## 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:

1. Install the operating system and components (including drivers for hardware, system services, and so forth).
2. Install Service Packs and hotfixes.
3. Install Windows updates.
4. Upgrade the operating system
5. Repair the operating system.
6. 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 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 Usersare 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:

1. Install and remove applications per computer that do not install system services.
2. 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.

## Configuring Security During Setup

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

1. **%windir%\inf\defltwk.inf**
2. **%windir%\inf\defltsv.inf**
3. **%windir%\inf\defltdc.inf**

The default Windows 2000 permissions for file system, registry and service objects are also applied to upgraded machines using the following files:

* %windir%\inf\dwup.inf
* %windir%\inf\dsup.inf
* %windir%\inf\dcup.inf (NT4 DC Upgrade Only)

These security template files are applied by the [Security Configuration Toolset](http://www.microsoft.com/WINDOWS2000/library/howitworks/security/sctoolset.asp) at the beginning of GUI-mode setup. Security is applied during the upgrade process to ensure that Windows 2000 operating-specific objects are configured consistently regardless of whether the Windows 2000 machine was upgraded or clean-installed.

Security for optional component files installed during GUI-mode setup is applied at the end of GUI-mode setup using the following Security Configuration Toolset template: %windir%\inf\syscomp.inf

## 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**

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:

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

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 |
| %Windir%\Temp | Synchronize, Traverse, Add File, Add Subdir | Per-Machine temp directory. This location is 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. |

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 are required to 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 Table 2 below. 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[[1]](#footnote-1) | 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 |

Table 2, continued

|  |  |  |
| --- | --- | --- |
| User Right | Default Workstation | Default Server |
| 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 |  |  |

## Additional Power User Permissions

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

1. Create local users and groups.
2. Modify users and groups that they have created.
3. Create and delete non-admin file shares.
4. 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.

Table 3 below 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 | Members on Clean-Installed Workstation | Members on Upgraded Workstation | Members on Clean-Installed & Upgraded Server |
| Administrators | Administrator | Administrator | Administrator |
| Power Users |  | Authenticated Users, Interactive Users |  |
| Users | Authenticated Users, Interactive Users | Authenticated Users, Interactive Users | Authenticated Users, Interactive Users |

By default, the Authenticated Users group and the Interactivegroup 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.

Authenticated Users and Interactive are added to the Power Users group when a computer running Windows NT Workstation 4.0 is upgraded to Windows 2000 Professional. This allows non-certified applications which ran successfully under a user context on Windows NT 4 to continue running successfully under the backward compatible Power User context on Windows 2000. For clean-installed workstations and servers, as well as upgraded servers, there are no members of the Power Users group by default. Thus, non-administrative users that log on to a Windows 2000-based server, or a clean-installed Windows 2000-based workstation will automatically be subject to the secure access control policy granted to Users (assuming Windows 2000 was installed onto an NTFS partition). Although these users can run any certified Windows 2000-based application, 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, 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](http://msdn.microsoft.com//certification/default.asp) [Specification](http://msdn.microsoft.com//certification/default.asp), 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](http://msdn.microsoft.com//certification/default.asp) [2000 Application Specification](http://msdn.microsoft.com//certification/default.asp) 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. Point them to the [Windows 2000 Application Specification](http://msdn.microsoft.com//certification/default.asp). Deploying certified Windows 2000 applications will allow end users to be moved from the Power Users group into the Users group and is thus the single most significant action you can take to secure your Windows 2000 environment. Other aspects of the certification program (such as support for the Microsoft Installer) will also make

1. The Guest account must be enabled before it is allowed to log on interactively. [↑](#footnote-ref-1)