prevent system maintenance of computer account password	Prevents the password of the computer account from being changed every seven days.	Disabled	Disabled
Prevent users from installing printer drivers	Prevents members of the Users group from installing printer drivers.	Disabled	Disabled
Prompt user to change password before expiration	The number of days of advanced warning to give computer users about an impending expiring password.	14 days	14 days
Recovery Console:	Allows login to the recovery console	Disabled	Disabled

Allow automatic administrative logon	without an administrator password. The Recovery Console is a system repair option that can be installed as an NT Loader boot option.		
Recovery Console: Allow floppy copy and access to all drives and all folders	Enables the recovery console's SET command so that you can enable wildcard support, enable access to all files, enable access to removable media, and disable the prompt when overwriting a file.	Disabled	Disabled
Rename administrator account	Change the account designated as the computer Administrator account to make it more difficult for intruders to attack a system. Don't put a value here in a template you are going to apply to many machines or you will change the name of the Administrator account on every machine to the same value.	Not defined	Not defined
Rename guest account	Change the account designated as the Guest account to make it more difficult for intruders to attack a system. Don't put a value here in a template that is going to be applied to many machines or you will change the name of the Guest account on every machine to the same name.	Not defined	Not defined
Restrict CD-ROM access to locally logged-on user only	Prevents the CD-ROM from being shared over the network.	Disabled	Disabled
Restrict floppy access to locally logged-on user only	Prevents the floppy disk from being shared over the network.	Disabled	Disabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Requires that the secure channel between the computer and the domain server encrypt or sign the data in the channel. Set this only if all servers in a domain support secure channel encryption. Automatically enables "Secure channel: Digitally sign secure channel data (when possible)" when enabled.	Disabled	Disabled

Secure channel: Digitally encrypt secure channel data (when possible)	Encrypt the secure channel between a computer and the domain server when possible. Enable this to use the highest encryption possible when a computer communicates with a server using the secure channel. Automatically enables “Secure channel: Digitally sign secure channel data (when possible)” when enabled.	Enabled	Enabled
Secure channel: Digitally sign secure channel data (when possible)	Sign the secure channel between a computer and the domain server when possible. Enable this to increase the authentication of the secure channel to a server. This is automatically enabled if “Secure channel: Digitally encrypt secure channel data (when possible)” or “Secure channel: Digitally encrypt or sign secure channel data (always)” are enabled.	Enabled	Enabled
Secure channel: Require strong (Windows 2000 or later) session key	Requires the use of strong encryption in the secure channel between a computer and a server. Only enable if all trusted domain controllers can handle strong encryption.	Disabled	Disabled
Secure system partition (for RISC platforms only)	Prevent access to the system partition of RISC platform to all but the Administrator. This applies only to RISC systems.	Enabled	Enabled
Send unencrypted password to connect to third-party SMB servers	Send unencrypted passwords to older SMB (Windows networking) servers. This should not be enabled unless there is no other way to connect to the older SMB servers.	Disabled	Disabled
Shut down system immediately if unable to log security audits	Enabling this causes a system to be halted if a security log cannot be written. Security log failures are usually caused by the security log being full. Be careful when enabling this on a server. This can also be set in Event Log/Settings for Event Logs.	Disabled	Disabled
Smart card removal behavior	Determine the behavior of a system when the logged in users smart card	Lock Workstation	Lock Workstation

	is removed. The options are: • No Action • Lock Workstation • Force Logoff		
Strengthen default permissions of global system objects (e.g. Symbolic Links)	When enabled, shared system resources such as DOS names and semaphores can be read but not changed by non-Administrator users that created them. Disabling it allows non-Administrator users to change objects they create.	Enabled	Enabled
Unsigned driver installation behavior	Determines the behavior of a system when there is an attempt to install an unsigned device driver. The options are: • Silently succeed • Warn but allow installation • Do not allow installation You may need to change this behavior if you must use an unsigned driver and you trust the driver.	Do not allow installation	Do not allow installation
Unsigned non-driver installation behavior	Determines the behavior of a system when unsigned software (other than drivers) is installed on a system. The options are: • Silently succeed • Warn but allow installation • Do not allow installation	Silently succeed	Silently succeed

EVENT LOG/SETTINGS FOR EVENT LOGS

Policy	Description	Workstation Setting	DC Setting
Maximum application log size	Sets the maximum size for the application log file.	2048 kilobytes	2048 kilobytes
Maximum security log size	Sets the maximum size for the security log file.	2048 kilobytes	2048 kilobytes
Maximum system log size	Sets the maximum size of the system log file.	2048 kilobytes	2048 kilobytes
Restrict guest access to application log	Prevents the guest account from accessing the application log.	Enabled	Enabled
Restrict guest	Prevents the guest account from	Enabled	Enabled

access to security log	accessing the security log.		
Restrict guest access to system log	Prevents the guest account from accessing the system log.	Enabled	Enabled
Retain application log	If the retention method for the application log is “By days”, list the number of days of log data to maintain in the file.	Not Defined	Not Defined
Retain security log	If the retention method for the security log is “By days”, list the number of days of log data to maintain in the file.	Not Defined	Not Defined
Retain system log	If the retention method for the system log is “By days”, list the number of days of log data to maintain in the file.	Not Defined	Not Defined
Retention method for application log	Set the method for wrapping the application log file. The options are: • Overwrite events as needed Overwrite old events only when the space is needed for new events. • Overwrite events by days Delete events older than the number of days set in “Retain application log.” • Do not overwrite events Do not overwrite any events. When the log file fills, generate an error.	As needed	As needed
Retention method for security log	Set the method for wrapping the application log file. The options are: • Overwrite events as needed Overwrite old events only when the space is needed for new events. • Overwrite events by days Delete events older than the number of days set in “Retain application log.” • Do not overwrite events Do not overwrite any events. When the log file fills, generate	As needed	As needed

	an error or shut down the system. See "Shut down the computer when the security audit log is full."		
Retention method for system log	Set the method for wrapping the application log file. The options are: • **As needed -** Overwrite events as needed Overwrite old events only when the space is needed for new events. • **By days -** Overwrite events by days Delete events older than the number of days set in "Retain application log." • **Manually -** Do not overwrite events (clear manually) Do not overwrite any events. When the log file fills, generate an error.	As needed	As needed
Shut down the computer when the security audit log is full	Don't use. Use "Shut down system immediately if unable to log security audits" in Local Policies/Security Options instead. Enabling this causes a system to be halted when the security log is full.	Disabled	Disabled

RESTRICTED GROUPS

Members are the users who are in a group and *Members Of* are the groups this group is a member of. Most of these are not set in the templates as the settings tend to be site specific and the template will overwrite whatever users are already defined for the groups. Windows 2000 will not let you overwrite everything. For example, the Administrator is always a member of the Administrators group. If you try to remove him with this template, Windows 2000 will put him back.

Group Name	Members	Member Of
Administrators	Not defined	Not defined
Backup Operators	Not defined	Not defined
Guests	Not defined	Not defined
Power Users	Not defined	Not defined
Replicator	Not defined	Not defined

Users	Not defined	Not defined

SYSTEM SERVICES

System services are all the services running on the current system. On a single computer, system services are configured using the Services control panel. Using the System Services policy, you can override the control panel settings. In addition, you cans set the permissions and auditing for each service. Startup options are,

- Automatic – The service starts automatically when needed.
- Manual – The Service must be manually started by an application.
- Disabled – The service cannot be started.

The permission codes used in the template files are,

- CC - Query template
- DC - Change template
- LC - Query status
- SW - Enumerate dependents
- RP - Start
- WP - Stop
- DT - Pause and continue
- LO - Interrogate
- CR - User-defined control
- SD - Delete
- RC - Read permissions
- WD - Change permissions
- WO - Take ownership

These permissions are grouped as the following,

- Read = CC, LC, SW, LO, CR, RC
- Read – CR = CC, LC, SW, LO, RC
- Write = DC, RC
- Start, stop, and pause = RP, WP, DT, RC
- Delete = SD
- Full Control = CC, DC, LS, SW, RP, WP, DT, LO, CR, SD, RC, WE, WO

Workstation Settings

Service Name	Startup	Permission	Auditing
Application Management	Manual	**Authenticated Users:** Read - CR **Administrators:** Full Control **Power Users:** Read - CR **INTERACTIVE:** Read - CR - RC + Start **Users:** Read - CR - RC + Start	**Everyone:** Fail, Full Control
ClipBook	Manual	**Authenticated Users:** Read - CR	**Everyone:** Fail, Full Control

		Administrators: Full Control **Power Users:** Read - CR **INTERACTIVE:** Read - CR - RC + Start	
Computer Browser	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
DHCP Client	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Distributed Link Tracking Client	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
DNS Client	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Event Log	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
IPSEC Policy Agent	Automatic	(A;;CCLCSWLORC;;;AU) **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Logical Disk Manager	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Messenger	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Net Logon	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start	**Everyone:** Fail, Full Control

		Administrators: Full Control **SYSTEM:** Read + Start + Stop + Pause	
Network DDE	Manual	**Authenticated Users:** Read - CR **Administrators:** Full Control **Power Users:** Read - CR **INTERACTIVE:** Read - CR - RC + Start	**Everyone:** Fail, Full Control
Network DDE DSDM	Manual	D:**Authenticated Users:** Read - CR **Administrators:** Full Control **Power Users:** Read - CR **INTERACTIVE:** Read - CR - RC + Start	**Everyone:** Fail, Full Control
Plug and Play	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Print Spooler	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Protected Storage	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Remote Procedure Call (RPC)	Automatic	**Authenticated Users:** Read - CR **Administrators:** Full Control **Power Users:** Read - CR **INTERACTIVE:** Read - CR - RC + Start **Users:** Read - CR - RC + Start	**Everyone:** Fail, Full Control
Remote Registry Service	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Removable Storage	Automatic	**Administrators:** Full Control **Authenticated Users:** Read **Power Users:** Read+Start **SYSTEM:** Read + Start + Stop	**Everyone:** Fail, Full Control

		+ Pause	
RunAs Service	Automatic	**Administrators:** Full Control **Authenticated Users:** Read **Power Users:** Read+Start **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Security Accounts Manager	Automatic	**Authenticated Users:** Read - CR **Administrators:** Full Control **Power Users:** Read - CR **INTERACTIVE:** Read - CR - RC + Start **Users:** Read - CR - RC + Start	**Everyone:** Fail, Full Control
Server	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
System Event Notification	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Task Scheduler	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
TCP/IP NetBIOS Helper Service	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Windows Time	Automatic	**Authenticated Users:** Read - CR **Administrators:** Full Control **Power Users:** Read - CR **INTERACTIVE:** Read - CR - RC + Start **Users:** Read - CR - RC + Start	
Workstation	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control

Server Settings

Service Name	Startup	Permission	Auditing
Alerter	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Application Management	Manual	**Authenticated Users:** Read - CR **Administrators:** Full Control **Power Users:** Read - CR **INTERACTIVE:** Read - CR - RC + Start **Users:** Read - CR - RC + Start	**Everyone:** Fail, Full Control
ClipBook	Manual	**Authenticated Users:** Read - CR **Administrators:** Full Control **Server Operators:** Full Control **Power Users:** Read - CR **INTERACTIVE:** Read - CR - RC + Start	**Everyone:** Fail, Full Control
Computer Browser	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
DFS	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
DHCP Client	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Distributed Transaction Coordinator	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control	**Everyone:** Fail, Full Control

		Server Operators: Full Control **SYSTEM:** Read + Start + Stop + Pause **Authenticated Users:** Start	
Distributed Link Tracking Client	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
DNS Client	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Event Log	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
IPSEC Policy Agent	Automatic	**Authenticated Users:** Read - CR **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
License Agent	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Logical Disk Manager	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Messenger	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop	**Everyone:** Fail, Full Control

		+ Pause	
Net Logon	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Network DDE	Manual	**Authenticated Users:** Read - CR **Administrators:** Full Control **Server Operators:** Full Control **Power Users:** Read - CR **INTERACTIVE:** Read - CR - RC + Start	**Everyone:** Fail, Full Control
Network DDE DSDM	Manual	D:**Authenticated Users:** Read - CR **Administrators:** Full Control **Server Operators:** Full Control **Power Users:** Read - CR **INTERACTIVE:** Read - CR - RC + Start	**Everyone:** Fail, Full Control
Plug and Play	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Print Spooler	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Protected Storage	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Remote Procedure Call (RPC)	Automatic	**Authenticated Users:** Read - CR **Administrators:** Full Control **Power Users:** Read - CR **INTERACTIVE:** Read - CR - RC + Start **Users:** Read - CR - RC + Start	**Everyone:** Fail, Full Control

Remote Registry Service	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Removable Storage	Automatic	**Administrators:** Full Control **Authenticated Users:** Read **Power Users:** Read+Start **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
RunAs Service	Automatic	**Administrators:** Full Control **Server Operators:** Full Control **Authenticated Users:** Read **Power Users:** Read+Start **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Security Accounts Manager	Automatic	**Authenticated Users:** Read - CR **Administrators:** Full Control **Power Users:** Read - CR **INTERACTIVE:** Read - CR - RC + Start **Users:** Read - CR - RC + Start	**Everyone:** Fail, Full Control
Server	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
SMTPSVC	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
System Event Notification	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Task Scheduler	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control	**Everyone:** Fail, Full Control

		Server Operators: Full Control **SYSTEM:** Read + Start + Stop + Pause	
TCP/IP NetBIOS Helper Service	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control
Windows Time	Automatic	**Authenticated Users:** Read - CR **Administrators:** Full Control **Power Users:** Read - CR **Server Operators:** Full Control **INTERACTIVE:** Read - CR - RC + Start **Users:** Read - CR - RC + Start	**Everyone:** Fail, Full Control
Workstation	Automatic	**Authenticated Users:** Read **Power Users:** Read + Start **Administrators:** Full Control **Server Operators:** Full Control **SYSTEM:** Read + Start + Stop + Pause	**Everyone:** Fail, Full Control

REGISTRY

The registry area allows you to set permissions and auditing on registry keys in the HKEY_LOCAL_MACHINE (machine) and HKEY_USERS (user) hives of the system registry. The actual permission settings are somewhat complicated so you will have to examine the Setup Security template with the Security Templates console to see them.

Object Name	Workstaions Permissions	Server Permissions
machine\software	**Users:** Read (key and subkeys) **Power Users:** Read, Write, and Delete (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read, Write, and Delete (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys) **Terminal Services User:**

		Read, Write, and Delete (key and subkeys)
machine\software\classes	**Users:** Read (key and subkeys) **Power Users:** Read, Write, and Delete (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys) **Authenticated Users:** Read (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read, Write, and Delete (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys) **Terminal Services User:** Read, Write, and Delete (key and subkeys) **Authenticated Users:** Read (key and subkeys)
machine\software\classes\.hlp	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys) **Authenticated Users:** Read (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys) **Terminal Services User:** Read, Write, and Delete (key and subkeys) **Authenticated Users:** Read (key and subkeys)
machine\software\classes\helpfile	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)

	Authenticated Users: Read (key and subkeys)	**Terminal Services User:** Read, Write, and Delete (key and subkeys) **Authenticated Users:** Read (key and subkeys)
machine\software\microsoft\command processor	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\cryptography	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\cryptography\oid		**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\cryptography\providers\trust		**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys)

		CREATOR OWNER: Full Control (key and subkeys)
machine\software\microsoft\ cryptography\services		**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\driver signing	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ enterprisecertificates	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\netdde	**Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ non-driver signing	**Users:** Read (key and subkeys) **Power Users:** Read (key	**Users:** Read (key and subkeys) **Power Users:** Read (key

	and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ole	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ protected storage system provider	Inherit from parent	Inherit from parent
machine\software\microsoft\rpc	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\secure	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\system certificates	**Users:** Read (key and subkeys) **Power Users:** Read (key	**Users:** Read (key and subkeys) **Power Users:** Read (key

	and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion	**Authenticated Users:** Read (key and subkeys)	**Authenticated Users:** Read (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\ accessibility	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\aedebug	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\ asrcommands	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys) (A;CI;GRGWSD;;;BO)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\classes	**Users:** Read (key and subkeys)	**Users:** Read (key and subkeys)

	Power Users: Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\ drivers32	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\efs	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\font drivers	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\ fontmapper	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys)

	Administrators: Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\image file execution options	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\ inifilemapping	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\perflib	(A;CI;GR;;;IU) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	(A;CI;GR;;;IU) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\ perflib\009	Inherit from parent	Inherit from parent
machine\software\microsoft\ windows nt\currentversion\ports		**Users:** Read (key and subkeys) **Power Users:** Read, Write, and Delete (key and subkeys) **Administrators:** Full

		Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\ profilelist	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\secedit	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\setup\ recoveryconsole	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\svchost	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control

	(key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	(key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\time zones	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\ windows	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows\currentversion		**Users:** Read (key and subkeys) **Power Users:** Read, Write, and Delete (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows\currentversion\group policy	Inherit from parent	Inherit from parent
machine\software\microsoft\ windows\currentversion\installer	Inherit from parent	Inherit from parent
machine\software\microsoft\ windows\currentversion\policies	Inherit from parent	Inherit from parent
machine\software\microsoft\	**Users:** Read (key and	**Users:** Read (key and

windows\currentversion\explorer\ user shell folders	subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows\currentversion\runonce	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows\currentversion\runonceex	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\microsoft\ windows nt\currentversion\ winlogon	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\software\policies	**Users:** Read (key and subkeys) **Power Users:** Read (key	**Users:** Read (key and subkeys) **Power Users:** Read (key

	and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\system	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\system\clone	Inherit from parent	Inherit from parent
machine\system\controlset001	Inherit from parent	Inherit from parent
machine\system\controlset002	Inherit from parent	Inherit from parent
machine\system\controlset003	Inherit from parent	Inherit from parent
machine\system\controlset004	Inherit from parent	Inherit from parent
machine\system\controlset005	Inherit from parent	Inherit from parent
machine\system\controlset006	Inherit from parent	Inherit from parent
machine\system\controlset007	Inherit from parent	Inherit from parent
machine\system\controlset008	Inherit from parent	Inherit from parent
machine\system\controlset009	Inherit from parent	Inherit from parent
machine\system\controlset010	Inherit from parent	Inherit from parent
machine\system\currentcontrolset\control\class	Inherit from parent	Inherit from parent
machine\system\currentcontrolset\control\computername	**Authenticated Users:** Read (key and subkeys)	**Authenticated Users:** Read (key and subkeys)
machine\system\currentcontrolset\control\contentindex	**Authenticated Users:** Read (key and subkeys)	**Authenticated Users:** Read (key and subkeys)
machine\system\currentcontrolset\control\keyboard layout	**Authenticated Users:** Read (key and subkeys)	**Authenticated Users:** Read (key and subkeys)
machine\system\currentcontrolset\control\keyboard layouts	**Authenticated Users:** Read (key and subkeys)	**Authenticated Users:** Read (key and subkeys)
machine\system\currentcontrolset\control\print\printers	**Authenticated Users:** Read (key and subkeys)	**Authenticated Users:** Read (key and subkeys)
machine\system\currentcontrolset\control\productoptions	**Authenticated Users:** Read (key and subkeys)	**Authenticated Users:** Read (key and subkeys)
machine\system\currentcontrolset\	**Administrators:** Full	**Administrators:** Full

control\securepipeservers\winreg	Control (key and subkeys) (A;;GR;;;BO)	Control (key and subkeys) (A;;GR;;;BO)
machine\system\currentcontrolset\control\session manager\executive	**Power Users:** Read, Write, and Delete (key and subkeys)	**Power Users:** Read, Write, and Delete (key and subkeys)
machine\system\currentcontrolset\control\timezoneinformation	**Power Users:** Read, Write, and Delete (key and subkeys)	**Power Users:** Read, Write, and Delete (key and subkeys)
machine\system\currentcontrolset\control\wmi\security	**Administrators:** Read (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Administrators:** Read (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
machine\system\currentcontrolset enum	Inherit from parent	Inherit from parent
machine\system\currentcontrolset\hardware profiles	Inherit from parent	Inherit from parent
machine\system\currentcontrolset\services\eventlog	**Authenticated Users:** Read (key and subkeys)	**Authenticated Users:** Read (key and subkeys)
machine\system\currentcontrolset\services\tcpip	**Authenticated Users:** Read (key and subkeys)	**Authenticated Users:** Read (key and subkeys)
users\.default	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Users:** Read (key and subkeys) **Power Users:** Read (key and subkeys) **Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
users\.default\software\microsoft\netdde	**Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)	**Administrators:** Full Control (key and subkeys) **SYSTEM:** Full Control (key and subkeys) **CREATOR OWNER:** Full Control (key and subkeys)
users\.default\software\microsoft\protected storage system provider	Inherit from parent	Inherit from parent

FILE SYSTEM

The file system permissions and auditing are set in the File System area of the templates. The following file system objects are set by the Setup Security template. To view the individual permissions settings you will have to view the template with the Security Templates console. Here, %SystemDrive% is the boot drive letter (for example C:) and %SystemRoot% is the active Windows directory (for example, C:\winnt or C:\windows) %SystemDirectory% is the active System directory (for example, C:\windows\system32).

Object Name	Workstation Permissions	Server Permissions
%SystemDrive%\autoexec.bat	**Users:** Read and Execute **Power Users:** Modify **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Modify **Administrators:** Full Control **SYSTEM:** Full Control
%SystemDrive%\boot.ini	**Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemDrive%\config.sys	**Users:** Read and Execute **Power Users:** Modify **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Modify **Administrators:** Full Control **SYSTEM:** Full Control
%SystemDrive%\ntbootdd.sys	**Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemDrive%\ntdetect.com	**Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemDrive%\ntldr	**Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemDrive%\program files	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder, subfolders, and files)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder, subfolders, and files)

	Administrators: Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files) **Terminal Server Users:** Full Control (folder, subfolder, and files)
%SystemRoot%	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files) **Authenticated Users:** Read and Execute	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files) **Authenticated Users:** Read and Execute
%SystemRoot%_default.pif	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\addins	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folders and subfolders) Power Users Read and Execute (folders, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folders and subfolders) Power Users Read and Execute (folders, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files)

	SYSTEM: Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemRoot%\clock.avi	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\config\general.idf	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\config\hindered.idf	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\config\msadlib.idf	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\connection wizard	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder,	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder,

	subfolder, and files)	subfolder, and files)
%SystemRoot%\csc	Inherit from parent	Inherit from parent
%SystemRoot%\debug\usermode	**Users:** Create Files and Create Folders (files only) **Users:** Traverse/Execute, List/Read, Create files (folder only) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files)	**Users:** Create Files and Create Folders (files only) **Users:** Traverse/Execute, List/Read, Create files (folder only) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files)
%SystemRoot%\discover.exe	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	
%SystemRoot%\driver cache	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemRoot%\explorer.exe	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control **Authenticated Users:**	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control **Authenticated Users:**

	Read and Execute	Read and Execute
%SystemRoot%\explorer.scf	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control **Authenticated Users:** Read and Execute
%SystemRoot%\fonts\ app850.fon, arial.ttf, arialbd.ttf, arialbi.ttf, ariali.ttf, ariblk.ttf, cga40850.fon, cga40woa.fon, cga80850.fon, cga80woa.fon, comic.ttf, comicbd.ttf, cour.ttf, courbd.ttf, courbi.ttf, coure.fon, courf.fon, couri.ttf, desktop.ini, dosapp.fon, ega40850.fon, ega40woa.fon, ega80850.fon, ega80woa.fon, georgia.ttf, georgiab.ttf, georgiai.ttf, georgiaz.ttf, impact.ttf, l_10646.ttf, lucon.ttf, marlett.ttf, micross.ttf, modern.fon, pala.ttf, palab.ttf, palabi.ttf, palai.ttf, roman.fon, script.fon, serife.fon, seriff.fon, smalle.fon, sserife.fon, sseriff.fon, symbol.ttf, symbole.fon, tahoma.ttf, tahomabd.ttf, times.ttf, timesbd.ttf, timesbi.ttf, timesi.ttf, trebuc.ttf, trebucbd.ttf, trebucbi.ttf, trebucit.ttf, verdana.ttf, verdanab.ttf, verdanai.ttf, verdanaz.ttf, vga850.fon, vgafix.fon, vgaoem.fon, vgasys.fon, webdings.ttf, wingding.ttf	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%Systemroot%\Help		**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder,

		and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files) **Terminal Server Users:** Read, Write, and Execute (folder, subfolders, and files)
%SystemRoot%\help\ acc_dis.chm, access.chm, accessib.chm, aclui.chm, aclui.hlp, adcadmin.chm, addremov.chm, ade.hlp, adprop.hlp, agt0406.hlp, agt0407.hlp, agt0409.hlp, agt040b.hlp, agt040c.hlp, agt0410.hlp, agt0413.hlp, agt0414.hlp, agt0416.hlp, agt041d.hlp, agt0816.hlp, agt0c0a.hlp, apps.chm, asr.chm, atm.chm, audiocdc.hlp, bnts.dll, bootcons.chm, brep.chm, brep.hlp, brief.chm, camera.chm, certmgr.chm, certmgr.hlp, chnscsvr.hlp, ciadmin.htm, ciquery.htm, clipbrd.chm, clipbrd.hlp, cmconcepts.chm, colormgt.chm, common.chm, compmgmt.chm, compstui.hlp, concepts.chm, cpanel.chm, cpanel.chq, cscui.hlp, datetime.chm, dcntart.chm, dcomcnfg.chm, dcomcnfg.hlp, ddeshare.chm, ddeshare.hlp, defrag.chm, defrag.hlp, devmgr.chm, devmgr.hlp, diagboot.chm, dijoy.hlp, diskmgmt.chm, diskmgmt.hlp, display.chm, display.hlp, drivprop.chm, drvvfp.chm, drwtsn32.chm, drwtsn32.hlp, dsclient.hlp, dskquoui.chm, dskquoui.hlp, dvdplay.chm,	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control

dvdplay.hlp, dxdiag.chm, els.chm, els.hlp, encrypt.chm, errors.chm, eudcedit.chm, eudcedit.hlp, evntwin.hlp, fax.chm, fax.hlp, faxcover.chm, faxmgmt.chm, faxqueue.chm, fde.hlp, file_srv.chm, file_srv.hlp, filemgmt.hlp, find.chm, folderop.chm, fonts.chm, fonts.hlp, getstart.chm, glossary.chm, glossary.hlp, gpedit.chm, gpedit.hlp, gptext.hlp, halftone.hlp, hardware.chm, hardware.hlp, howto.chm, ident.hlp, ieakmmc.chm, iesupp.chm, iewebhlp.chm, iexplore.chm, iexplore.hlp, iis.chm, iismmc.chm, imghelp.hlp, imgmgt.chm, imgmgt.hlp, imgtasks.chm, imgview.chm, infrared.chm, infrared.hlp, intellimirror.chm, ipsecconcepts.chm, ipsecsnp.chm, ipsecsnp.hlp, is.chm, isconcepts.chm, ixhelp.hlp, ixqlang.htm, javaperm.hlp, javasec.hlp, joy.chm, keyb.chm, lang.chm, license.chm, localsec.chm, localsec.hlp, magnify.chm, magnify.hlp, mail.chm, mfcuix.hlp, mls_trb.chm, mmc.chm, mmc_dlg.hlp, mmdrv.hlp, mobsync.chm, mobsync.hlp, mode.chm, modem.hlp, mouse.chm, mouse.hlp, mpconcepts.chm, mplayer2.cnt, mplayer2.hlp, mpnetwrk.hlp, mqsnap.hlp, msdasc.chm, msinfo32.chm, msinfo32.hlp, msmq.chm, msmqconcepts.chm, msmqcpl.chm, msmqcpl.hlp, msnauth.cnt, msnauth.hlp, msorcl32.chm, mstask.chm, netcfg.chm, netcfg.hlp, newfeat1.chm, newfeat1.hlp, newfeat2.chm, newfeat2.hlp, newfeat3.chm, newfeat3.hlp,		

newfeat4.chm, newfeat4.hlp, newfeat5.chm, newfeat5.hlp, nocontnt.cnt, nofts.chm, notepad.chm, notepad.hlp, ntart.chm, ntbackup.chm, ntbackup.hlp, ntchowto.chm, ntcmds.chm, ntdef.chm, nthelp.chm, ntshared.chm, ntshrui.chm, ntshrui.hlp, nwdoc.chm, nwdoc.hlp, objsel.hlp, odbcinst.chm, odbcjet.chm, offlinefolders.chm, omc.chm, osk.chm, osk.hlp, printfnd.chm, printing.chm, proccon.chm, progman.cnt, progman.hlp, pwrmn.chm, pwrmn.hlp, rasadmin.cnt, rasadmin.hlp, ratings.chm, ratings.cnt, ratings.hlp, reader.chm, reader.hlp, recycle.chm, regedit.chm, regedit.hlp, regedt32.chm, regedt32.hlp, regopt.chm, remote.chm, rsm.chm, rsm.hlp, rsmconcepts.chm, sc.chm, scarddlg.hlp, sce.chm, sceconcepts.chm, scenario.chm, scm.chm, scmconcepts.chm, secauth.hlp, secedit.chm, secsetconcepts.chm, secsettings.chm, sendcmsg.chm, sfmmgr.hlp, shell.hlp, signin.hlp, sigverif.hlp, smlogcfg.chm, snmpconcepts.chm, snmpsnap.hlp, soundrec.chm, soundrec.hlp, sounds.chm, spconcepts.chm, splash.chm, supp_ed.chm, sys_srv.chm, sys_srv.hlp, sysdm.chm, sysdm.hlp, sysmon.chm, sysmon.hlp, sysprop.chm, tapi.chm, tapi.hlp, taskmgr.chm, taskmgr.hlp, tcpip.chm, tcpmon.hlp, telnet.chm, telnet.hlp, trouble.chm, tshoot.chm, tshoot.chq, tshoot.hlp, tshoot.ocx, update.cnt, upwizun.chm, usercpl.chm, users.hlp,		

utilmgr.chm, utilmgr.hlp, webfoldr.chm, webhelp.chm, whatsnew.chm, where_98.chm, where_nw.chm, win_dos.chm, windows.chm, windows.chq, windows.cnt, windows.hlp, winhlp32.cnt, winhlp32.hlp, wininstl.chm, wscript.chm, wscript.hlp, wsd.chm, wsecedit.hlp		
%SystemRoot%\hh.exe	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control

%SystemRoot%\inf\ 1394.inf, accessor.inf, acpi.inf, adm_mult.inf, adm_port.inf, agtinst.inf, amovie.inf, apcompat.inf, apps.inf, asynceqn.inf, atividin.inf, avmisdn.inf, axant5.inf, banshee.inf, battery.inf, biosinfo.inf, ccdecode.inf, cdrom.inf, certclas.inf, cfmcanon.inf, cfmmustk.inf, cfmricoh.inf, chips5.inf, communic.inf, comnt5.inf, conf.adm, corelist.inf, ctlegacy.inf, ctmaport.inf, ctmvport.inf, defltsv.inf, defltwk.inf, dfrg.inf, dgaport.inf, dgasync.inf, didiva.inf, digiisdn.inf, digirp.inf, digirprt.inf, disk.inf, dispdet.inf, display.inf, dot4.inf, dot4prt.inf, drvindex.inf, dshowext.inf, dtcnt5.inf, dvd.inf, eclandd.inf, ecwandd.inf, eiccard.inf, eicpcard.inf, eicvirta.inf, eqnport.inf, faxsetup.inf, fdc.inf, fjtscan.inf, flash.inf, flpydisk.inf, font.inf, fp40ext.inf, fsvga.inf, fsvgaadd.inf, fsvgadel.inf, gameport.inf, games.inf, genprint.inf, hal.inf, hidserv.inf, hpojscan.inf, hpscan.inf, i740nt5.inf, i81xnt5.inf, ibmsync.inf, ibmvcap.inf, icminst.inf, icwnt5.inf, ie.inf, iereset.inf, iis.inf, iisdbg.inf, image.inf, imagevue.inf, ims.inf, inetcorp.adm, inetres.adm, inetset.adm, input.inf, intl.inf, irdaalif.inf, irdasmc.inf, irnsc.inf, irtos4mo.inf, irtos4mu.inf, kdk2x0.inf, keyboard.inf, kodak.inf, ks.inf, kscaptur.inf, ksfilter.inf, layout.inf, legcydrv.inf, logiscan.inf, lvcam.inf, lvcomp.inf, lvsound.inf, lwngmadi.inf, lwusbhid.inf, machine.inf,	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control

mchgr.inf, mdac.inf, mdm3cisa.inf, mdm3com.inf, mdm3cpcm.inf, mdm3cusb.inf, mdm3x.inf, mdm656n5.inf, mdmaceex.inf, mdmadc.inf, mdmairte.inf, mdmar1.inf, mdmarch.inf, mdmarcht.inf, mdmarn.inf, mdmati.inf, mdmatt.inf, mdmaus.inf, mdmblatz.inf, mdmboca.inf, mdmbsb.inf, mdmbsch.inf, mdmcm28.inf, mdmcmcm.inf, mdmcodex.inf, mdmcom1.inf, mdmcommu.inf, mdmcpi.inf, mdmcpq.inf, mdmcpq2.inf, mdmcpv.inf, mdmcrtix.inf, mdmctm1.inf, mdmdefd.inf, mdmdgitn.inf, mdmdigi.inf, mdmdisco.inf, mdmdsi.inf, mdmdyna.inf, mdmeiger.inf, mdmelink.inf, mdmelsa.inf, mdmeric.inf, mdmeric2.inf, mdmess.inf, mdmetech.inf, mdmexp.inf, mdmeyp.inf, mdmgatew.inf, mdmgcs.inf, mdmgen.inf, mdmgl001.inf, mdmgl002.inf, mdmgl003.inf, mdmgl004.inf, mdmgl005.inf, mdmgl006.inf, mdmgl007.inf, mdmgl008.inf, mdmgl009.inf, mdmgl010.inf, mdmgsm.inf, mdmgv.inf, mdmgvc.inf, mdmhaeu.inf, mdmhaeus.inf, mdmhandy.inf, mdmhay2.inf, mdmhayes.inf, mdminfot.inf, mdminsys.inf, mdmintel.inf, mdmintpc.inf, mdmisdn.inf, mdmitex.inf, mdmke.inf, mdmkortx.inf, mdmlasat.inf, mdmlasno.inf, mdmlce.inf, mdmlngsh.inf, mdmlt3.inf, mdmltleo.inf, mdmmart.inf, mdmmcom.inf, mdmmetri.inf, mdmmhrtz.inf, mdmmhza.inf, mdmmhzel.inf, mdmmhzk1.inf, mdmmix.inf, mdmmod.inf, mdmmoto.inf,		

mdmmoto1.inf, mdmmotou.inf, mdmmtd.inf, mdmmts.inf, mdmmulog.inf, mdmneuhs.inf, mdmnokia.inf, mdmnokno.inf, mdmnova.inf, mdmnovfx.inf, mdmolic.inf, mdmoptn.inf, mdmosi.inf, mdmpace.inf, mdmpbit.inf, mdmpenr.inf, mdmphils.inf, mdmpn1.inf, mdmpnb.inf, mdmpp.inf, mdmprodm.inf, mdmpsion.inf, mdmracal.inf, mdmrisa.inf, mdmrock.inf, mdmrock2.inf, mdmrock3.inf, mdmrock4.inf, mdmrock5.inf, mdmrpciw.inf, mdmsecdy.inf, mdmsetup.inf, mdmsier.inf, mdmsimpl.inf, mdmsmart.inf, mdmsnit1.inf, mdmsnitn.inf, mdmsonix.inf, mdmspq28.inf, mdmsrt.inf, mdmsupr3.inf, mdmsupra.inf, mdmsuprv.inf, mdmtaicm.inf, mdmtdk.inf, mdmtelbt.inf, mdmtelin.inf, mdmtelnk.inf, mdmtexas.inf, mdmtger.inf, mdmti.inf, mdmtosh.inf, mdmtripl.inf, mdmtron.inf, mdmucom.inf, mdmusrcr.inf, mdmusrf.inf, mdmusrg.inf, mdmusrk1.inf, mdmusrsp.inf, mdmusrwp.inf, mdmvdot.inf, mdmvict.inf, mdmvv.inf, mdmwell.inf, mdmwhql0.inf, mdmwoer.inf, mdmx5560.inf, mdmyorik.inf, mdmzoom.inf, mdmzyp.inf, mdmzyxel.inf, mdmzyxld.inf, mdmzyxlg.inf, memcard.inf, mf.inf, mf3c562.inf, mfc21.inf, mfc550.inf, mfcem28.inf, mfcem33.inf, mfcem56.inf, mff56n5.inf, mfgenb.inf, mfle56.inf, mfm16b.inf, mfmhzn5.inf, mfoce2m.inf, mfoct35.inf, mfsocket.inf, mfsupra.inf, mfx56nf.inf, mga64.inf,		

mgsync.inf, mgwan5.inf, minioc.inf, mmopt.inf, modemcsa.inf, monitor.inf, monitor2.inf, monitor3.inf, monitor4.inf, monitor5.inf, monitor6.inf, monitor7.inf, monitor8.inf, monitor9.inf, mpcodecs.inf, mplayer2.inf, mpsstln.inf, mqsysoc.inf, msdv.inf, mshdc.inf, msinfo32.inf, msmouse.inf, msmqocm.inf, msmscsi.inf, msmusb.inf, msnetmtg.inf, msoe50.inf, msports.inf, mstask.inf, mstts.inf, multimed.inf, multiprt.inf, mwavmdm1.inf, mwmbatam.inf, mwremove.inf, mwtpdsp.inf, n3bridge.inf, neo20xx.inf, net08a.inf, net21x4.inf, net3c562.inf, net3c589.inf, net5515n.inf, net557.inf, net575nt.inf, net656n5.inf, net713.inf, netacc.inf, netalt.inf, netambcb.inf, netambi.inf, netamd.inf, netamdhl.inf, netana.inf, netasp2k.inf, netatlk.inf, netauni.inf, netbrzw.inf, netc20.inf, netc21.inf, netc550.inf, netcb325.inf, netcbe.inf, netce2.inf, netce3.inf, netcem28.inf, netcem33.inf, netcem56.inf, netcis.inf, netcpqg.inf, netcpqi.inf, netcpqmt.inf, netctmrk.inf, netctmva.inf, netdefxa.inf, netdgdxb.inf, netdgisa.inf, netdgsxb.inf, netdlc.inf, netdlh5x.inf, netdstar.inf, nete100.inf, nete1000.inf, nete100i.inf, nete100s.inf, netejet.inf, netejxmp.inf, netel515.inf, netel574.inf, netel59x.inf, netel5x9.inf, netel90x.inf, netel980.inf, netenet.inf, neteni25.inf, netepc.inf, netepicn.inf, netepro.inf, netet32.inf, netex10.inf,		

netf56n5.inf, netfjvi.inf, netfjvj.inf, netflex.inf, netfore.inf, netforeh.inf, netgena.inf, netgenb.inf, netgpc.inf, nethppci.inf, netias.inf, netibm.inf, netibm2.inf, netibmge.inf, netibmn5.inf, netiprip.inf, netirda.inf, netirsir.inf, netjat5.inf, netlanem.inf, netlanep.inf, netle56.inf, netloop.inf, netlpd.inf, netm16a.inf, netm16b.inf, netm32a.inf, netmadge.inf, netmhzn5.inf, netmscli.inf, netnb.inf, netnbf.inf, netnf3.inf, netngr.inf, netnm.inf, netnovel.inf, netnwcli.inf, netnwlnk.inf, netoc.inf, netoca1p.inf, netoca2p.inf, netoce2m.inf, netoce3m.inf, netoce4m.inf, netoce55.inf, netoct35.inf, netoct4p.inf, netoemdh.inf, netosi5.inf, netpc100.inf, netpnic.inf, netpsa.inf, netpschd.inf, netpwr2.inf, netrasa.inf, netrass.inf, netrast.inf, netrlw2k.inf, netrnse.inf, netrsvp.inf, netrtpnt.inf, netrtsnt.inf, netrwan.inf, netsap.inf, netserv.inf, netsk_fp.inf, netsk98.inf, netslant.inf, netsmc.inf, netsnip.inf, netsnmp.inf, netstrm.inf, netsym.inf, nettb155.inf, nettcpip.inf, nettiger.inf, nettpro.inf, nettpsmp.inf, nettsbnt.inf, netupgrd.inf, netvt86.inf, netw840.inf, netw926.inf, netw940.inf, netwlan2.inf, netwv48.inf, netx500.inf, netx56n5.inf, netxcpq.inf, nt5java.inf, ntapm.inf, ntprint.inf, nv3.inf, nv4.inf, optional.inf, pcmcia.inf, perm2.inf, phil1vid.inf, pinball.inf, ppa.inf, ppa3.inf, printupg.inf, proccon.inf, rca.inf, rmvv1.inf, rmvv2.inf, rsm.inf, rstorage.inf, s3sav3d.inf, s3sav4.inf, s3trio3d.inf, sbp2.inf, sceregvl.inf, scsi.inf, scsidev.inf, setupqry.inf,		

sgiu.inf, shell.inf, sis300.inf, sis6306.inf, sisv6326.inf, smartcrd.inf, spchapi.inf, spx.inf, spxports.inf, stalport.inf, sti.inf, stillcam.inf, svcpack.inf, swnt.inf, sysoc.inf, syssetup.inf, system.adm, tape.inf, tgiu.inf, trid3d.inf, tridkb.inf, tsbvcap.inf, tshoot.inf, umax.inf, unknown.inf, unregmp2.exe, usb.inf, usbprint.inf, usbstor.inf, usermig.inf, volume.inf, voodoo3.inf, wab50.inf, wanmgfr.inf, wanmgs.inf, wave.inf, wbemnt5.inf, wbfirdma.inf, wbfirdma.sys, wdma_adi.inf, wdma_aur.inf, wdma_ava.inf, wdma_azt.inf, wdma_csc.inf, wdma_csf.inf, wdma_ctl.inf, wdma_ens.inf, wdma_es2.inf, wdma_ess.inf, wdma_int.inf, wdma_ne2.inf, wdma_neo.inf, wdma_usb.inf, wdma_wss.inf, wdma_ym2.inf, wdma_ymh.inf, wdma10k1.inf, wdmaudio.inf, wdmjoy.inf, wkstamig.inf, wmp.adm, wordpad.inf		
%SystemRoot%\java	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%Systemroot%\lanma256.bmp		**Users:** Read and Execute **Power Users:** Read and Execute

		Administrators: Full Control **SYSTEM:** Full Control
%Systemroot%\lanmannt.bmp		**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\media\ ir_begin.wav, ir_end.wav, ir_inter.wav, ringin.wav, ringout.wav, start.wav, the microsoft sound.wav, windows logoff sound.wav, windows logon sound.wav	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\msagent	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemRoot%\msdfmap.ini	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\offline pages	Inherit from parent	Inherit from parent
%Systemroot%\poledit.exe		**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control

		SYSTEM: Full Control
%SystemRoot%\profiles	Inherit from parent	Inherit from parent
%SystemRoot%\regedit.exe	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\registration	Inherit from parent	Inherit from parent
%SystemRoot%\repair	**Users:** Read and Execute (folder and subfolders) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder and subfolders) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemRoot%\security	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemRoot%\speech	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder)

	Administrators: Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemRoot%\system.ini	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\system\setup.inf	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\system\stdole.tlb	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemDirectory%	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files) **Authenticated Users:** Read and Execute	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files) **Authenticated Users:** Read and Execute

%SystemDirectory%\ ~clbcatq.dll, 12520437.cpx, 12520850.cpx, aaaamon.dll, acelpdec.ax, acledit.dll, aclui.dll, acsetupc.dll, acsmib.dll, activeds.dll, activeds.tlb, actmovie.exe, actxprxy.dll, admparse.dll, adptif.dll, adsldp.dll, adsldpc.dll, adsmsext.dll, adsnds.dll, adsnt.dll, adsnw.dll, advapi32.dll, advpack.dll, alrsvc.dll, amstream.dll, ansi.sys, apcups.dll, append.exe, appmgmts.dll, appmgr.dll, appwiz.cpl, arp.exe, asctrls.ocx, asfsipc.dll, asycfilt.dll, at.exe, atkctrs.dll, atl.dll, atmadm.exe, atmfd.dll, atmlib.dll, attrib.exe, autochk.exe, autoconv.exe, autofmt.exe, autolfn.exe, avicap.dll, avicap32.dll, avifil32.dll, avifile.dll, basenote.cov, basesrv.dll, batmeter.dll, bios1.rom, bios4.rom, bootok.exe, bootvid.dll, bootvrfy.exe, br549.dll, browselc.dll, browser.dll, browseui.dll, c_037.nls, c_10000.nls, c_10079.nls, c_1026.nls, c_1250.nls, c_1251.nls, c_1252.nls, c_1253.nls, c_1254.nls, c_1255.nls, c_1256.nls, c_1257.nls, c_1258.nls, c_20261.nls, c_20866.nls, c_20905.nls, c_21866.nls, c_28591.nls, c_28592.nls, c_28593.nls, c_28598.nls, c_28605.nls, c_437.nls, c_500.nls, c_775.nls, c_850.nls, c_860.nls, c_861.nls, c_863.nls, c_865.nls, c_874.nls, c_932.nls, c_936.nls, c_949.nls, c_950.nls, cabinet.dll, cabview.dll, cacls.exe, capesnpn.dll, cards.dll, catroot, ccfgnt.dll, cdfview.dll, cdm.dll, cdonts.dll, cdosys.dll, certcli.dll, certmgr.dll, certmgr.msc, cfgmgr32.dll, channel screen	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control **Authenticated Users:** Read and Execute	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control **Authenticated Users:** Read and Execute

saver.scr, chcp.com, chkdsk.exe, chkntfs.exe, ciadmin.dll, ciadv.msc, cic.dll, cidaemon.exe, ciodm.dll, cipher.exe, cisvc.exe, ckcnv.exe, clb.dll, cleanmgr.exe, cliconf.hlp, cliconfg.dll, cliconfg.exe, clipsrv.exe, clspack.exe, clusapi.dll, cluster.exe, cmcfg32.dll, cmd.exe, cmdial32.dll, cmdl32.exe, cmmgr32.exe, cmmgr32.hlp, cmmon32.exe, cmnquery.dll, cmpbk32.dll, cmprops.dll, cmstp.exe, cmutil.dll, cnbjmon.dll, cnetcfg.dll, cnvfat.dll, comcat.dll, comctl32.dll, comdlg32.dll, comm.drv, command.com, commdlg.dll, comp.exe, compact.exe, compmgmt.msc, compobj.dll, compstui.dll, config, confmsp.dll, conime.exe, console.dll, control.exe, convert.exe, corpol.dll, country.sys, crtdll.dll, crypt32.dll, cryptdlg.dll, cryptdll.dll, cryptext.dll, cryptnet.dll, cryptsvc.dll, cryptui.dll, cscdll.dll, cscript.exe, cscui.dll, csrsrv.dll, csrss.exe, ctl3d32.dll, ctl3dv2.dll, ctype.nls, d3dim.dll, d3dim700.dll, d3dpmesh.dll, d3dramp.dll, d3dref.dll, d3drm.dll, d3dxof.dll, danim.dll, dataclen.dll, datime.dll, daxctle.ocx, dbghelp.dll, dbmsadsn.dll, dbmsrpcn.dll, dbmssocn.dll, dbmsspxn.dll, dbmsvinn.dll, dbnmpntw.dll, dciman32.dll, dcomcnfg.exe, ddeml.dll, ddeshare.exe, ddmprxy.exe, ddraw.dll, ddrawex.dll, debug.exe, desk.cpl, deskadp.dll, deskmon.dll, deskperf.dll, devenum.dll, devmgmt.msc, devmgr.dll, dfrg.msc, dfrgfat.exe, dfrgntfs.exe, dfrgres.dll, dfrgsnap.dll, dfrgui.dll, dfsshlex.dll, dhcp, dhcpcsvc.dll,		

dhcpmon.dll, dhcpsapi.dll, diantz.exe, digest.dll, dinput.dll, diskcomp.com, diskcopy.com, diskcopy.dll, diskmgmt.msc, diskperf.exe, dispex.dll, dlcapi.dll, dllcache, dllhost.exe, dllhst3g.exe, dmadmin.exe, dmband.dll, dmcompos.dll, dmconfig.dll, dmdlgs.dll, dmdskmgr.dll, dmdskres.dll, dmime.dll, dmintf.dll, dmloader.dll, dmocx.dll, dmremote.exe, dmserver.dll, dmstyle.dll, dmsynth.dll, dmusic.dll, dmutil.dll, dmview.ocx, dnsapi.dll, dnsrslvr.dll, docprop.dll, docprop2.dll, doshelp.hlp, doskey.exe, dosx.exe, dplay.dll, dplaysvr.exe, dplayx.dll, dpmodemx.dll, dpserial.dll, dpwsock.dll, dpwsockx.dll, drivers, drmclien.dll, drmstor.dll, drwatson.exe, drwtsn32.exe, ds16gt.dll, ds32gt.dll, dsauth.dll, dsctl.dll, dsfolder.dll, dskquota.dll, dskquoui.dll, dsound.dll, dsound.vxd, dsound3d.dll, dsprop.dll, dsquery.dll, dssbase.dll, dssec.dat, dssec.dll, dsuiext.dll, dvdplay.exe, dx3j.dll, dx7vb.dll, dxdiag.exe, dxmasf.dll, dxmrtp.dll, dxtmsft.dll, dxtmsft3.dll, dxtrans.dll, edit.com, edit.hlp, edlin.exe, efsadu.dll, ega.cpi, els.dll, es.dll, esent.dll, esentprf.dll, esentprf.hxx, esentprf.ini, esentutl.exe, eudcedit.exe, eula.txt, eventlog.dll, eventvwr.exe, eventvwr.msc, exe2bin.exe, expand.exe, expsrv.dll, extrac32.exe, fastopen.exe, fax.cpl, faxadmin.dll, faxcom.dll, faxcount.h, faxcover.exe, faxdrv.dll, faxevent.dll, faxext32.dll, faxmapi.dll, faxocm.dll, faxperf.dll, faxperf.ini, faxqueue.exe, faxroute.dll,		

faxsend.exe, faxserv.msc, faxshell.dll, faxsvc.exe, faxt30.dll, faxtiff.dll, faxui.dll, faxxp32.dll, fc.exe, fde.dll, fdeploy.dll, feclient.dll, filemgmt.dll, find.exe, findstr.exe, finger.exe, fixmapi.exe, fmifs.dll, fontext.dll, fontsub.dll, fontview.exe, forcedos.exe, format.com, fsmgmt.msc, ftp.exe, ftsrch.dll, g711codc.ax, g723codc.ax, gcdef.dll, gdi.exe, gdi32.dll, getstart.gif, glmf32.dll, glu32.dll, gpedit.dll, gpedit.msc, gpkcsp.dll, gpkrsrc.dll, gptext.dll, graftabl.com, graphics.com, graphics.pro, grpconv.exe, h261_32.ax, h263_32.ax, h323.tsp, h323msp.dll, hardware.inf, hdwwiz.cpl, help.exe, hhctrl.ocx, hhsetup.dll, hid.dll, himem.sys, hlink.dll, homepage.inf, hostname.exe, hotplug.dll, htui.dll, iac25_32.ax, ias, ias.msc, iasacct.dll, iasads.dll, iashlpr.dll, iasnap.dll, iasperf.dll, iasperf.h, iasperf.ini, iaspipe.dll, iaspolcy.dll, iasrad.dll, iasrecst.dll, iassam.dll, iassdo.dll, iassvcs.dll, iasuserr.dll, iccvid.dll, icm32.dll, icmp.dll, icmui.dll, idq.dll, idwlog.exe, ie4uinit.exe, ieakeng.dll, ieaksie.dll, ieakui.dll, iedkcs32.dll, iepeers.dll, iernonce.dll, iesetup.dll, ieshwiz.exe, ieuinit.inf, iexpress.exe, ifmon.dll, ifsutil.dll, igmpagnt.dll, iissuba.dll, imaadp32.acm, imagehlp.dll, imeshare.dll, imgutil.dll, imm32.dll, indicdll.dll, inetcpl.cpl, inetcplc.dll, inetmib1.dll, inetpp.dll, infosoft.dll, initpki.dll, inseng.dll, instcat.sql, instcm.inf, internat.exe, intl.cpl, iologmsg.dll, ipconf.tsp, ipconfig.exe, iphlpapi.dll, ipmontr.dll, ipnathlp.dll, ippromon.dll, iprop.dll, iprtprio.dll,		

iprtrmgr.dll, ipsecmon.exe, ipsecsnp.dll, ipxmontr.dll, ipxpromn.dll, ipxrip.dll, ipxroute.exe, ipxrtmgr.dll, ipxsap.dll, ipxwan.dll, ir32_32.dll, ir41_32.ax, ir41_qc.dll, ir41_qcx.dll, ir50_32.dll, ir50_qc.dll, ir50_qcx.dll, irclass.dll, irftp.exe, irmon.dll, irprops.cpl, itircl.dll, itss.dll, ivfsrc.ax, ixsso.dll, javacypt.dll, javaprxy.dll, javart.dll, jdbgmgr.exe, jet500.dll, jit.dll, jobexec.dll, joy.cpl, jscript.dll, jsproxy.dll, jview.exe, kb16.com, kbdbe.dll, kbdbene.dll, kbdbr.dll, kbdca.dll, kbdcan.dll, kbdda.dll, kbddv.dll, kbdes.dll, kbdfc.dll, kbdfi.dll, kbdfo.dll, kbdfr.dll, kbdgae.dll, kbdgr.dll, kbdgr1.dll, kbdic.dll, kbdir.dll, kbdit.dll, kbdit142.dll, kbdla.dll, kbdmac.dll, kbdne.dll, kbdno.dll, kbdpo.dll, kbdsf.dll, kbdsg.dll, kbdsp.dll, kbdsw.dll, kbduk.dll, kbdus.dll, kbdusl.dll, kbdusr.dll, kbdusx.dll, kerberos.dll, kernel32.dll, key01.sys, keyboard.drv, keyboard.sys, kmddsp.tsp, krnl386.exe, ksqmf.ax, l_except.nls, l_intl.nls, l3codecx.ax, label.exe, lanman.drv, legacy.inf, licmgr10.dll, lights.exe, linkinfo.dll, lmhsvc.dll, lmrt.dll, lnkstub.exe, loadfix.com, loadperf.dll, locale.nls, localsec.dll, localspl.dll, localui.dll, locator.exe, lodctr.exe, logdrive.dll, loghours.dll, login.cmd, logon.scr, lpk.dll, lpq.exe, lpr.exe, lprhelp.dll, lprmonui.dll, lsasrv.dll, lsass.exe, lusrmgr.msc, lz32.dll, lzexpand.dll, mag_hook.dll, magnify.exe, main.cpl, makecab.exe, mapistub.dll, mbslgn32.dll, mcastmib.dll, mcd32.dll, mcdsrv32.dll, mciavi.drv, mciavi32.dll, mcicda.dll,		

mciole16.dll, mciole32.dll, mciqtz32.dll, mciseq.dll, mciseq.drv, mciwave.dll, mciwave.drv, mdhcp.dll, mdminst.dll, mem.exe, mf3216.dll, mfc40.dll, mfc40u.dll, mfc42.dll, mfc42u.dll, mfcsubs.dll, mgmtapi.dll, mib.bin, midimap.dll, migisol.exe, migpwd.exe, mimefilt.dll, mlang.dat, mlang.dll, mll_hp.dll, mll_mtf.dll, mll_qic.dll, mmc.exe, mmcndmgr.dll, mmcshext.dll, mmdet.dll, mmdriver.inf, mmdrv.dll, mmefxe.ocx, mmfutil.dll, mmsys.cpl, mmsystem.dll, mmtask.tsk, mmutilse.dll, mobsync.dll, mobsync.exe, mode.com, modemui.dll, modex.dll, more.com, moricons.dll, mountvol.exe, mouse.drv, mpg2splt.ax, mpg4ds32.ax, mpnotify.exe, mpr.dll, mprapi.dll, mprddm.dll, mprdim.dll, mprmsg.dll, mprui.dll, mrinfo.exe, msacm.dll, msacm32.dll, msacm32.drv, msadds32.ax, msadp32.acm, msafd.dll, msapsspc.dll, msasn1.dll, msaudite.dll, msawt.dll, mscat32.dll, mscdexnt.exe, msclus.dll, mscms.dll, mscpxl32.dll, msdart32.dll, msdatsrc.tlb, msdxm.ocx, msdxmlc.dll, msencode.dll, msexch40.dll, msexcl40.dll, msfaxmon.dll, msg711.acm, msgina.dll, msgsm32.acm, msgsvc.dll, mshta.exe, mshtml.dll, mshtml.tlb, mshtmled.dll, mshtmler.dll, msi.dll, msident.dll, msidle.dll, msidlpm.dll, msidntld.dll, msidpe.dll, msieftp.dll, msiexec.exe, msihnd.dll, msimg32.dll, msimsg.dll, msjava.dll,		

msjdbc10.dll, msjet40.dll, msjetoledb40.dll, msjint40.dll, msjter40.dll, msjtes40.dll, msls31.dll, msltus40.dll, msnsspc.dll, msobjs.dll, msorcl32.dll, mspatcha.dll, mspbde40.dll, msports.dll, msprivs.dll, msr2c.dll, msr2cenu.dll, msrating.dll, msrclr40.dll, msrd2x40.dll, msrd3x40.dll, msrecr40.dll, msrepl40.dll, msrle32.dll, msscript.ocx, mssign32.dll, mssip32.dll, msswch.dll, msswchx.exe, mstext40.dll, msv1_0.dll, msvbvm50.dll, msvbvm60.dll, msvcirt.dll, msvcp50.dll, msvcrt.dll, msvcrt20.dll, msvcrt40.dll, msvfw32.dll, msvidc32.dll, msvideo.dll, msw3prt.dll, mswdat10.dll, mswsock.dll, mswstr10.dll, msxbde40.dll, msxml.dll, mtstocom.exe, mtxclu.dll, mui, mycomput.dll, mydocs.dll, narrator.exe, narrhook.dll, nbtstat.exe, ncpa.cpl, nddeapi.dll, nddeapir.exe, nddenb32.dll, ndptsp.tsp, net.exe, net.hlp, net1.exe, netapi.dll, netapi32.dll, netcfgx.dll, netdde.exe, netdet.dll, netdtect.dll, netevent.dll, neth.dll, netid.dll, netlogon.dll, netman.dll, netmsg.dll, netplwiz.dll, netrap.dll, netsh.exe, netshell.dll, netstat.exe, netui0.dll, netui1.dll, netui2.dll, netware.drv, newdev.dll, nlhtml.dll, nlsfunc.exe, nmctrs.h, nmctrs.ini, nmperf.dll, noise.dat, noise.deu, noise.eng, noise.enu, noise.esn, noise.fra, noise.ita, noise.nld, noise.sve, notepad.exe, npptools.dll, nslookup.exe, nt.fnt, nt2.fnt, ntbackup.exe, ntdll.dll, ntdos.sys, ntdos404.sys, ntdos411.sys,		

ntdos412.sys, ntdos804.sys, ntdsa.dll, ntdsapi.dll, ntdsatq.dll, ntdsbcli.dll, ntdsbsrv.dll, ntdsetup.dll, ntdskcc.dll, ntdsutil.exe, ntdsxds.dll, ntimage.gif, ntio.sys, ntio404.sys, ntio411.sys, ntio412.sys, ntio804.sys, ntlanman.dll, ntlanui.dll, ntlanui2.dll, ntlsapi.dll, ntmarta.dll, ntmsapi.dll, ntmsdba.dll, ntmsevt.dll, ntmsmgr.dll, ntmsmgr.msc, ntmsoprq.msc, ntmssvc.dll, ntprint.dll, ntsd.exe, ntsdexts.dll, ntshrui.dll, ntvdm.exe, ntvdmd.dll, nw16.exe, nwapi16.dll, nwapi32.dll, nwc.cpl, nwcfg.dll, nwevent.dll, nwprovau.dll, nwscript.exe, nwwks.dll, oakley.dll, objsel.dll, occache.dll, ocmanage.dll, odbc16gt.dll, odbc32.dll, odbc32gt.dll, odbcad32.exe, odbcbcp.dll, odbcconf.dll, odbcconf.exe, odbcconf.rsp, odbccp32.cpl, odbccp32.dll, odbccr32.dll, odbccu32.dll, odbcint.dll, odbcji32.dll, odbcjt32.dll, odbctrac.dll, oddbse32.dll, odexl32.dll, odfox32.dll, odpdx32.dll, odtext32.dll, offfilt.dll, ole2.dll, ole2disp.dll, ole2nls.dll, ole32.dll, oleacc.dll, oleaccrc.dll, oleaut32.dll, olecli.dll, olecli32.dll, olecnv32.dll, oledlg.dll, oleprn.dll, olepro32.dll, olesvr.dll, olesvr32.dll, olethk32.dll, opengl32.dll, os2.exe, os2\dll\doscalls.dll, os2\dll\netapi.dll, os2\oso001.009, os2srv.exe, os2ss.exe, osk.exe, other.inf, panmap.dll, pathping.exe, pautoenr.dll, pax.exe, pcl.sep, pdh.dll, pentnt.exe, perfc009.dat, perfci.h, perfci.ini, perfctrs.dll, perfd009.dat, perfdisk.dll, perffilt.h,		

perffilt.ini, perfh009.dat, perfi009.dat, perfmon.exe, perfmon.msc, perfnet.dll, perfnw.dll, perfos.dll, perfproc.dll, perfwci.h, perfwci.ini, pidgen.dll, pifmgr.dll, ping.exe, pjlmon.dll, plugin.ocx, plustab.dll, pmspl.dll, pngfilt.dll, polagent.dll, polstore.dll, posix.exe, powercfg.cpl, powrprof.dll, prflbmsg.dll, print.exe, printmon.inf, printui.dll, proctexe.ocx, prodspec.ini, profmap.dll, progman.exe, proquota.exe, psapi.dll, psbase.dll, pschdcnt.h, pschdprf.dll, pschdprf.ini, pscript.sep, psnppagn.dll, pstorec.dll, psxdll.dll, psxss.exe, pubprn.vbs, qcap.dll, qcut.dll, qdv.dll, qdvd.dll, qosname.dll, quartz.dll, query.dll, rapilib.dll, ras\cis.scp, ras\pad.inf, ras\pppmenu.scp, ras\slip.scp, ras\slipmenu.scp, ras\switch.inf, rasadhlp.dll, rasadmin.exe, rasapi32.dll, rasauth.dll, rasauto.dll, rasautou.exe, raschap.dll, rasctrnm.h, rasctrs.dll, rasctrs.ini, rasdial.exe, rasdlg.dll, rasgprxy.dll, rasgtwy.dll, rasman.dll, rasmans.dll, rasmontr.dll, rasmxs.dll, rasphone.exe, rasppp.dll, rasrad.dll, rassapi.dll, rassauth.dll, rasscrpt.dll, rasser.dll, rastapi.dll, rastls.dll, rcamsp.dll, rcp.exe, recover.exe, redir.exe, regapi.dll, regedt32.exe, registry.inf, regsvc.exe, regsvr32.exe, regwiz.exe, regwizc.dll, remotesp.tsp, rend.dll, replace.exe, resutils.dll, rexec.exe, riched20.dll, riched32.dll, rnr20.dll, route.exe, routeext.dll, routemon.exe, routetab.dll, rpcns4.dll, rpcrt4.dll, rpcss.dll, rsabase.dll, rsaci.rat, rsfsaps.dll, rsh.exe, rshx32.dll, rsm.exe, rsnotify.exe, rsvp.exe, rsvp.ini,		

rsvpcnts.h, rsvpmsg.dll, rsvpperf.dll, rsvpsp.dll, rtipxmib.dll, rtm.dll, rtutils.dll, runas.exe, rundll32.exe, runonce.exe, samlib.dll, samsrv.dll, savedump.exe, scarddlg.dll, scardssp.dll, scardsvr.exe, scecli.dll, scesrv.dll, schannel.dll, sclgntfy.dll, scripto.dll, scrnsave.scr, scrobj.dll, scrrun.dll, sdpblb.dll, secedit.exe, seclogon.dll, secpol.msc, secur32.dll, security.dll, sefilshr.dll, sendcmsg.dll, sendmail.dll, sens.dll, sensapi.dll, senscfg.dll, serialui.dll, servdeps.dll, services.exe, services.msc, serwvdrv.dll, sethc.exe, setreg.exe, setup.bmp, setup.exe, setupapi.dll, setupdll.dll, setver.exe, sfc.dll, sfc.exe, sfcfiles.dll, sfmapi.dll, sfmatmsg.dll, sfmmon.dll, sfmwshat.dll, share.exe, shdoclc.dll, shdocvw.dll, shell.dll, shell32.dll, shellext, shfolder.dll, shim.dll, shimgvw.dll, shlwapi.dll, shmgrate.exe, shrpubw.exe, shscrap.dll, sigtab.dll, sigverif.exe, sisbkup.dll, skdll.dll, skeys.exe, slbcsp.dll, slbkygen.dll, slbrsrc.dll, smlogcfg.dll, smlogsvc.exe, smss.exe, snmpapi.dll, snmpsnap.dll, softpub.dll, sort.exe, sortkey.nls, sorttbls.nls, sound.drv, spcmdcon.sys, spoolss.dll, spoolsv.exe, sprestrt.exe, sqlsodbc.hlp, sqlsrv32.dll, sqlstr.dll, sqlwid.dll, sqlwoa.dll, srvsvc.dll, ss3dfo.scr, ssbezier.scr, ssflwbox.scr, ssmarque.scr, ssmaze.scr, ssmyst.scr, sspipes.scr, ssstars.scr, sstext3d.scr, stdole2.tlb, stdole32.tlb, sti.dll, sti_ci.dll, sticpl.cpl, stimon.exe, stisvc.exe, stobject.dll, storage.dll, streamci.dll, strmdll.dll, subroutn.inf, subst.exe, svchost.exe,		

svcpack.dll, syncapp.exe, synceng.dll, syncui.dll, sysdm.cpl, sysedit.exe, sysinv.dll, syskey.exe, sysmon.ocx, sysocmgr.exe, sysprint.sep, sysprtj.sep, syssetup.dll, system.drv, systray.exe, t2embed.dll, tapi.dll, tapi3.dll, tapi32.dll, tapiperf.dll, tapisrv.dll, tapiui.dll, taskman.exe, taskmgr.exe, tcmsetup.exe, tcpmib.dll, tcpmon.dll, tcpmon.ini, tcpmonui.dll, tcpsvcs.exe, tdc.ocx, telephon.cpl, telnet.exe, termcap, termmgr.dll, tftp.exe, themes.exe, thumbvw.dll, timedate.cpl, timer.drv, tlntadmn.exe, tlntsess.exe, tlntsvr.exe, tlntsvrp.dll, toolhelp.dll, tracert.exe, traffic.dll, tree.com, trkwks.dll, tsbyuv.dll, tsd32.dll, tssoft32.acm, typelib.dll, ufat.dll, ulib.dll, umandlg.dll, umdmxfrm.dll, umpnpmgr.dll, unicode.nls, unimdm.tsp, unimdmat.dll, uniplat.dll, unlodctr.exe, untfs.dll, ups.exe, ureg.dll, url.dll, urlmon.dll, usbmon.dll, user.exe, user32.dll, userenv.dll, userinit.exe, usp10.dll, utildll.dll, utilman.exe, v7vga.rom, vbajet32.dll, vbisurf.ax, vbscript.dll, vcdex.dll, vdmdbg.dll, vdmredir.dll, ver.dll, verifier.exe, version.dll, vfpodbc.dll, vga.dll, vga.drv, view channels.scf, vjoy.dll, vmhelper.dll, vwipxspx.dll, vwipxspx.exe, w32time.dll, w32tm.exe, w32topl.dll, w95upgnt.dll, wavemsp.dll, wbcache.deu, wbcache.enu, wbcache.esn, wbcache.fra, wbcache.ita, wbcache.nld, wbcache.sve, wbdbase.deu, wbdbase.enu, wbdbase.esn, wbdbase.fra, wbdbase.ita, wbdbase.nld, wbdbase.sve, wbem, wbem\mof, wdl.trm, webcheck.dll,		

webfldrs.msi, webhits.dll, webvw.dll, wextract.exe, wfwnet.drv, wifeman.dll, win.com, win32k.sys, win32spl.dll, win87em.dll, winfax.dll, winhelp.hlp, winhlp32.exe, wininet.dll, winlogon.exe, winmm.dll, winmsd.exe, winnls.dll, winoldap.mod, winrnr.dll, winscard.dll, winsmon.dll, winsock.dll, winspool.drv, winspool.exe, winsrv.dll, winsta.dll, winstrm.dll, wintrust.dll, winver.exe, wjview.exe, wkssvc.dll, wldap32.dll, wlnotify.dll, wmi.dll, wmicore.dll, wmimgmt.msc, wow32.dll, wow64.dll, wow64cpu.dll, wowdeb.exe, wowexec.exe, wowfax.dll, wowfaxui.dll, wpnpinst.exe, ws2_32.dll, ws2help.dll, wscript.exe, wsecedit.dll, wshatm.dll, wshext.dll, wshirda.dll, wshisn.dll, wshnetbs.dll, wshom.ocx, wshtcpip.dll, wsnmp32.dll, wsock32.dll, wtsapi32.dll, wupdinfo.dll, wupdmgr.exe, xactsrv.dll, xcopy.exe, xenroll.dll		
%SystemDirectory%\appmgm	Inherit from parent	Inherit from parent
%SystemDirectory%\catroot	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder,	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder,

	subfolder, and files)	subfolder, and files)
%SystemDirectory%\config	**Users:** Read and Execute (folder and subfolders) **Power Users:** Read and Execute (folder and subfolders) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder and subfolders) **Power Users:** Read and Execute (folder and subfolders) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemDirectory%\dhcp	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemDirectory%\dllcache	**Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemDirectory%\drivers	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Administrators:** Full	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Administrators:** Full

	Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemDirectory%\dtclog	Inherit from parent	Inherit from parent
%SystemDirectory%\grouppolicy	Inherit from parent	Inherit from parent
%SystemDirectory%\hal.dll	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemDirectory%\ias	**Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemDirectory%\mui	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemDirectory%\ntmsdata	Inherit from parent	Inherit from parent
%SystemDirectory%\ntoskrnl.exe	**Users:** Read and Execute **Power Users:** Read and Execute	**Users:** Read and Execute **Power Users:** Read and Execute

	Administrators: Full Control **SYSTEM:** Full Control	**Administrators:** Full Control **SYSTEM:** Full Control
%SystemDirectory%\os2\dll\ doscalls.dll	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemDirectory%\os2\dll\ netapi.dll	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemDirectory%\os2\ oso001.009	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemDirectory%\ras cis.scp, pad.inf, pppmenu.scp, slip.scp, slipmenu.scp, switch.inf	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemDirectory%\reinstallbackups	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files) ****1	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemDirectory%\repl	**Users:** Read and Execute (folder, subfolders, and	**Users:** Read and Execute (folder, subfolders, and

	files) **Power Users:** Read and Execute (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files) ****1	files) **Power Users:** Read and Execute (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemDirectory%\repl\ export	**Replicator:** Modify (folder, subfolders, and files)	**Replicator:** Modify (folder, subfolders, and files)
%SystemDirectory%\repl\ import	**Replicator:** Modify (folder, subfolders, and files)	**Replicator:** Modify (folder, subfolders, and files)
%SystemDirectory%\setup	Inherit from parent	Inherit from parent
%SystemDirectory%\shellext	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemDirectory%\spool\ printers	**Users:** Read and Execute (folder and subfolder) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control	**Users:** Read and Execute (folder and subfolder) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control

	(folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	(folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemDirectory%\wbem	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemDirectory%\wbem\ mof	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemRoot%\tasks	Inherit from parent	Inherit from parent
%SystemRoot%\temp	**Users:** Traverse/execute, Create files, and Create folders (folder and subfolders) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full	**Users:** Traverse/execute, Create files, and Create folders (folder and subfolders) **Power Users:** Modify (folder, subfolders, and files) **Administrators:** Full

	Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemRoot%\twain.dll	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\twain_32	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemRoot%\twain_32.dll	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:**

		Full Control (folder, subfolder, and files)
%SystemRoot%\twunk_16.exe	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\twunk_32.exe	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\upwizun.exe	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\vmmreg32.dll	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\web	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)	**Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Read and Execute (folder, subfolders, and files) **Power Users:** Modify (folder sad subfolder) **Administrators:** Full Control (folder, subfolder, and files) **SYSTEM:** Full Control (folder, subfolder, and files) **CREATOR OWNER:** Full Control (folder, subfolder, and files)
%SystemRoot%\welcome.exe	**Users:** Read and Execute **Power Users:** Read and Execute	

	Administrators: Full Control **SYSTEM:** Full Control	
%SystemRoot%\welcome.ini	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	
%SystemRoot%\winhelp.exe	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\winhlp32.exe	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control
%SystemRoot%\winnt.bmp	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	
%SystemRoot%\winnt256.bmp	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	
%SystemRoot%\winrep.exe	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control	**Users:** Read and Execute **Power Users:** Read and Execute **Administrators:** Full Control **SYSTEM:** Full Control

APPENDIX F – GROUP POLICY SETTINGS VS. REGISTRY KEYS

This table is a cross reference between the Group Policy settings and the Windows 2000 registry keys that are changed by the policy setting. Here, HKLM = HKEY_LOCAL_MACHINE and HKCU = HKEY_CURRENT_USER.

Group Policy	Registry entry
Action on server disconnect (Computer)	**Name:** GoOfflineAction **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Action on server disconnect (User)	**Name:** GoOfflineAction **Key:** HKCU\Software\Policies\Microsoft\Windows\NetCache
Active Desktop Wallpaper	**Name:** Wallpaper, WallpaperStyle **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Add "Run in Separate Memory Space" check box to Run dialog box	**Name:** MemCheckBoxInRunDlg **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Add Logoff to the Start Menu	**Name:** ForceStartMenuLogOff **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Add/Delete items	**Name:** Add, Delete **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop
Administratively assigned offline files (Computer)	**Name:** AssignedOfflineFolders subkey **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache\AssignedOfflineFolders
Administratively assigned offline files (User)	**Name:** AssignedOfflineFolders subkey **Key:** HKCU\Software\Policies\Microsoft\Windows\NetCache\AssignedOfflineFolders
Allow access to current user's RAS connection properties	**Name:** NC_RasMyProperties **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Allow admin to install from Terminal Services session	**Name:** EnableAdminTSRemote **Key:** HKLM\Software\Policies\Microsoft\Windows\Installer
Allow configuration of connection sharing (Computer)	**Name:** NC_ShowSharedAccessUI **Key:** HKLM\Software\Policies\Microsoft\Windows\Network Connections
Allow configuration of connection sharing (User)	**Name:** NC_ShowSharedAccessUI **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Allow connection components to be enabled or disabled	**Name:** NC_ChangeBindState **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Allow only bitmapped wallpaper	**Name:** NoHTMLWallPaper **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop
Allow printers to be published	**Name:** PublishPrinters **Key:** HKLM\Software\Policies\Microsoft\Windows NT\Printers
Allow pruning of published printers	**Name:** Immortal **Key:** HKLM\Software\Policies\Microsoft\Windows NT\Printers
Allow TCP/IP advanced configuration	**Name:** NC_AllowAdvancedTCPIPConfig **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Always install with elevated privileges (Computer)	**Name:** AlwaysInstallElevated **Key:** HKLM\Software\Policies\Microsoft\Windows\Installer
Always install with elevated privileges (User)	**Name:** AlwaysInstallElevated **Key:** HKCU\Software\Policies\Microsoft\Windows\Installer

Apply group policy for computers asynchronously during startup	**Name:** SynchronousMachineGroupPolicy **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
Apply group policy for users asynchronously during logon	**Name:** SynchronousUserGroupPolicy **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
Apply policy to removable media	**Name:** ApplyToRemovableMedia **Key:** HKLM\Software\Policies\Microsoft\Windows NT\DiskQuota
At logoff, delete local copy of user's offline files	**Name:** PurgeAtLogoff **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Automatically publish new printers in Active Directory	**Name:** Auto Publishing **Key:** HKLM\Software\Policies\Microsoft\Windows NT\Printers\Wizard
Browse a common web site to find printers	**Name:** Printers Page URL **Key:** HKCU\Software\Policies\Microsoft\Windows NT\Printers\Wizard
Browse the network to find printers	**Name:** Downlevel Browse **Key:** HKCU\Software\Policies\Microsoft\Windows NT\Printers\Wizard
Cache transforms in secure location on workstation	**Name:** TransformsSecure **Key:** HKLM\Software\Policies\Microsoft\Windows\Installer
Century interpretation for Year 2000	**Name:** <Calendar-ID> **Key:** HKCU\Software\Policies\Microsoft\Control Panel\International\Calendars\TwoDigitYearMax
Check published state	**Name:** VerifyPublishedState **Key:** HKLM\Software\Policies\Microsoft\Windows NT\Printers
Clear history of recently opened documents on exit	**Name:** ClearRecentDocsOnExit **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Code signing for device drivers	**Name:** BehaviorOnFailedVerify **Key:** HKCU\Software\Policies\Microsoft\Windows NT\Driver Signing
Computer location	**Name:** PhysicalLocation **Key:** HKLM\Software\Policies\Microsoft\Windows NT\Printers
Connect home directory to root of the share	**Name:** ConnectHomeDirToRoot **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Create new Group Policy Object links disabled by default	**Name:** NewGPOLinksDisabled **Key:** HKCU\Software\Policies\Microsoft\Windows\Group Policy Editor
Custom support URL in the Printers folder's left pane	**Name:** SupportLink, SupportLinkName **Key:** HKLM\Software\Policies\Microsoft\Windows NT\Printers
Custom user interface	**Name:** Shell **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Default Active Directory path when searching for printers	**Name:** Default Search Scope **Key:** HKCU\Software\Policies\Microsoft\Windows NT\Printers\Wizard
Default cache size	**Name:** DefCacheSize **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Default quota limit and warning level	**Name:** Limit, LimitUnits, Threshold, ThresholdUnits **Key:** HKLM\Software\Policies\Microsoft\Windows NT\DiskQuota
Delete cached copies of roaming profiles	**Name:** DeleteRoamingCache **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
Directory pruning interval	**Name:** PruningInterval **Key:** HKLM\Software\Policies\Microsoft\Windows NT\Printers
Directory pruning priority	**Name:** PruningPriority

	Key: HKLM\Software\Policies\Microsoft\Windows NT\ Printers
Directory pruning retry	**Name:** PruningRetries **Key:** HKLM\Software\Policies\Microsoft\Windows NT\ Printers
Disable "Make Available Offline" (Computer)	**Name:** NoMakeAvailableOffline **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Disable "Make Available Offline" (User)	**Name:** NoMakeAvailableOffline **Key:** HKCU\Software\Policies\Microsoft\Windows\ NetCache
Disable Active Desktop	**Name:** NoActiveDesktop **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Disable Add/Remove Programs	**Name:** NoAddRemovePrograms **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Uninstall
Disable adding, dragging, dropping and closing the Taskbar's toolbars	**Name:** NoCloseDragDropBands **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Disable addition of printers	**Name:** NoAddPrinter **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Disable adjusting desktop toolbars	**Name:** NoMovingBands **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Disable Advanced Menu (Computer)	**Name:** Disable Advanced **Key:** HKLM\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Disable Advanced Menu (User)	**Name:** Disable Advanced **Key:** HKCU\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Disable all items	**Name:** NoComponents (Software\Microsoft\Windows\CurrentVersion\Policies\ ActiveDesktop
Disable and remove links to Windows Update	**Name:** NoWindowsUpdate **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Disable and remove the Shut Down command	**Name:** NoClose **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Disable automatic update of ADM files	**Name:** DisableAutoADMUpdate **Key:** HKCU\Software\Policies\Microsoft\Windows\Group Policy Editor
Disable Autoplay (Computer)	**Name:** NoDriveTypeAutoRun **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Disable Autoplay (User)	**Name:** NoDriveTypeAutoRun **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Disable background refresh of group policy	**Name:** DisableBkGndGroupPolicy **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\ Policies\System
Disable Boot / Shutdown / Logon / Logoff status messages	**Name:** DisableStatusMessages **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\ Policies\System
Disable browse dialog box for new source	**Name:** DisableBrowse **Key:** HKLM\Software\Policies\Microsoft\Windows\Installer
Disable Change Password	**Name:** Disable Change Password **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\System
Disable changes to Taskbar and Start Menu Settings	**Name:** NoSetTaskbar **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Disable changing wallpaper	**Name:** NoChangingWallPaper

	Key: HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop
Disable context menu for taskbar	**Name:** NoTrayContextMenu **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable Control Panel	**Name:** NoControlPanel **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable deletion of printers	**Name:** NoDeletePrinter **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable DFS tab	**Name:** NoDFSTab **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable Display in control panel	**Name:** NoDispCPL **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Disable Drag-and-Drop (Computer)	**Name:** DragAndDrop **Key:** HKLM\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Disable Drag-and-Drop (User)	**Name:** DragAndDrop **Key:** HKCU\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Disable drag-and-drop context menus on the Start Menu	**Name:** NoChangeStartMenu **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable IE security prompt for Windows Installer scripts	**Name:** SafeForScripting **Key:** HKLM\Software\Policies\Microsoft\Windows\Installer
Disable legacy run list (Computer)	**Name:** DisableLocalMachineRun **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable legacy run list (User)	**Name:** DisableLocalMachineRun **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable Lock Computer	**Name:** DisableLockWorkstation **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Disable Logoff	**Name:** NoLogoff **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable Logoff on the Start Menu	**Name:** StartMenuLogOff **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable media source for any install	**Name:** DisableMedia **Key:** HKCU\Software\Policies\Microsoft\Windows\Installer
Disable New Task Creation (Computer)	**Name:** Task Creation **Key:** HKLM\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Disable New Task Creation (User)	**Name:** Task Creation **Key:** HKCU\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Disable patching	**Name:** DisablePatch **Key:** HKLM\Software\Policies\Microsoft\Windows\Installer
Disable personalized menus	**Name:** Intellimenus **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable programs on Settings menu	**Name:** NoSetFolders **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable registry editing tools	**Name:** DisableRegistryTools **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Disable reminder balloons (Computer)	**Name:** NoReminders **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache

Disable reminder balloons (User)	**Name:** NoReminders **Key:** HKCU\Software\Policies\Microsoft\Windows\NetCache\AssignedOfflineFolders
Disable rollback (Computer)	**Name:** DisableRollback **Key:** HKLM\Software\Policies\Microsoft\Windows\Installer
Disable rollback (User)	**Name:** DisableRollback **Key:** HKCU\Software\Policies\Microsoft\Windows\Installer
Disable Support Information	**Name:** NoSupportInfo **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall
Disable Task Deletion (Computer)	**Name:** Task Deletion **Key:** HKLM\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Disable Task Deletion (User)	**Name:** Task Deletion **Key:** HKCU\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Disable Task Manager	**Name:** DisableTaskMgr **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Disable the command prompt	**Name:** DisableCMD **Key:** HKCU\Software\Policies\Microsoft\Windows\System
Disable the run once list (Computer)	**Name:** DisableLocalMachineRunOnce **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable the run once list (User)	**Name:** DisableLocalMachineRunOnce **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable UI to change keyboard navigation indicator setting	**Name:** NoChangeKeyboardNavigationIndicators **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable UI to change menu animation setting	**Name:** NoChangeAnimation **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable user configuration of Offline Files (Computer)	**Name:** NoConfigCache **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Disable user configuration of Offline Files (User)	**Name:** NoConfigCache **Key:** HKCU\Software\Policies\Microsoft\Windows\NetCache
Disable user tracking	**Name:** NoInstrumentation **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable Windows Explorer's default context menu	**Name:** NoViewContextMenu **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Disable Windows Installer	**Name:** DisableMSI **Key:** HKLM\Software\Policies\Microsoft\Windows\Installer
Disk Quota policy processing	**Name:** NoSlowLink, NoBackgroundPolicy, NoGPOListChanges **Key:** HKLM\Software\Policies\Microsoft\Windows\Group Policy\{3610eda5-77ef-11d2-8dc5-00c04fa31a66}
Display and enable the Network Connection wizard	**Name:** NC_NewConnectionWizard **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Do not add shares from recently opened documents to the My Network Places folder	**Name:** NoRecentDocsNetHood **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Do not automatically encrypt files moved to encrypted folders	**Name:** NoEncryptOnMove **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Do not detect slow network connections	**Name:** SlowLinkDetectEnabled **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
Do not keep history of recently opened documents	**Name:** NoRecentDocsHistory **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\

	Policies\Explorer
Do not request alternate credentials	**Name:** NoRunasInstallPrompt **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Do not track Shell shortcuts during roaming	**Name:** LinkResolveIgnoreLinkInfo **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Do not use the search-based method when resolving shell shortcuts	**Name:** NoResolveSearch **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Do not use the tracking-based method when resolving shell shortcuts	**Name:** NoResolveTrack **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Don't display welcome screen at logon (Computer)	**Name:** NoWelcomeScreen **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Don't display welcome screen at logon (User)	**Name:** NoWelcomeScreen **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Don't run specified Windows applications	**Name:** DisallowRun **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Don't save settings at exit	**Name:** NoSaveSettings **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Download missing COM components (Computer)	**Name:** COMClassStore **Key:** HKLM\Software\Policies\Microsoft\Windows\App Management
Download missing COM components (User)	**Name:** COMClassStore **Key:** HKCU\Software\Policies\Microsoft\Windows\App Management
EFS recovery policy processing	**Name:** NoSlowLink, NoBackgroundPolicy, NoGPOListChanges **Key:** HKLM\Software\Policies\Microsoft\Windows\Group Policy\{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}
Enable access to properties of a LAN connection	**Name:** NC_LanProperties **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Enable access to properties of components of a LAN connection	**Name:** NC_LanChangeProperties **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Enable access to properties of components of a RAS connection	**Name:** NC_RasChangeProperties **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Enable access to properties of RAS connections available to all users	**Name:** NC_RasAllUserProperties **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Enable Active Desktop	**Name:** ForceActiveDesktopOn **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop
Enable adding or removing components of a RAS or LAN connection	**Name:** NC_AddRemoveComponents **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Enable Classic Shell	**Name:** ClassicShell **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Enable connecting and disconnecting a LAN connection	**Name:** NC_LanConnect **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Enable connecting and disconnecting a RAS connection	**Name:** NC_RasConnect **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Enable deletion of RAS connections	**Name:** NC_DeleteConnection **Key:** HKCU\Software\Policies\Microsoft\Windows\Network

	Connections
Enable deletion of RAS connections available to all users	**Name:** NC_DeleteAllUserConnection **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Enable disk quotas	**Name:** Enable **Key:** HKLM\Software\Policies\Microsoft\Windows NT\ DiskQuota
Enable filter in Find dialog box	**Name:** EnableFilter **Key:** HKCU\Software\Policies\Microsoft\Windows\Directory UI
Enable renaming of connections, if supported	**Name:** NC_RenameConnection **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Enable renaming of RAS connections belonging to the current user	**Name:** NC_RenameMyRasConnection **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Enable status statistics for an active connection	**Name:** NC_Statistics **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Enable the Advanced Settings item on the Advanced menu	**Name:** NC_AdvancedSettings **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Enable the Dial-up Preferences item on the Advanced menu	**Name:** NC_DialupPrefs **Key:** HKCU\Software\Policies\Microsoft\Windows\Network Connections
Enable user control over installs	**Name:** EnableUserControl **Key:** HKLM\Software\Policies\Microsoft\Windows\Installer
Enable user to browse for source while elevated	**Name:** AllowLockdownBrowse **Key:** HKLM\Software\Policies\Microsoft\Windows\Installer
Enable user to patch elevated products	**Name:** AllowLockdownPatch **Key:** HKLM\Software\Policies\Microsoft\Windows\Installer
Enable user to use media source while elevated	**Name:** AllowLockdownMedia **Key:** HKLM\Software\Policies\Microsoft\Windows\Installer
Enabled	**Name:** Enabled **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Enforce disk quota limit	**Name:** Enforce **Key:** HKLM\Software\Policies\Microsoft\Windows NT\ DiskQuota
Enforce Show Policies Only	**Name:** ShowPoliciesOnly **Key:** HKCU\Software\Policies\Microsoft\Windows\Group Policy Editor
Event logging level (Computer)	**Name:** EventLoggingLevel **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Event logging level (User)	**Name:** EventLoggingLevel **Key:** HKCU\Software\Policies\Microsoft\Windows\ NetCache
Exclude directories in roaming profile	**Name:** ExcludeProfileDirs **Key:** HKCU\Software\Policies\Microsoft\Windows\System
FAX Service	**Name:** Restrict_Run **Key:** HKCU\Software\Policies\Microsoft\MMC\{753EDB4D-2E1B-11D1-9064-00A0C90AB504}
Files not cached	**Name:** ExcludeExtensions **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Folder Redirection policy processing	**Name:** NoSlowLink, NoGPOListChanges **Key:** HKLM\Software\Policies\Microsoft\Windows\Group Policy\{25537BA6-77A8-11D2-9B6C-0000F8080861}
Go directly to Components wizard	**Name:** NoServices **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Uninstall
Gray unavailable Windows Installer programs Start Menu shortcuts	**Name:** GreyMSIAds **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Group Policy domain controller selection	**Name:** DCOption **Key:** HKCU\Software\Policies\Microsoft\Windows\Group

	Policy Editor
Group Policy refresh interval for computers	**Name:** GroupPolicyRefreshTime, GroupPolicyRefreshTimeOffset **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
Group Policy refresh interval for domain controllers	**Name:** GroupPolicyRefreshTimeDC, GroupPolicyRefreshTimeOffsetDC **Key:** HKLM\Software\Policies\Microsoft\Windows\System
Group Policy refresh interval for users	**Name:** GroupPolicyRefreshTime , GroupPolicyRefreshTimeOffset **Key:** HKCU\Software\Policies\Microsoft\Windows\System
Group Policy slow link detection (Computer)	**Name:** GroupPolicyMinTransferRate **Key:** HKLM\Software\Policies\Microsoft\Windows\System
Group Policy slow link detection (User)	**Name:** GroupPolicyMinTransferRate **Key:** HKCU\Software\Policies\Microsoft\Windows\System
Group Policy snap-in	**Name:** Restrict_Run **Key:** HKCU\Software\Policies\Microsoft\MMC\{8FC0B734-A0E1-11D1-A7D3-0000F87571E3}
Hide Active Directory folder	**Name:** HideDirectoryFolder **Key:** HKCU\Software\Policies\Microsoft\Windows\Directory UI
Hide Add New Programs page	**Name:** NoAddPage **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall
Hide Add/Remove Windows Components page	**Name:** NoWindowsSetupPage **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall
Hide all icons on Desktop	**Name:** NoDesktop **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Hide Appearance tab	**Name:** NoDispAppearancePage **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Hide Background tab	**Name:** NoDispBackgroundPage **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Hide Change or Remove Programs page	**Name:** NoRemovePage **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall
Hide Hardware tab	**Name:** NoHardwareTab **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Hide Internet Explorer icon on desktop	**Name:** NoInternetIcon **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Hide My Network Places icon on desktop	**Name:** NoNetHood **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Hide Property Pages (Computer)	**Name:** Property Pages **Key:** HKLM\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Hide Property Pages (User)	**Name:** Property Pages **Key:** HKCU\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Hide Screen Saver tab	**Name:** NoDispScrSavPage **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Hide Settings tab	**Name:** NoDispSettingsPage **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Hide specified control panel applets	**Name:** DisallowCpl, HREF="mk:@MSITStore:regentry.chm::/93227.asp"> DisallowCpl subkey **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\

	Policies\Explorer
Hide the "Add a program from CD-ROM or floppy disk" option	**Name:** NoAddFromCDorFloppy **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall
Hide the "Add programs from Microsoft" option	**Name:** NoAddFromInternet **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall
Hide the "Add programs from your network" option	**Name:** NoAddFromNetwork **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Uninstall
Hide the common dialog back button	**Name:** NoBackButton **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
Hide the common dialog places bar	**Name:** NoPlacesBar **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
Hide the dropdown list of recent files	**Name:** NoFileMru **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Comdlg32
Hide the file scan progress window	**Name:** SfcShowProgress **Key:** HKLM\Software\Policies\Microsoft\Windows NT\Windows File Protection
Hide these specified drives in My Computer	**Name:** NoDrives **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Hides the Manage item on the Windows Explorer context menu	**Name:** NoManageMyComputerVerb **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Initial reminder balloon lifetime (Computer)	**Name:** InitialBalloonTimeoutSeconds **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Initial reminder balloon lifetime (User)	**Name:** InitialBalloonTimeoutSeconds **Key:** HKCU\Software\Policies\Microsoft\Windows\NetCache\AssignedOfflineFolders
Internet Explorer Maintenance policy processing	**Name:** NoSlowLink, NoBackgroundPolicy, NoGPOListChanges **Key:** HKLM\Software\Policies\Microsoft\Windows\Group Policy\{A2E30F80-D7DE-11d2-BBDE-00C04F86AE3B}
IP Security policy processing	**Name:** NoSlowLink, NoBackgroundPolicy, NoGPOListChanges **Key:** HKLM\Software\Policies\Microsoft\Windows\Group Policy\{e437bc1c-aa7d-11d2-a382-00c04f991e27}
Limit profile size	**Name:** EnableProfileQuota, IncludeRegInProQuota, MaxProfileSize, ProfileQuotaMessage, WarnUser, WarnUserTimeout **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Limit Windows File Protection cache size	**Name:** SfcQuota **Key:** HKLM\Software\Policies\Microsoft\Windows NT\Windows File Protection
Log event when quota limit exceeded	**Name:** LogEventOverLimit **Key:** HKLM\Software\Policies\Microsoft\Windows NT\DiskQuota
Log event when quota warning level exceeded	**Name:** LogEventOverThreshold **Key:** HKLM\Software\Policies\Microsoft\Windows NT\DiskQuota
Log users off when roaming profile fails	**Name:** ProfileErrorAction **Key:** HKLM\Software\Policies\Microsoft\Windows\System
Logging	**Name:** Logging **Key:** HKLM\Software\Policies\Microsoft\Windows\Installer
Maximum number of Recent documents	**Name:** MaxRecentDocs **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Maximum retries to unload and update user profile	**Name:** ProfileUnloadTimeout **Key:** HKLM\SOFTWARE\Policies\Microsoft\Windows\

	System
Maximum size of Active Directory searches	**Name:** QueryLimit **Key:** HKCU\Software\Policies\Microsoft\Windows\Directory UI
Maximum wait time for Group Policy scripts	**Name:** MaxGPOScriptWait **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\ Policies\System
No "Computers Near Me" in My Network Places	**Name:** NoComputersNearMe **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
No "Entire Network" in My Network Places	**Name:** NoEntireNetwork **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Network
No screen saver	**Name:** ScreenSaveActive **Key:** HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop
Non-default server disconnect actions (Computer	**Name:** CustomGoOfflineActions subkey **Key:** HKLM\Software\Policies\Microsoft\Windows\ NetCache\CustomGoOfflineActions
Non-default server disconnect actions (User	**Name:** CustomGoOfflineActions subkey **Key:** HKCU\Software\Policies\Microsoft\Windows\ NetCache\CustomGoOfflineActions
Only allow approved Shell extensions	**Name:** EnforceShellExtensionSecurity **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Password protect the screen saver	**Name:** ScreenSaverIsSecure **Key:** HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop
Pre-populate printer search location text	**Name:** PhysicalLocationSupport **Key:** HKLM\Software\Policies\Microsoft\Windows NT\ Printers
Prevent access to drives from My Computer	**Name:** NoViewOnDrive **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Prevent Task Run or End (Computer	**Name:** Execution **Key:** HKLM\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Prevent Task Run or End (User	**Name:** Execution **Key:** HKCU\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Prevent use of Offline Files folder (Computer)	**Name:** NoCacheViewer **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Prevent use of Offline Files Folder (User)	**Name:** NoCacheViewer **Key:** HKCU\Software\Policies\Microsoft\Windows\ NetCache
Primary DNS Suffix	**Name:** NV PrimaryDnsSuffix, PrimaryDnsSuffix **Key:** HKLM\Software\Policies\Microsoft\System\DNSclient
Printer browsing	**Name:** ServerThread **Key:** HKLM\Software\Policies\Microsoft\Windows NT\ Printers
Prohibit adding items	**Name:** NoAddingComponents **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\ ActiveDesktop
Prohibit Browse (Computer)	**Name:** Allow Browse **Key:** HKLM\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Prohibit Browse (User)	**Name:** Allow Browse **Key:** HKCU\Software\Policies\Microsoft\Windows\Task Scheduler5.0
Prohibit changes	**Name:** NoActiveDesktopChanges **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Prohibit closing items	**Name:** NoClosingComponents **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\

	Policies\ActiveDesktop
Prohibit deleting items	**Name:** NoDeletingComponents **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop
Prohibit editing items	**Name:** NoEditingComponents **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\ActiveDesktop
Prohibit user from changing My Documents path	**Name:** DisablePersonalDirChange **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Prompt user when slow link is detected	**Name:** SlowLinkUIEnabled **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
Prune printers that are not automatically republished	**Name:** PruneDownlevel **Key:** HKLM\Software\Policies\Microsoft\Windows NT\Printers
Registry policy processing	**Name:** NoBackgroundPolicy, NoGPOListChanges **Key:** HKLM\Software\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}
Reminder balloon frequency (Computer)	**Name:** ReminderFreqMinutes **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Reminder balloon frequency (User)	**Name:** ReminderFreqMinutes **Key:** HKCU\Software\Policies\Microsoft\Windows\NetCache\AssignedOfflineFolders
Reminder balloon lifetime (Computer)	**Name:** ReminderBalloonTimeoutSeconds **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Reminder balloon lifetime (User)	**Name:** ReminderBalloonTimeoutSeconds (ReminderBalloonTimeoutSeconds) **Key:** HKCU\Software\Policies\Microsoft\Windows\NetCache
Remove "Map Network Drive" and "Disconnect Network Drive"	**Name:** NoNetConnectDisconnect **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove common program groups from Start Menu	**Name:** NoCommonGroups **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove Disconnect item from Start menu (Terminal Services only)	**Name:** NoDisconnect **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove Documents menu from Start Menu	**Name:** NoRecentDocsMenu **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove Favorites menu from Start Menu	**Name:** NoFavoritesMenu **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove File menu from Windows Explorer	**Name:** NoFileMenu **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove Help menu from Start Menu	**Name:** NoSMHelp **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove My Documents icon from desktop	**Name:** {450D8FBA-AD25-11D0-98A8-0800361B1103} **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\NonEnum
Remove My Documents icon from Start Menu	**Name:** NoSMMyDocs **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove Network & Dial-up Connections from Start Menu	**Name:** NoNetworkConnections **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove Run menu from Start Menu	**Name:** NoRun **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove Search button from Windows	**Name:** NoShellSearchButton

Explorer	**Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove Search menu from Start Menu	**Name:** NoFind **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove security option from Start menu (Terminal Services only	**Name:** NoNTSecurity **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove the Folder Options menu item from the Tools menu	**Name:** NoFolderOptions **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Remove user's folders from the Start Menu	**Name:** NoStartMenuSubFolders **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Request credentials for network installations	**Name:** PromptRunasInstallNetPath **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Restrict selection of Windows 2000 menus and dialogs language	**Name:** MultiUILanguageID **Key:** HKCU\Software\Policies\Microsoft\Control Panel\Desktop
Restrict the user from entering author mode	**Name:** RestrictAuthorMode **Key:** HKCU\Software\Policies\Microsoft\MMC
Restrict users to the explicitly permitted list of snap-ins	**Name:** RestrictToPermittedSnapins **Key:** HKCU\Software\Policies\Microsoft\MMC
Run legacy logon scripts hidden	**Name:** HideLegacyLogonScripts **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Run logoff scripts visible	**Name:** HideLogoffScripts **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Run logon scripts synchronously (Computer)	**Name:** RunLogonScriptSync **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
Run logon scripts synchronously (User)	**Name:** RunLogonScriptSync **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Run logon scripts visible	**Name:** HideLogonScripts **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System
Run only allowed Windows applications	**Name:** RestrictRun **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer
Run shutdown scripts visible	**Name:** HideShutdownScripts **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
Run startup scripts asynchronously	**Name:** RunStartupScriptSync **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
Run startup scripts visible	**Name:** HideStartupScripts **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\System
Run these programs at user logon (Computer)	**Name:** Run subkey **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
Run these programs at user logon (Use)r	**Name:** Run subkey **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run
Screen saver executable name	**Name:** SCRNSAVE.EXE **Key:** HKCU\Software\Policies\Microsoft\Windows\Control Panel\Desktop
Scripts policy processing	**Name:** NoSlowLink, NoBackgroundPolicy, NoGPOListChanges **Key:** HKLM\Software\Policies\Microsoft\Windows\Group Policy\{42B5FAAE-6536-11d2-AE5A-0000F87571E3}

Search order	**Name:** SearchOrder **Key:** HKCU\Software\Policies\Microsoft\Windows\Installer
Security policy processing	**Name:** NoBackgroundPolicy, NoGPOListChanges **Key:** HKLM\Software\Policies\Microsoft\Windows\Group Policy\{827D319E-6EAC-11D2-A4EA-00C04F79F83A}
Set Windows File Protection scanning	**Name:** SfcScan **Key:** HKLM\Software\Policies\Microsoft\Windows NT\ Windows File Protection
Show only specified control panel applets	**Name:** RestrictCpl, HREF="mk:@MSITStore:regentry.chm::/93230.asp"> RestrictCpl subkey **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Explorer
Slow network connection timeout for user profiles	**Name:** SlowLinkTimeOut, UserProfileMinTransferRate **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\ Policies\System
Software Installation policy processing	**Name:** NoGPOListChanges, NoSlowLink **Key:** HKLM\Software\Policies\Microsoft\Windows\Group Policy\{c6dc5466-785a-11d2-84d0-00c04fb169f7}
Specify default category for Add New Programs	**Name:** DefaultCategory **Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\ Policies\Uninstall
Specify Windows File Protection cache location	**Name:** SFCDllCacheDir **Key:** HKLM\Software\Policies\Microsoft\Windows NT\ Windows File Protection
Subfolders always available offline	**Name:** AlwaysPinSubFolders **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Synchronize all offline files before logging off (Computer)	**Name:** SyncAtLogoff **Key:** HKLM\Software\Policies\Microsoft\Windows\NetCache
Synchronize all offline files before logging off (User)	**Name:** SyncAtLogoff **Key:** HKCU\Software\Policies\Microsoft\Windows\ NetCache
Timeout for dialog boxes	**Name:** ProfileDlgTimeOut **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\ Policies\System
User Group Policy loopback processing mode	**Name:** UserPolicyMode **Key:** HKLM\Software\Policies\Microsoft\Windows\System
Verbose vs normal status messages	**Name:** VerboseStatus **Key:** HKLM\Software\Microsoft\Windows\CurrentVersion\ Policies\System
Wait for remote user profile	**Name:** SlowLinkProfileDefault **Key:** HKLM\Software\Policies\Microsoft\Windows\System
Web-based printing	**Name:** DisableWebPrinting **Key:** HKLM\Software\Policies\Microsoft\Windows NT\ Printers

For more information, see the Group Policy Registry Table in the *Windows 2000 Professional Resource Kit*; “Group Policy Reference” (CD-ROM).

Department of Energy
CIAC
Computer Incident Advisory Capability

Technical Information Department • Lawrence Livermore National Laboratory
University of California • Livermore, California 94551