File permissions

File permissions include Full Control, Modify, Read & Execute, Read, and Write. Each of these permissions consists of a logical group of special permissions. The following table lists each file permission and specifies which special permissions are associated with that permission.

Special Permissions	Full Control	Modify	Read & Execute	Read	Write
Traverse Folder/Execute File	x	x	x		
List Folder/Read Data	x	x	x	x	
Read Attributes	x	x	x	x	
Read Extended Attributes	x	x	x	x	
Create Files/Write Data	x	x			x
Create Folders/Append Data	x	x			x
Write Attributes	x	x			x
Write Extended Attributes	x	x			x
Delete Subfolders and Files	x				
Delete	x	x			
Read Permissions	x	x	x	x	x
Change Permissions	x				
Take Ownership	x				
Synchronize	x	x	x	x	x

Notes

Groups or users granted Full Control on a folder can delete any files in that folder regardless of the permissions protecting the file.
For information on setting permissions and descriptions of each special permission, see Related Topics.

Related Topics

Default security settings

The default security settings for Windows 2000 can be described by summarizing the permissions granted to four default groups (Administrators, Power Users, Users, and Backup Operators) and three special groups.

Administrators

Members of the Administrators group can perform all functions supported by the operating system. The default security settings do not restrict administrative access to any registry or file system object. Administrators can grant themselves any rights that they do not have by default.

Ideally, administrative access should only be used to:

- Install the operating system and components (such as hardware drivers, system services, and so on).
- Install Service Packs and Windows Packs.
- Upgrade the operating system.
- Repair the operating system.
- Configure critical operating system parameters (such as password policy, access control, audit policy, kernel mode driver configuration, and so on).
- Take ownership of files that have become inaccessible.
- Manage the security and auditing logs.
- Back up and restore the system.

In practice, Administrator accounts often must be used to install and run programs written for previous versions of Windows.

Users

The Users group provides the most secure environment in which to run programs. On a volume formatted with NTFS, the default security settings on a newly installed system (but not on an upgraded system) are designed to prevent members of this group from compromising the integrity of the operating system and installed programs. Users cannot modify system -wide registry settings, operating system files, or program files. Users can shut down workstations, but not servers. Users can create local groups, but can manage only the local groups that they created. They can run certified Windows 2000 programs that have been installed or deployed by administrators. Users have full control over all of their own data files (%userprofile%) and their own portion of the registry (HKEY_CURRENT_USER).

Users cannot install programs that can be run by other Users (this prevents Trojan horse programs). They also cannot access other Users' private data or desktop settings.

To secure a Windows 2000 system, an administrator should:

- Make sure that end users are members of the Users group only.
- Deploy programs, such as certified Windows 2000 programs, that members of the Users group can run successfully.

Users will not be able to run most programs written for previous versions of Windows because previous versions of Windows either did not support file system and registry security (Windows 95 and Windows 98) or shipped with lax default security settings (Windows NT). If Users have problems running legacy applications on newly installed NTFS systems, then do one of the following:

1. Install new versions of the applications that are certified for Windows 2000.
2. Move end users from the Users group into the Power Users group.
3. Decrease the default security permissions for the Users group. This can be accomplished by using the compatible security template. For more information, see "Predefined security templates" in Related Topics.

Power Users

Members of the Power Users group have more permissions than members of the Users group and fewer than members of the Administrators group. Power Users can perform any operating system task except tasks reserved for the Administrators group. The default Windows 2000 security settings for Power Users are very similar to the default security settings for Users in Windows NT 4.0. Any program that a User can run in Windows NT 4.0, a Power User can run in Windows 2000.

Power Users can:

- Run legacy applications in addition to Windows 2000 certified applications.
- Install programs that do not modify operating system files or install system services.
- Customize system -wide resources including Printers, Date/Time, Power Options, and other Control Panel resources.
- Create and manage local user accounts and groups.
- Stop and start system services which are not started by default.

Power Users do not have permission to add themselves to the Administrators group. Power Users do not have access to the data of other users on an NTFS volume, unless those users grant them permission.

⚠ Warning

- Running legacy programs on Windows 2000 often requires modify access to certain system settings. The same default permissions that allow Power Users to run legacy programs also make it possible for a Power User to gain additional privileges on the system, even complete administrative control. Therefore, it is important to deploy certified Windows 2000 programs in order to achieve maximal security without sacrificing program functionality. Programs that are certified for Windows 2000 can run successfully under the secure configuration provided by the Users group. For more information, see Securing Windows 2000 Installations at the Microsoft Security Advisor Web site.
- Since Power Users can install or modify programs, running as a Power User when connected to the Internet could make the system vulnerable to Trojan horse programs and other security risks. For more information, see "Why you should not run your computer as an administrator" in Related Topics.

Backup Operators

Members of the Backup Operators group can back up and restore files on the computer, regardless of any permissions that protect those files. They can also log on to the computer and shut it down, but they cannot change security settings.

⚠ Warning

- Backing up and restoring data files and system files requires permissions to read and write those files. The same default permissions granted to Backup Operators that allow them to back up and restore files also make it possible for them to use the group's permissions for other purposes, such as reading another user's files or installing Trojan horse programs. Group Policy settings can be used to create an environment in which Backup Operators only can run a backup program. For more information, see Securing Windows 2000 Installations at the Microsoft Security Advisor Web site.

Special Groups

Several additional groups are automatically created by Windows 2000.

- **Interactive**. This group contains the user who is currently logged on to the computer. During an upgrade to Windows 2000, members of the Interactive group will also be added to the Power Users group, so that legacy applications will continue to function as they did before the upgrade.
- **Network**. This group contains all users who are currently accessing the system over the network.
- **Terminal Server User**. When Terminal Servers are installed in application serving mode, this group contains any users who are currently logged on to the system using Terminal Server. Any program that a user can run in Windows NT 4.0 will run for a Terminal Server User in Windows 2000. The default permissions assigned to the group were chosen to enable a Terminal Server User to run most legacy programs.

  ⚠ Warning

  - Running legacy programs in Windows 2000 requires permission to modify certain system settings. The same default permissions that allow a Terminal Server User to run legacy programs also make it possible for a Terminal Server User to gain additional privileges on the system, even complete administrative control. Applications that are certified for Windows 2000 can run successfully under the secure configuration provided by the Users group. For more information, see Securing Windows 2000 Installations at the Microsoft Security Advisor Web site.

  Note

  - When Terminal Server is installed in remote administration mode, users logged on using Terminal Server will not be members of this group.

Related Topics

Differences between Windows NT 4.0 and Windows 2000 default security settings

Windows NT 4.0 provided two key groups whose membership could be controlled by the administrator: Administrators and Users. There was one group, Everyone, whose membership was controlled by the operating system or domain. Every user who was authenticated by the domain was a member of the Everyone group. If an administrator wanted stricter control of access to the computer's resources, the discretionary access control list (DACL) could be modified by removing the Everyone group.

Windows 2000 provides three groups whose membership is controlled by the administrator: Users, Power Users, and Administrators. The group whose membership is controlled by the operating system or domain is Authenticated Users. It is the same as the Everyone group, except that it does not contain anonymous users or guests.

Unlike the Everyone group in Windows NT 4.0, the Authenticated Users group is not used to assign permissions. Only groups controlled by the administrator, primarily Users, Power Users, and members of the Administrators group, are used to assign permissions. The default members of each group are listed below.

Local Group	Windows 2000 Professional	Windows 2000 Server
Administrators	Administrator	Administrator
Power Users	Authenticated Users	none
Users	Authenticated Users	Authenticated Users

By default in Windows 2000, any authenticated user is a member of the Users group. Windows 2000 Power Users have all the capabilities that Windows NT 4.0 Users had. This ensures backward compatibility with Windows NT 4.0. If an administrator wants to implement higher security on a Windows 2000 computer, Authenticated Users should be made members of the Users group only.

When a Windows 2000 Professional or Server computer joins a domain, the same domain groups are added to the computer that were added to a Windows NT 4.0 computer. Domain Administrators are added to the local Administrators group and Domain Users are added to the local Users group.

Related Topics

Default Access Control Settings in Windows 2000

Operating System

White Paper

Abstract

This white paper describes the default security settings for components of the Microsoft® Windows® 2000 operating system, including the registry and file system, as well as user rights and group membership. Implications for developers and system administrators are discussed, and answers to frequently asked questions are provided.

Default Access Control Settings for Windows 2000

Overview

A significant portion of the Microsoft® Windows® 2000 operating system security is defined by the default access permissions granted to three groups: Administrators, Power Users, and Users. At a very high level, these groups may be described as follows:

Administrators are all-powerful. The default Windows 2000 security settings do not restrict administrative access to any registry or file system object. Administrators can perform any and all functions supported by the operating system. Any right that the administrator does not have by default, they can grant to themselves.

Ideally, administrative access to the system should only be needed to:

- Install the operating system and components (including drivers for hardware, system services, and so forth).
- Install Service Packs and hotfixes.
- Install Windows updates.
- Upgrade the operating system
- Repair the operating system.
- Configure critical machine-wide operating system parameters, for example, kernel mode driver configuration, password policy, access control, and audit functions.

In practice, administrative accounts must often be used to install and run legacy Windows-based applications.

Users are the opposite of administrators. Provided that the Windows 2000 operating system is clean-installed onto an NTFS partition, the default security settings are designed to prohibit Users from compromising the integrity of the operating system and installed applications. Users cannot modify computer-wide registry settings, operating system files, or program files. Users cannot install applications that can be run by other members of the Users group (preventing Trojan horses). Users cannot access other users' private data. Thus, two significant aspects of securing a Windows 2000-based system are as follows:

1. Make sure that end-users are members of the Users group only.
2. Deploy applications that members of the Users group can successfully run.

Ideally, Users should be able to run any application that has been previously installed by an Administrator, Power User, or themselves. Users should not be able to run applications that are installed by other Users.

In practice, members of the Users group will not be able to run most legacy applications because most legacy applications were not designed with operating system security in mind. Members of the Power Users group should be able to run such applications.

Applications that comply with the Windows 2000 Application Specification (http://msdn.microsoft.com/certification/default.asp) can successfully run in a normal Users context.

Power Users are ranked between Administrators and Users in terms of system access. The default Windows 2000 security settings for Power Users are backward-compatible with the default security settings for Users in the Windows NT® 4.0 operating system. In short, Power Users are indeed powerful.

Ideally, Power Users should be able to perform any task except for the administrative tasks described above. Thus, Power Users should be able to:

- Install and remove applications per computer that do not install system services.
- Customize system-wide resources (for example, System Time, Display Settings, Shares, Power Configuration, Printers, and so forth).

Power Users are not allowed to access other users' data stored on an NTFS partition.

In practice, Power Users cannot install many legacy applications, because these applications attempt to replace operating system files during the setup process.

This is a nice safety feature. If you can't install an application as a Power User, maybe it shouldn't be installed at all.

Configuring Security During Setup

Default security settings are applied at the beginning of GUI-mode setup during a clean install of Windows 2000 or an upgrade from Windows NT/9x.

Note File system security settings can only be applied when the Windows 2000 operating system is installed onto an NTFS partition.

The default security settings for workstations, servers, and domain controllers can be found in the following files respectively:

- **%windir%\inf\defltwk.inf**
- **%windir%\inf\defltsv.inf**
- **%windir%\inf\defltdc.inf** (Note that default domain controller security settings are applied during DCPromo.)

Since security is applied at the beginning of GUI-mode setup, no explicit security settings are defined for optional components; for example, Internet Information Services (IIS) or Terminal Services that may be chosen during the GUI-mode phase of setup. This allows optional components to specify their own security if it should be different than what is inherited by default.

Default File System and Registry Permissions

The backward compatible permissions (access control) for Windows 2000 Power Users are included in Appendix A for file system objects and Appendix B for registry objects. The backward compatible default permissions for Power Users are liberal enough that most applications should be able to be installed by a Power User. For example, Power Users have Modify access to:

- **HKEY_LOCAL_MACHINE\Software**
- Program Files
- **%windir%**
- **%windir%\system32**

Power Users have only Read access to the core Windows 2000 system files.

Even though Power Users have Modify access to the **%windir%** and **%windir%\system32** directories, Power Users have Read access to the files that are installed in these directories during Windows 2000 text-mode setup. This allows legacy applications to write new files into the system directories, but prevents Power Users from modifying the Windows 2000 system files. Additionally, Power Users are not allowed to install Windows 2000 services.

The default permissions for Administrators and Users are more easily described as follows:

- Administrators, System, and Creator Owner are given Full Control to all file system and registry objects that exist at the beginning of GUI-mode setup.

- Users are explicitly granted Write access to the locations specified in Table 1.

Table 1 Users Write Access Locations

Object	Permission	Comment
HKEY_Current_User	Full Control	User's portion of the registry
%UserProfile%	Full Control	User's Profile directory
All Users\Documents	Read, Create File	Shared Documents Location. Allows Users to create files that can subsequently be read (but not modified) by other Users.
%Windir%\Temp	Synchronize, Traverse, Add File, Add Subdir	Per-Machine temp directory. This is a concession made for service-based applications so that Profiles do not need to be loaded in order to get the per-User temp directory of an impersonated user.
\ (Root Directory)	Not Configured during setup	Not configured during setup because the Windows 2000 ACL Inheritance model would impact all child objects including those outside the scope of setup.

By default, Users have Read (or less) access to the rest of the system.

It is possible for applications that are installed by administrators to create their own subfolders and specify their own permissions on those subfolders. Certified applications that do not want to inherit the default security settings must create such subfolders in All Users\Documents or All Users\Application Data. For example, an application might want to store a centralized clip-art gallery that any User is allowed to modify. Such configurations should be reviewed by system administrators to determine whether the application functionality requiring this configuration is worth the potential security risk posed by the configuration. Isolating such configurations to these two locations (for certified applications), promises to make the task of identifying these potential security vulnerabilities easier.

Also of note is the fact that permissions on the root directory are not defined during setup. Setup does not change the permissions on the root directory because the Windows 2000 ACL Inheritance model would recursively try to configure all subdirectories of the root. This could result in undesired changes for non-Windows 2000-based directories that may exist on the install partition.

Since setup does not change permissions on the root directory, the permissions that previously existed on the root directory are maintained. These root permissions are inherited by any new subdirectories created off of the root, and may be inherited by non-Windows 2000-based directories that already exist off of the root. Thus, after a clean-install setup, the root directory and any non-Windows-based subdirectories should be configured according to the security needs of the organization and the requirements of the applications that need to be run.

Default User Rights

The default User rights for clean-installed workstation and member servers are defined in the Table 2. They differ only in one respect and that is in the *Shutdown the system* right. On servers, Users are not granted this right by default.

Table 2 Default User Rights

User Right	Default Workstation	Default Server
Replace a Process-Level Token		
Generate Security Audits		
Logon as a Batch Job		

Backup Files and Directories	Administrators, Backup Ops	Administrators, Backup Ops
Bypass Traverse Checking	Administrators, Backup Ops, Power Users, Users, Everyone	Administrators, Backup Ops, Power Users, Users, Everyone
Create a Pagefile	Administrators	Administrators
Create Permanent Shared Objects		
Create a Token Object		
Debug Programs	Administrators	Administrators
Increase Scheduling Priority	Administrators	Administrators
Increase Quotas	Administrators	Administrators
Logon Interactively	Administrators, Backup Ops, Power Users, Users, Guest	Administrators, Backup Ops, Power Users, Users, Guest
Load and Unload Device Drivers	Administrators	Administrators
Lock Pages in Memory		
Add workstations to the domain		
Access this computer from the network	Administrators, Backup Ops, Power Users, Users, Everyone	Administrators, Backup Ops, Power Users, Users, Everyone
Profile a single process	Administrators, Power Users	Administrators, Power Users
Force shutdown from a remote system	Administrators	Administrators
Restore files and directories	Administrators, Backup Ops	Administrators, Backup Ops
Manage audit and security logs	Administrators	Administrators
Log on as a service		
Shutdown the system	**Administrators, Backup Ops, Power Users, Users**	**Administrators, Backup Ops, Power Users**
Modify firmware environment variables	Administrators	Administrators
Profile system performance	Administrators	Administrators
Change system time	Administrators, Power Users	Administrators, Power Users
Take ownership of files or other objects	Administrators	Administrators
Act as part of the OS		
Deny Interactive Logon		
Deny Batch Logon		
Deny Service Logon		
Deny Network Logon		
Remove Computer from a Docking Station	Administrators, Power Users, Users	Administrators, Power Users, Users

Synchronize Directory Service Data		
Enable computer and user accounts to be trusted for delegation		

[1] The Guest account must be enabled before it is allowed to log on interactively.

Additional Power User Permissions

In addition to those capabilities permitted by the default ACLs and User rights, Power Users can also:

- Create local users and groups.
- Modify users and groups that they have created.
- Create and delete non-admin file shares.
- Create, manage, delete and share local printers.

Administrators can also perform all of these actions. In the case of account management however, Administrators can create, delete or modify any account, while Power Users can only modify or delete accounts that they themselves have created. Users cannot perform any of these additional Power User actions.

Default Group Membership

A significant difference between Windows NT 4.0 and Windows 2000 default security settings is the way access control is assigned in each version of the operating system. In computers running Windows NT 4.0, the Everyone group was used as a catchall for file system ACLs, registry ACLs, and User rights. In a sense, the Everyone group is not a traditional group because an Administrator cannot define who should and should not belong to the group. Instead, the Windows NT operating system or domain automatically controls the group membership so that everyone is a member of the Everyone group. If an administrator wanted more granular access control, the default ACLs would have to be modified in order to remove the Everyone group and add the groups which the administrator could control.

In the Windows 2000 operating system, a different philosophy is used. Groups such as Everyone and Authenticated Users whose membership is automatically configured by the operating system are not used to assign permissions (There are some exceptions. For example, the Everyone group is used to grant read access to some file system and registry objects for backward compatibility with applications requiring anonymous read access. Also, the interactive group is used on Service ACLs where access depends on how you are logged on to the system rather than who you are logged in as). Instead, only those groups whose membership can be controlled by an administrator are used. Primarily, these are the three user groups discussed in this paper: Users, Power Users, and Administrators.

The following table, Table 3, describes which users constitute the default membership in these groups. When a user is a member of a group, they automatically have the permissions that have been assigned to that group.

Table 3 Default members of groups

Local Group	**Default Workstation Members**	**Default Server Members**
Administrators	Administrator	Administrator
Power Users		
Users	Authenticated Users, Interactive Users	Authenticated Users, Interactive Users

By default, on computers with clean installations, the Authenticated Users group and the Interactive group are added to the Users group on Windows 2000 Professional and Windows 2000 Server-based computers. Membership in the Authenticated Users and Interactive groups is automatically controlled by the operating system.

Authenticated Users is the same as the Everyone group except it does not contain anonymous users. Interactive includes anyone who is locally logged on to the system rather than connected over the network.

Since there are no members of the Power Users group by default, non-administrative users that log on to a Windows 2000-based computer that has been clean-installed onto an NTFS partion will automatically be subject to a secure access control policy. Although these users can run any certified Windows 2000-based application (http://msdn.microsoft.com/certification/default.asp), it is likely that they will not be able to successfully run non-certified legacy applications. In order to run legacy applications, one of two things must happen:

- The Users must be added to the Power Users group
- The default security granted to Users must be loosened up

Since Power Users have at least the same access that Windows NT 4.0 Users had, any application that ran as a User on a Windows NT 4.0-based system should run as a Power User on Windows 2000-based system.

Finally, when a workstation or server joins a domain, the same domain groups that were added to Windows NT 4.0 local groups are added to Windows 2000-based local groups. Specifically, Domain Administrators and Domain Users are added to the local Administrators and local Users groups respectively upon joining the domain.

Summary

A significant portion of the Windows 2000 operating system security is defined by the access permissions granted to three groups: Administrators, Power Users, and Users. By default, on clean-installed NTFS systems, Administrators have complete access to critical operating system components while Users have read access (or less). These default access control settings defined for members of the (non-administrative, non-power) Users group provides a standard, secure Windows-based environment that application developers can target and which is easily testable.

Applications that satisfy the Windows 2000 Application Specification (http://msdn.microsoft.com/certification/default.asp) can run successfully in the normal Users context. Non-certified legacy applications are likely to require increased access such as that granted to Power Users in order to run. Thus, the single most important action customers can take to secure their desktops is to deploy certified applications that can run successfully in the Users context. Until such applications are deployed, the Power Users group provides a convenient, but insecure, backward compatibility mechanism for legacy applications that do not run successfully as a Windows 2000-based User.

Frequently Asked Questions

What do the Windows 2000 default security settings mean for developers, testers, and system administrators?

If you are a developer, make sure your code meets the Windows 2000 Application Specification, specifically Chapter 4: "Data and Settings Management." Meeting these requirements offers customers maximum security without loss of application functionality and can be marketed as such.

If you are a tester, make sure the application you are testing meets the Windows 2000 Application Specification requirements, specifically Chapter 4: "Data and Settings Management." Testing the run-time aspects of the application is straightforward:

1. Perform a clean installation of the Windows 2000 operating system on an NTFS partition (join a domain as necessary).
2. Log on as an Administrator.
3. Install the application into the Program Files directory.
4. Create a test user account (non-administrative).
5. Log on as the test user created in step 4.
6. Run the application.

If you are a system administrator, contact the in-house developers or independent software vendors for each of the applications that are supported in your environment. The Windows 2000 operating system defines a standard secure platform that any developer can target and which is easily tested. Applications are required that can run successfully on this platform. As applications that can successfully run as User are deployed, users can be moved from the Power Users group into the Users group, resulting in significant improvements in security, reliability, and management. Applications that meet the Windows 2000 Application Specification requirements, specifically Chapter 4: "Data and Settings Management," will successfully run as User.

How can I synchronize upgraded computers with Windows 2000 default security settings?

Since the security on upgraded computers is not modified during Windows 2000 setup, the default security settings must be applied by an administrator after setup has completed: From the **%windir%\security\templates** directory, the following command can be run on workstations:

```
Secedit /configure /cfg basicwk.inf /db basicwk.sdb /log basicwk.log
/verbose
```

For servers, the default security settings are defined in basicsv.inf:

```
Secedit /configure /cfg basicsv.inf /db basicsv.sdb /log basicsv.log
/verbose
```

The basic configuration files will apply all default security settings except for User Rights and Group Membership.

The file system that the Windows 2000 operating system is installed on must be NTFS in order to obtain the default file system ACLs.

Why is the root directory not secure by default?

Setup does not change the permissions on the root directory because the Windows 2000 ACL Inheritance model would recursively try to configure all subdirectories of the root. This could result in undesired changes for non-Windows 2000-based directories that may exist on the install partition. As a result, administrators should configure root directory security according to their own system configurations and application requirements.

How will Windows 2000 default security settings impact legacy desktop applications?

Legacy desktop applications that ran under a User context on computers running Windows NT 4.0 will more than likely have to run under a Power User context on a Windows 2000-based system. By default, non-administrative Users that log onto clean-installed Windows 2000 computers are members of the Users group, so an administrator will need to add these users to the less secure Power Users group in order to run non-certified legacy applications. Applications that meet the Windows 2000 application specification do not require Power User capabilities in order to run successfully.

How will Windows 2000 default security settings impact legacy server-based applications?

Server based applications that ran under a User context on computers running Windows NT 4.0 will more than likely need to run under a Power User context in a Windows 2000-based system. Thus, the service accounts for such applications should be added to the Power Users group on Windows 2000 Server platforms in order to achieve backward compatibility with the Windows NT 4.0-based environment.

Service accounts that ran as local system or under an administrative context are not impacted by the default security settings.

What applications can successfully run as user?

Any application that meets the Windows 2000 Application Specification, specifically Chapter 4: "Data and Settings Management ," will successfully run as User. The Windows 2000 Application Catalog (http://www.microsoft.com/windows/compatible/) may be consulted to determine which applications meet this requirement. Note that it is possible for an application to successfully run as User, but still not meet all of the other Windows 2000 Application Specification requirements.

Why define default security settings that few applications can run on?

The Internet has changed the threat landscape significantly. In response, customers are demanding secure environments in which to operate. Although the Windows NT operating system provides security mechanisms to meet these demands, these features often cannot be turned on because doing so causes problems for applications written on earlier versions of the Windows operating system. Providing a secure access control policy out of the box sets a standard that ISVs can target and that is easily testable. This, in conjunction with customer demand, will drive the development of security conscious applications necessary the security of any operating system environment. In short, for customers that have fully implemented the Windows 2000 operating system, an application that runs out of the box will have a competitive advantage over an application that does not. Furthermore, an application that runs out of the box on Windows 2000-based computers allows customers to easily secure their desktops simply by making sure that end-users are members of the Users group rather than Power Users or Administrators. Until such applications can be deployed, the Power Users group provides a convenient backward compatibility mechanism for running legacy applications.

What if I don't want end users to be Power Users when running legacy applications?

Some system administrators may consider the Power Users group too liberal because of the built-in permissions that members of the Power Users group have:

- Create local users and groups.
- Modify users and groups that they have created.
- Create and delete non-admin file shares.
- Create, manage, delete and share local printers.

All other additional rights, such as Change System Time, or Stop and Start non-autostarted services, can be reconfigured for the Power User by modifying the appropriate user rights or configuring the appropriate ACL.

Since there is no way to disable the built-in permissions allotted to Power Users, administrators who need to support non-certified legacy applications must loosen up the permissions allotted to members of the Users group to the point where their installed base of applications can be successfully run. The Windows 2000 operating system includes a security template for precisely this purpose. The template is named compatws.inf and can be found in the %windir%\security\templates directory. The template can be applied to a system using the Security Configuration Toolset. For example, the secedit.exe command line component of the Toolset can apply the template as follows:

```
secedit /configure /cfg compatws.inf /db compatws.sdb
```

This template loosens up security for Users in a matter consistent with the requirements of most legacy applications.

What can an Administrator do that a Power User can't?

By default, an administrator can:

- Install the operating system.
- Install or configure hardware device drivers, although Power Users are allowed to install Print Drivers.
- Install system services.
- Install Service Packs, hotfixes, and Windows Updates.
- Upgrade the operating system.
- Repair the operating system.

- Install applications that modify Windows system files.
- Configure password policy.
- Configure audit policy.
- Manage security logs.
- Create administrative shares.
- Create administrative accounts.
- Modify groups or accounts created by other users.
- Remotely access the registry.
- Stop or start any service.
- Configure services.
- Increase quotas.
- Increase execution priorities
- Remotely shutdown the system.
- Take ownership of arbitrary objects.
- Assign User rights.
- Override a locked computer.
- Format a hard drive.
- Modify system-wide environment variable's
- Access other Users' private data.
- Backup and restore files.

What can a Power User do that a User can't?

A Power User can:

- Create local users and groups.
- Modify users and groups that they have created.
- Create and delete non-administrator file shares.
- Create, manage, delete and share local printers.
- Change system time (default user right).
- Stop or start non auto-started services.

By default, Power Users also have

- Modify access to the Program Files directory.
- Modify access to many locations within the **HKEY_LOCAL_MACHINE \Software** registry hive.
- Write access to most system directories including **%windir%** and **%windir%\system32**.

These permissions allow Power Users to

- Perform per-computer installation of many applications. For example, applications that do not modify Windows system files or do not modify HKEY_LOCAL_MACHINE \System.
- Run legacy applications that improperly store per-user data in per-computer locations (without receiving error messages).

Unfortunately, these permissions are also the same permissions that allow Power Users to

- Plant Trojan horses that, if executed by administrators or other users, can compromise system and data security.

- Make system-wide operating system and application changes that affect other users of the system.

Can Users install applications?

Users cannot install applications per computer, because they cannot write to system-wide locations. However, there is no reason why a (non-administrator, non-power) User cannot install an application per user, provided that the application setup program supports this. Such an application would have to be installed in the User's Profile directory, and would have to modify only **HKEY_CURRENT_USER** registry settings and per-user Start menu items. As a result, only the User who installed the application can run that application. This is the only secure way to allow untrusted users to install applications.

Is it possible to easily switch between user contexts?

Yes, because administrators have complete control over the operating system, it is critical that system administrators avoid logging in as an administrator when performing non-administrative tasks. This can protect your system from malicious code executing under the privileged security context. The most common scenario is downloading and executing code from the Internet.

To promote running under a least privileged context, the Windows 2000 operating system provides a convenient tool that allows administrators to log on as a User or Power User, then start trusted administrative programs under an administrative context without having to log off and log back on. The tool is called RUNAS.EXE. As an example, to start a command window under the administrators context:

```
RUNAS /u:computername\administrator cmd
```

Applications started from this command window inherit the parent's access token. Runas is also integrated into the Windows 2000 shell so that programs and shortcuts to programs can be started from the user interface under a different user's context. To use Runas from the shell, select an executable, and press Shift+Right Click.

What about domain controllers?

Domain controllers support a broader range of built-in groups than workstations or servers. For example, domain controllers support the notion of Account Operators and Print Operators. Rather than granting default access permissions to all of the Domain Controller built-in groups, file system and registry access on Domain Controllers is primarily granted to

- Authenticated Users
- Server Operators
- Administrators

Authenticated users, whether they are Account Operators, or Print Operators, or any normal User remotely accessing the domain controller, have the same restricted default permissions that Users have on workstations or servers (that is, Read access to System Locations, Full Control over their own profile and HKCU).

Server Operators on domain controllers are much more powerful than Power Users are on workstations or servers. For example, Server Operators can replace Windows System files and thus must be completely trusted users.

Note that the Power Users group does not exist in domain controllers, thus there is no backward compatibility mechanism for applications that ran under a User context on Windows NT 4.0-based domain controllers. In Microsoft does not recommend running applications on computers configured as domain controllers, and certainly not applications that require more than Authenticated User privileges in order to run successfully.

Appendix A: Default File System ACLs for Power Users and Users

Table 4 describes the default access control settings that are applied to file system objects for Power Users and Users during a clean installation of the Windows 2000 operating system onto an NTFS partition. For directories, unless otherwise stated (in parentheses), the permissions apply to the directory, subdirectories, and files.

- **%systemdir%** refers to **%windir%\system32**.
- *.* refers to the files (not directories) contained in a directory.
- RX means Read and Execute.

Table 4 Default Access Control Settings for File System Objects

File System Object	Default Power User Permissions	Default User Permissions
c:\boot.ini	RX	None
c:\ntdetect.com	RX	None
c:\ntldr	RX	None
c:\ntbootdd.sys	RX	None
c:\autoexec.bat	Modify	RX
c:\config.sys	Modify	RX
\ProgramFiles	Modify	RX
%windir%	Modify	RX
%windir%*.*	RX	RX
%windir%\config\*.*	RX	RX
%windir%\cursors\*.*	RX	RX
%windir%\Temp	Modify	Synchronize, Traverse, Add File, Add Subdir
%windir%\repair	Modify	List
%windir%\addins	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\Connection Wizard	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\fonts\*.*	RX	RX
%windir%\help\*.*	RX	RX
%windir%\inf\*.*	RX	RX
%windir%\java	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\media\*.*	RX	RX
%windir%\msagent	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\security	RX	RX
%windir%\speech	Modify (Dir\Subdirs) RX (Files)	RX
%windir%\system\*.*	Read, Execute	RX
%windir%\twain_32	Modify (Dir\Subdirs) RX (Files)	RX

%windir%\Web	Modify (Dir\Subdirs) RX (Files)	RX
%systemdir%	Modify	RX
%systemdir%*.*	RX	RX
%systemdir%\config	List	List
%systemdir%\dhcp	RX	RX
%systemdir%\dllcache	None	None
%systemdir%\drivers	RX	RX
%systemdir%\CatRoot	Modify (Dir\Subdirs) RX (Files)	RX
%systemdir%\ias	Modify (Dir\Subdirs) RX (Files)	RX
%systemdir%\mui	Modify (Dir\Subdirs) RX (Files)	RX
%systemdir%\OS2\*.*	RX	RX
%systemdir%\OS2\DLL\*.*	RX	RX
%systemdir%\RAS\*.*	RX	RX
%systemdir%\ShellExt	Modify (Dir\Subdirs) RX (Files)	RX
%systemdir%\Viewers\*.*	RX	RX
%systemdir%\wbem	Modify (Dir\Subdirs) RX (Files)	RX
%systemdir%\wbem\mof	Modify	RX
%UserProfile%	Full Control	Full Control
All Users	Modify	Read
All Users\Documents	Modify	Read, Create File
All Users\Application Data	Modify	Read

Note that a Power User can write new files into the following directories, but cannot modify the files that are installed there during text-mode setup. Furthermore, all other Power Users inherit Modify permissions on files created in these directories.

- **%windir%**
- **%windir%\config**
- **%windir%\cursors**
- **%windir%\fonts**
- **%windir%\help**
- **%windir%\inf**
- **%windir%\media**
- **%windir%\system**
- **%systemdir%**

- **%systemdir%\OS2**
- **%systemdir%\OS2\DLL**
- **%systemdir%\RAS**
- **%systemdir%\Viewers**

For directories designated as [Modify (Dir\Subdirs) RX (Files)], Power Users can write new files, however, other Power Users will only have Read access to those files.

Appendix B: Default Registry ACLs for Power Users and Users

Table 5 describes the default access control settings that are applied to registry objects for Power Users and Users during a clean installation of the Windows 2000 operating system. For a given object, permissions apply to that object and all child objects unless the child object is also listed in the table.

Table 5 Default Registry ACLs

Registry Object	**Default Power User Permissions**	**Default User Permissions**
HKEY_LOCAL_MACHINE		
HKLM\Software	**Modify**	**Read**
HKLM\SW\Classes\helpfile	Read	Read
HKLM\SW\Classes\.hlp	Read	Read
HKLM\SW\MS\Command Processor	Read	Read
HKLM\SW\MS\Cryptography	Read	Read
HKLM\SW\MS\Driver Signing	Read	Read
HKLM\SW\MS\EnterpriseCertificates	Read	Read
HKLM\SW\MS\Non-Driver Signing	Read	Read
HKLM\SW\MS\NetDDE	None	None
HKLM\SW\MS\Ole	Read	Read
HKLM\SW\MS\Rpc	Read	Read
HKLM\SW\MS\Secure	Read	Read
HKLM\SW\MS\SystemCertificates	Read	Read
HKLM\SW\MS\Windows\CV\RunOnce	Read	Read
HKLM\SW\MS\W NT\CV\DiskQuota	Read	Read
HKLM\SW\MS\W NT\CV\Drivers32	Read	Read
HKLM\SW\MS\W NT\CV\Font Drivers	Read	Read
HKLM\SW\MS\W NT\CV\FontMapper	Read	Read
HKLM\SW\MS\W NT\CV\Image File Execution Options	Read	Read
HKLM\SW\MS\W NT\CV\IniFileMapping	Read	Read
HKLM\SW\MS\W NT\CV\Perflib	Read (via Interactive)	Read (via Interactive)

HKLM\SW\MS\W NT\CV\SecEdit	Read	Read
HKLM\SW\MS\W NT\CV\Time Zones	Read	Read
HKLM\SW\MS\W NT\CV\Windows	Read	Read
HKLM\SW\MS\W NT\CV\Winlogon	Read	Read
HKLM\SW\MS\W NT\CV\AsrCommands	Read	Read
HKLM\SW\MS\W NT\CV\Classes	Read	Read
HKLM\SW\MS\W NT\CV\Console	Read	Read
HKLM\SW\MS\W NT\CV\ProfileList	Read	Read
HKLM\SW\MS\W NT\CV\Svchost	Read	Read
HKLM\SW\Policies	Read	Read
HKLM\System	**Read**	**Read**
HKLM\SYSTEM\CCS\Control\SecurePipeServers\winreg	None	None
HKLM\SYSTEM\CCS\Control\Session Manager\Executive	Modify	Read
HKLM\SYSTEM\CCS\Control\TimeZoneInformation	Modify	Read
HKLM\SYSTEM\CCS\Control\WMI\Security	None	None
HKLM\Hardware	**Read (via Everyone)**	**Read (via Everyone)**
HKLM\SAM	**Read (via Everyone)**	**Read (via Everyone)**
HKLM\Security	**None**	**None**
HKEY_USERS		
USERS\.DEFAULT	Read	Read
USERS\.DEFAULT\SW\MS\NetDDE	None	None
HKEY_CURRENT_CONFIG	= HKLM\System\CCS\HardwareProfiles\Current	
HKEY_CURRENT_USER	Full Control	Full Control
HKEY_CLASSES_ROOT	= HKLM\SW\Classes	

- HKLM = HKEY_LOCAL_MACHINE
- SW = Software
- MS = Microsoft
- CV = CurrentVersion
- CCS = CurrentControlSet
- W NT = Windows NT

For More Information

For the latest information on the Windows 2000 operating system, check out Microsoft TechNet or our World Wide Web site (http://www.microsoft.com/windows2000/guide/server/overview/default.asp), or the Windows 2000 Forum on the Microsoft Network (GO WORD: MSNTS).

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation.

Other product