Microsoft Windows 2000 Networking

如對本課程有任何意見或投訴，請聯絡
課程管理委員會電話 2136-1936 或電郵至
supervisory@welkin.com.hk

Should you have any comment or complaint on
our training courses, please contact our
Training Administration Committee at 2136-1936 or email to
supervisory@welkin.com.hk

Table of Contents

1. Creating and Managing User Accounts

User accounts enable users to log on and gain access to local or domain resources. This module discusses how to create local and domain user accounts and set properties for them.

1.1. Introduction to User Accounts

A user account contains a user's unique credentials and enables a user to log on to the domain to gain access to network resources or to log on to a specific computer to access resources on that computer. Each person who regularly uses the network should have a user account.

The following table describes the types of user accounts that Microsoft Windows 2000 provides.

User account type	Description
Local user account	Enables a user to log on to a specific computer to gain access to resources on that computer. Users can gain access to resources on another computer if they have a separate account on the other computer. These user accounts reside in the Security Accounts Manager (SAM) of the computer.
Domain user account	Enables a user to log on to the domain to gain access to network resources. The user can gain access to network resources from any computer on the network with a single user account and password. These user accounts reside in the Active Directory ™ directory service.
Built-in user account	Enables a user to perform administrative tasks or to gain temporary access to network resources. There are two built-in user accounts that cannot be deleted: Administrator and Guest. The local Administrator and Guest user accounts reside in SAM and the domain Administrator and Guest user accounts reside in Active Directory. Built-in user accounts are automatically created during Windows 2000 installation and the installation of Active Directory.

1.2. Naming Conventions

The naming convention establishes how user accounts are identified in the domain. A consistent naming convention makes it easier to remember user logon names and locate them in lists. It is a good practice to adhere to the naming convention already in use in an existing network that supports a large number of users.

Consider the following guidelines for naming conventions:

- Domain user accounts must be unique in Active Directory. Domain user account full names must be unique within the domain in which you create the user account.
- Local user account names must be unique on the computer on which you create the local user account.

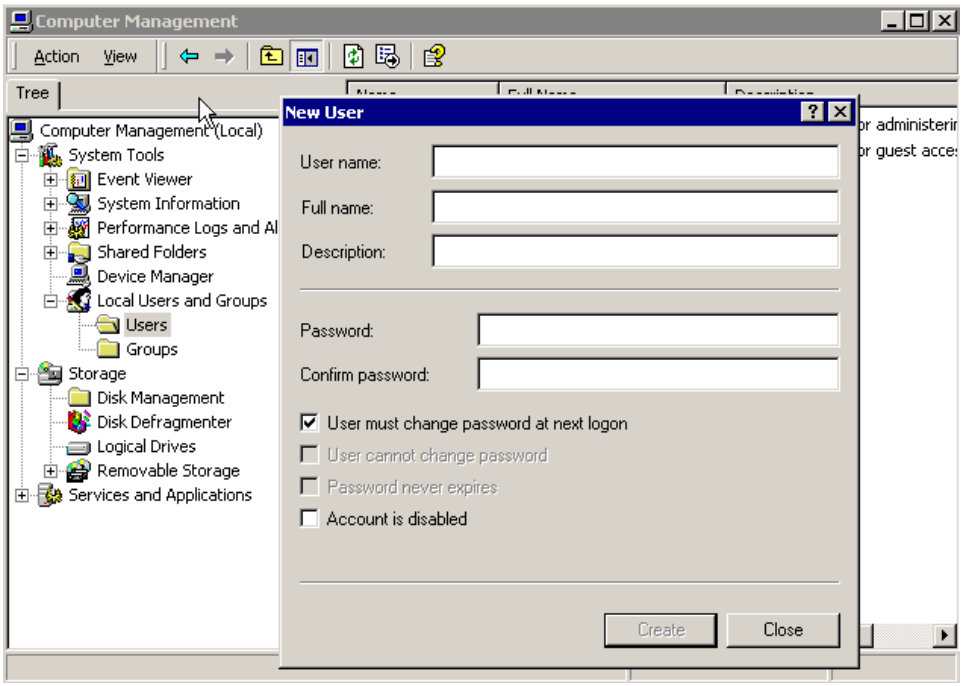
- User logon names can contain up to 20 uppercase and lowercase characters (the field accepts more than 20 characters, but Windows 2000 recognizes only 20), except for the following:

  " / \ [ ] : ; | = , + * ? < >

  You can use a combination of special and alphanumeric characters to help uniquely identify user accounts.
- Your naming convention for logon names should accommodate staffs with duplicate names if you have a large number of users.

1.3. Creating Local User Accounts

Use Computer Management to create a local user account. You can create local user accounts on Windows 2000 Professional, stand-alone or member servers running Windows 2000 Server or Windows 2000 Advanced Server. You cannot create local account on Domain Controller.



1.4. Creating and Configuring Domain User Accounts

Creating Local User Accounts

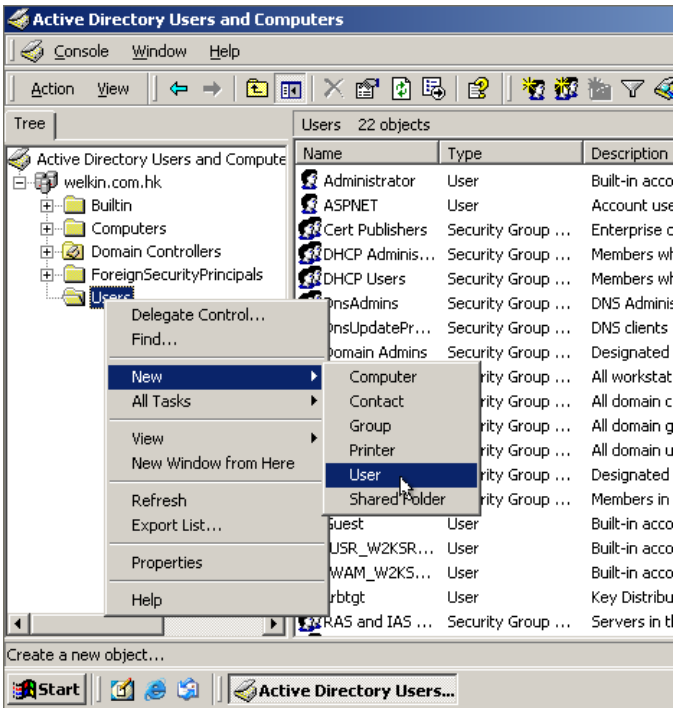
To create a local user account, perform the following steps:

- Click **Start**, point to **Programs**, point to **Administrative Tools**, and then click **Computer Management**.
- In **Computer Management**, expand **Local Users and Groups**.
- Right-click the **Users** folder, and then click **New User**.

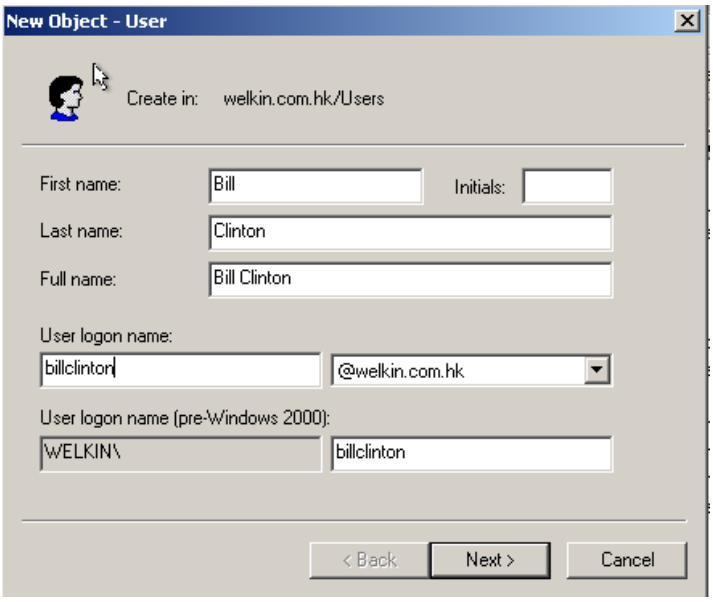
The following table describes the user information you provide for a local user account.

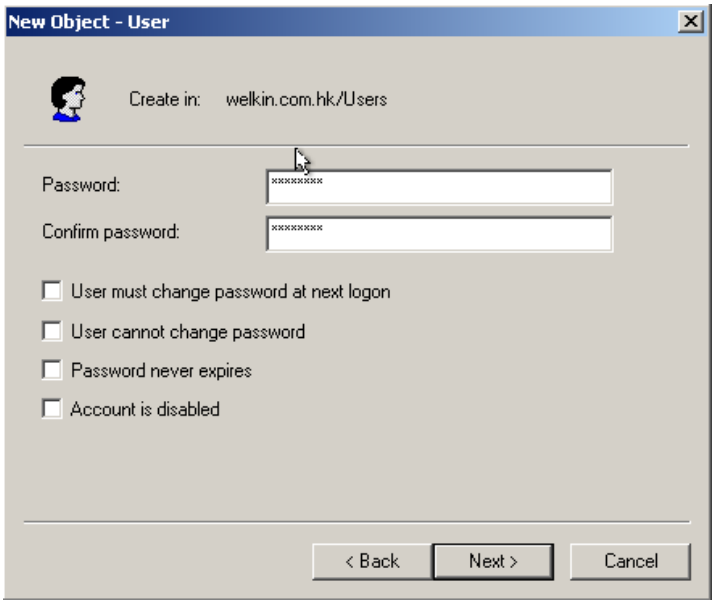
Option	Description
User name	The user's unique logon name, based on your naming convention..
Full name	The user's complete name. Use this to determine to which person the local user account belongs
Description	A description that you can use to identify the user by job title, department, or office location. This field is optional.

- In the **Password** and **Confirm Password** boxes, type the user's password.
- Select the appropriate check box or check boxes to set the password restrictions.
- Click **Create** to create the user account.

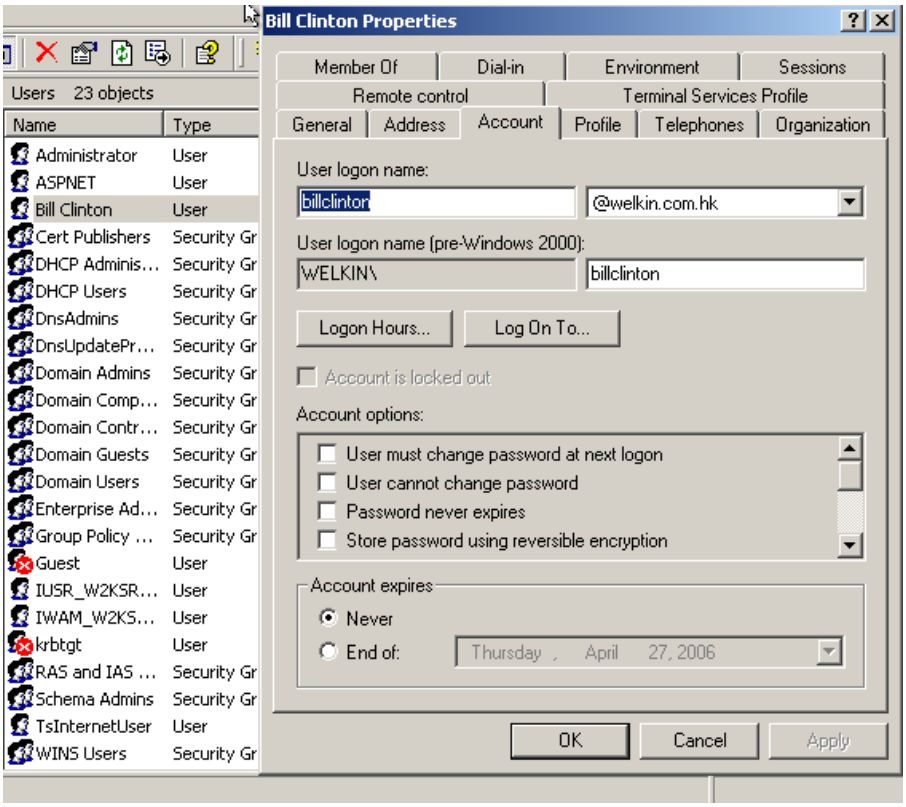


- Open Active Directory Users and Computers from the **Administrative Tools** menu, and then expand the domain in which you want to add the user account.
- Right-click the folder that will contain the user account, point to **New**, and then click **User**.





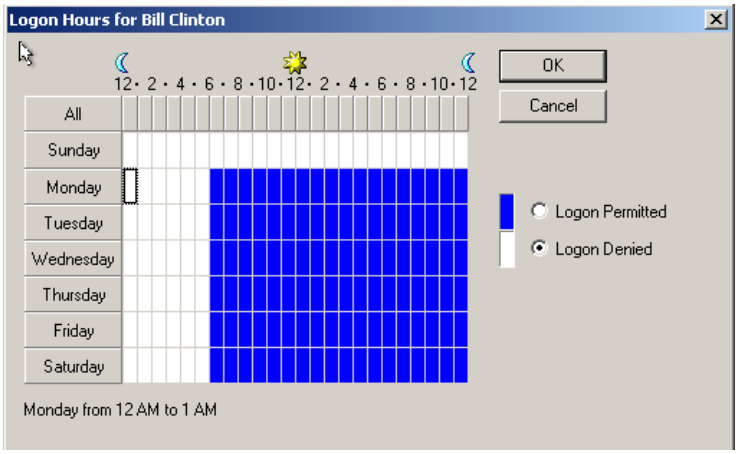
1.5. Setting Properties for Domain User Accounts



After you create a domain user account, you can configure personal and account properties, logon options, and dial-up settings, etc.

You can use the properties that you define for a domain user account to search for users in Active Directory. For example, you can search for a person by a telephone number, office location, manager's name, or last name. For this reason, you should provide detailed property definitions for each domain user account that you create.

1.6. Logon Hours



Setting logon options for a domain user account allows you to control the hours during which a user can log on to the domain, in addition to the computers from which a user can log on to the domain. These are settings you gain access to from the **Account** tab.

2. Managing Access to Resources by Using Groups

A group is a collection of user accounts. You use groups to simplify the management of user and computer access to shared resources. Groups allow you to grant access permissions to multiple users at one time. After you grant the access permission to a group, you add members to the group that require the permissions.

2.1. Introduction to Windows 2000 Groups

Before you can use groups effectively, you need to understand their basic purpose and have an overview of how they function in a workgroup or a domain. Where you create and use groups varies depending upon whether you are using them in a workgroup or a domain. For example, in a workgroup you can only use a group on the computer where the group resides. In addition, where a group resides varies depending upon whether it is used in a workgroup or a domain.

2.2. Implementing Groups in a Workgroup

You implement local groups when you implement groups in a workgroup. You can create local groups only on member servers and on computers running Windows 2000 Professional and you use them to assign permissions to resources only on the local computer.

In addition to the groups you create, Windows 2000 provides default groups with specific rights to perform system tasks on the local computer. You simply add users to these groups. There is a group strategy to help you efficiently create and use groups.

Local Groups

The Guidelines for Local Groups:

- Use local groups on computers that do not belong to a domain
- Use local groups to control access to resources and who can perform system tasks on the local computer

Membership Rules for Local Groups:

- Local groups can only contain local user accounts that are on the local computer
- Local groups cannot be a member of any other group

2.3. Built-in Local Groups

Built-in Local Groups:

- Members have rights to perform system tasks
- User accounts can be added

Special Identities (Special Groups):

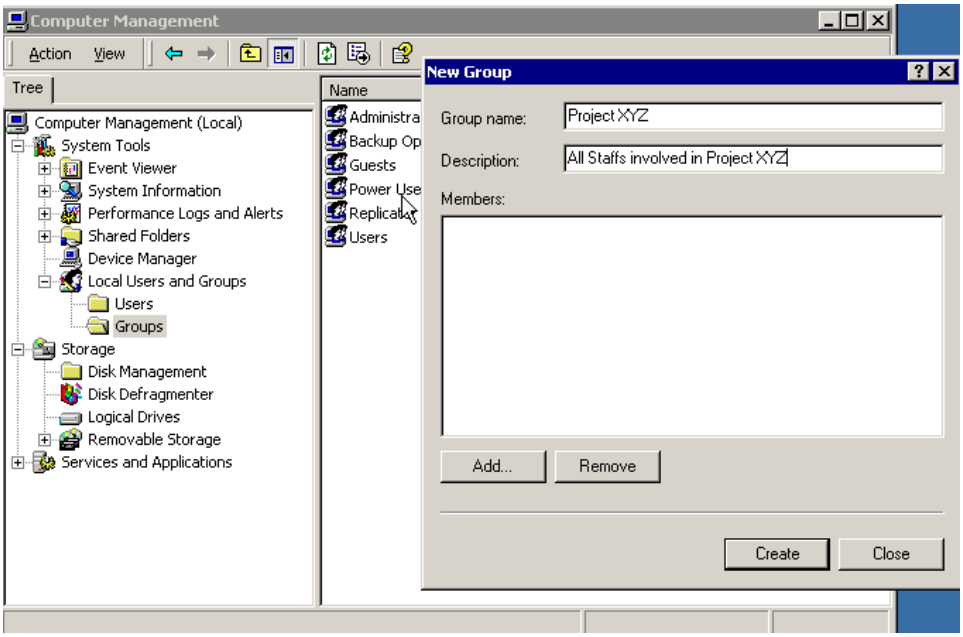
- Organize users for system use
- Have automatic membership that cannot be modified

The Strategy of using Local Groups in a Workgroup

This method is known as the ALP strategy:

- Place user accounts (A) in a local group (L) on the computer on which the resources reside or on which you want the users to perform system tasks.
- Grant permissions (P) or grant rights to the local group on the computer on which the network resource resides or on which the system tasks are to be performed.

2.4. Creating Local Groups



- In Computer Management, expand **Local Users and Groups**.
- Right-click the **Groups** folder, and then click **New Group.**
- Click **Add** to add Members
- Click **Create** to create the local group.

2.5. Group Types and Scopes

In a domain, Active Directory provides support for different types of groups and group scopes. Because they are stored in Active Directory, you can use these groups on any computer in your network. The group type determines the type of tasks that you manage with the group. The group scope determines whether the group spans multiple domains or is limited to a single domain.

Each type of domain group has a scope attribute that identifies how the group is applied on the network.

Group Types

There are two group types in Active Directory, which are:

Security groups. Use security groups for security-related purposes, such as granting permissions to gain access to resources. You can also use them to send e-mail messages to multiple users. Sending an e-mail message to a group sends the message to all members of the group. Therefore, security groups share the capabilities of distribution groups.

Distribution groups. Applications use distribution groups as lists for non-security related functions, such as sending e-mail messages to groups of users. You cannot grant permissions to distribution groups. Even though security groups have all of the capabilities of distribution groups, distribution groups are still required, because some applications can only read distribution groups.

Because distribution groups reside in Active Directory, only applications that are designed to work with Active Directory can use them. For example, future versions of Microsoft Exchange Server will be able to use Windows 2000 groups as distribution lists for e-mail messages.

Group Scopes

The scope of a group determines where you use a group in the domains. The group scope affects group membership and group nesting. Nesting is adding a group to another group as a member. Windows 2000 provides three group scopes:

Global group scope. Use this group scope to organize users who share similar network access requirements. You can use a global group to grant permissions to gain access to resources that are located in any domain.

- Global groups have limited membership. Add user accounts and global groups only from the domain in which you create the global group.
- Global groups can be nested within other groups. This function allows you to add a global group to another global group in the same domain or to universal and domain local groups in the same or other domains.

Domain local group scope. Use this scope to grant permissions to domain resources that are located in the same domain in which you created the domain local group. The resource does not have to reside on a domain controller.

- Domain local groups have open membership. Add user accounts, universal groups, and global groups from any domain.
- Domain local groups can contain other domain local groups from their domain, in addition to global groups and universal groups from any domain.

Universal group scope. Grant permissions to related resources in multiple domains. Use a universal group to grant access permissions to resources that are located in any domain.

- Universal groups have open membership. All domain user accounts and groups can be members.
- Universal groups can be nested within other domain groups. This capability allows you to add a universal group to domain local or universal groups in any domain.

2.6. The Strategy for Using Groups in a Single Domain

When you use groups in a single domain, you use the *A G DL P* strategy. The A G DL P strategy is: You put user accounts (A) into global groups (G), put the global groups into domain local groups (DL), and then grant permissions (P) to the domain local group.

When setting up the groups, use the following strategy:

- Identify users with common responsibilities and add the user accounts to a global group. For example, in a sales department, add user accounts for all sales staffs that use the same resources to a global group called Sales.
- Determine whether you can use a built-in domain local group, or if you need to create one to provide users with access to domain resources. For example, if you want users to be able to print to a shared color printer in the domain, create a domain local group called Color Printer Users.
- Make all global groups that share the same access needs for resources members of the appropriate domain local group. For example, add the appropriate global groups, including Sales, to the domain local group Color Printer Users.
- Grant the required permissions to the domain local group on the domain controller. You grant permissions at the resource. For example, grant the necessary permissions to use color printers to the Color Printers Users domain local group.

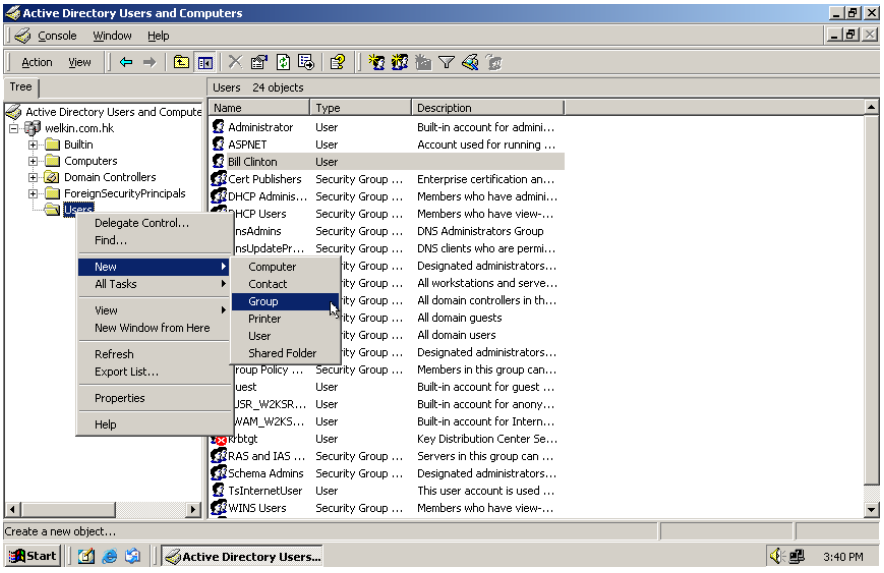
2.7. Creating and Deleting Domain Groups

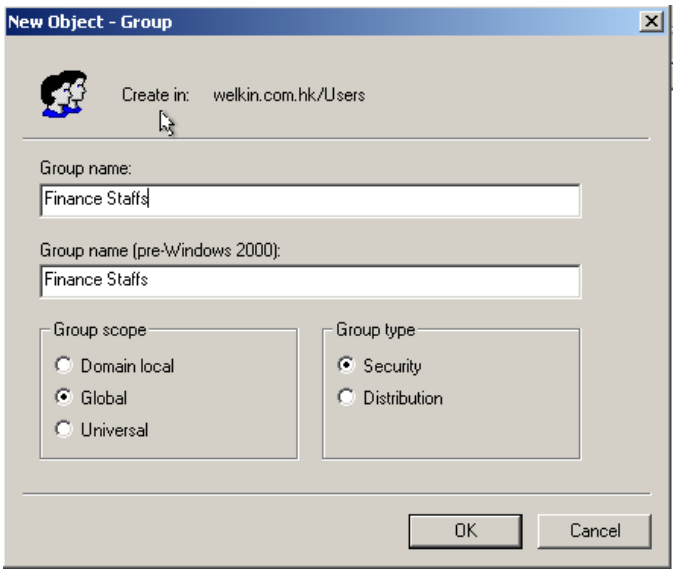
The Active Directory Users and Computers tool is the primary tool to create, delete and manage users and groups. You can create them in the default Users folder or in any folder that you create.

To avoid accidentally grant permissions to a unused group, be sure to delete it.

Creating a Group

To create a group, open Active Directory Users and Computers. Right-click the folder in which you want to create a group, point to **New**, and then click **Group**.





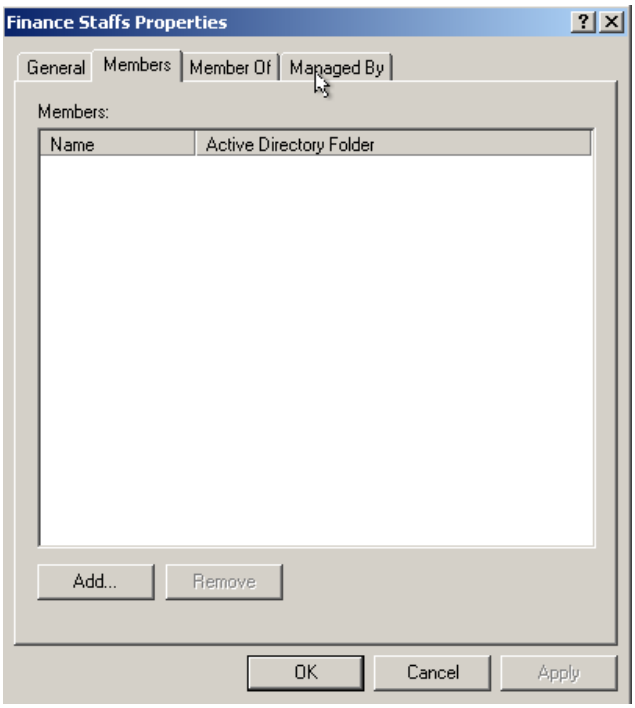
Deleting a Group

When you delete a group, you remove the permissions and rights that are associated with it. Deleting a group does not delete the user accounts or groups that are members of the group.

Each group that you create has a unique, non-reusable identifier, called the security identifier (SID). Windows 2000 uses the SID to identify the group and the permissions that are granted to it. When you delete a group, Windows 2000 never uses the SID again, even if you create a new group with the same name as the group that you deleted. Therefore, you cannot restore access to resources by creating a group with the same name.

To delete a group, open Active Directory Users and Computers. In the console tree, expand the domain, and then click the folder that contains the group that you want to delete. In the details pane, right-click the group that you want to delete, and then click **Delete**.

2.8. Adding Members to Domain Groups



After you create a group, you can add members to that group. User accounts, Groups and Computer accounts can become members of a group. Use Active Directory Users and Computers to add members to a group.

To add members to a group, perform the following steps:

- In the **Properties** dialog box for the appropriate group, click the **Members** tab, and then click **Add**.
- In the **Look in** list, select a domain from which to display user accounts and groups. You can also select **Entire Directory** to view user accounts and groups from anywhere in Active Directory. When adding members, you can sort members by the name or the folder in which they reside. In the **Select Users, Contacts, Computers, or Groups** dialog box, click the appropriate column.
- In the **Name** column, select the user account or group that you want to add, and then click **Add**. You can also type the name of the user account or group that you want to add. Repeat this step to add additional user accounts or groups.
- Click **OK** to add the members to the group, and then click **OK** again. You can also add a user account or group to another group by using the **Member Of** tab in the **Properties** dialog box for that user account or group. Use this method to add the same user or group to multiple groups quickly.

3. Managing Data by Using NTFS

With Windows 2000 NTFS, you can grant permissions to folders and files in order to control the level of access that users have to resources. NTFS also allows users to compress data to save disk space. It has a disk quotas feature to allows administrator manage how much space users can allocate in the disk. In addition, NTFS allows you to encrypt file data on the physical hard disk using the Encrypting File System (EFS). It is important that you understand NTFS and its capabilities so that you can efficiently implement this feature of Windows 2000.

3.1. NTFS Permissions

You use NTFS permissions to specify which users, groups, and computers can access files and folders. NTFS permissions also dictate what users, groups, and computers can do with the contents of the file or folder.

NTFS Folder Permissions

You grant folder permissions to control access to folders and the files and subfolders that are contained within those folders. The following table lists the standard NTFS folder permissions that you can grant and the type of access that each permission provides.

NTFS folder permission	Allows the user to
Read	View files and subfolders in the folder and view folder attributes, ownership, and permissions.
Write	Create new files and subfolders within the folder, change folder attributes, and view folder ownership and permissions.
List Folder	Contents View the names of files and subfolders in the folder.
Read & Execute	Traverse folders, plus perform actions permitted by the Read permission and the List Folder Contents permission
Modify	Delete the folder and perform actions permitted by the Write permission and the Read & Execute permission.
Full Control	Change permissions, take ownership, delete subfolders and files, and perform actions permitted by all other NTFS folder permissions.

NFTS File Permissions

You grant file permissions to control access to files. The following table lists the standard NTFS file permissions that you can grant and the type of access that each permission provides to users.

NTFS file permission	Allows the user to
Read	Read the file, and view file attributes, ownership, and permissions.
Write	Overwrite the file, change file attributes, and view file ownership and permissions.
Read & Execute	Run applications and perform the actions permitted by the Read permission.
Modify	Modify and delete the file and perform the actions permitted by the Write permission and the Read & Execute permission.
Full Control	Change permissions, take ownership, and perform the actions permitted by all other NTFS file permissions.

When you format a partition with NTFS, Windows 2000 automatically grants the Full Control permission for the root folder to the Everyone group. By default, the Everyone group will have Full Control to all folders and files that are created in the root folder. To restrict access to authorized users, you should change the default permissions for folders and files that you create.

3.2. How Windows 2000 Applies NTFS Permissions

By default, when you configure permission for a folder, the users or groups have access to the subfolders and files contained in the folder. It is important that you understand how subfolders and files inherit NTFS permissions from parent folders so that you can use inheritance to propagate permissions to files and folders.

If you grant permissions to an individual user account or to a group of which the user is a member for a file or folder, then the user has multiple permissions for the same resource. There are rules and priorities that are associated with how NTFS combines multiple permissions. In addition, you can also affect permissions when you copy or move files and folders. It is recommended that you assign permissions to a resource by using A G DL P. In other words, assign permissions to a resource by using domain local groups instead of individual user accounts.

3.3. Multiple NTFS Permissions

If you grant NTFS permissions to an individual user account in addition to a group to which the user belongs, then you have granted multiple permissions to the user. There are rules for how NTFS combines these multiple permissions to produce the user's effective permission.

Permissions Are Cumulative

A user's effective permissions for a resource are the combination of the NTFS permissions that you grant to the individual user account and the NTFS permissions that you grant to the groups to which the user belongs. For example, if a user has the Read permission for a folder and is a member of a group with the Write permission for the same folder, then the user has both the Read and Write permissions for that folder.

File Permissions Are Separate From Folder Permissions

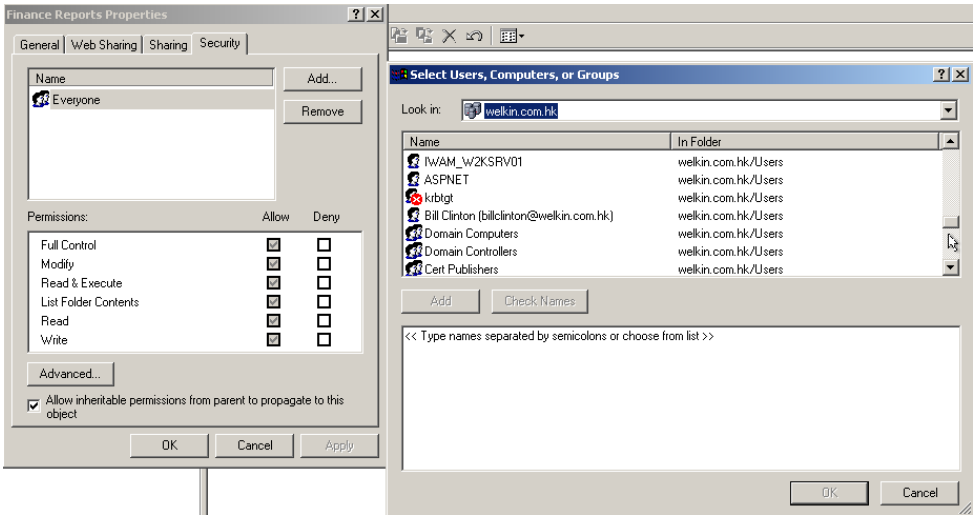
NTFS file permissions take priority over NTFS folder permissions. For example, a user with the Modify permission for a file will be able to make changes to the file even if he or she has only the Read permission for the folder containing the file.

Deny Overrides Other Permissions

You can deny access to a specific file or folder by granting the Deny permission to the user account or group. Even if a user has permission to access the file or folder as a member of a group, denying permission to the user blocks any other permission that the user has. Therefore, the Deny permission is an exception to the cumulative rule. You should avoid denying permission because it is easier to allow access to users and groups than to specifically deny access. It is preferable to structure groups and organize resources in folders so that allowing permissions is sufficient.

With Windows 2000, there is no difference between a user not having access, and specifically denying a user access by adding a deny entry to the ACL for the file or folder. This means that as an administrator, you have an alternative to denying access. Instead, you can simply choose to not allow a user access to a file or folder.

3.4. Granting NTFS Permissions

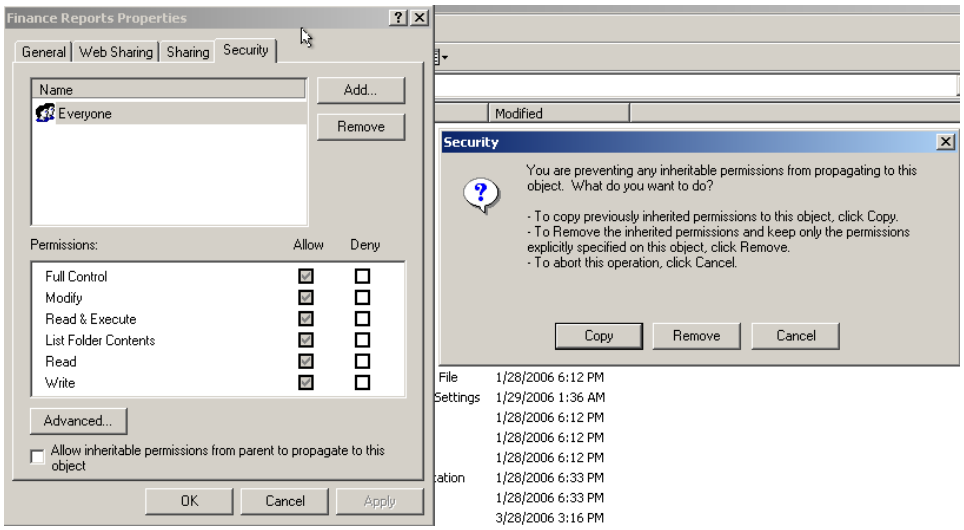


You grant NTFS permissions in the Properties dialog box for the folder. When you grant or modify NTFS permissions for a file or a folder, you can either add or remove users, groups, or computers for the file or folder. By selecting a user or group, you can modify the permissions for the user or group.

On the **Security** tab of the **Properties** dialog box for the file or folder, configure the options described in the following table.

Option	Description
Name	Selects the user account or group for which you want to change permissions or that you want to remove from the list.
Permissions	Allows a permission when you select the **Allow** check box. Denies a permission when you select the **Deny** check box.
Add	Opens the **Select User, Groups, or Computers** dialog box, which you use to select user accounts and groups to add to the **Name** list.
Remove	Removes the selected user account or group and the associated permissions for the file or folder.

3.5. Setting Permission Inheritance



In general, you should allow Windows 2000 to propagate permissions from a parent folder to subfolders and files contained in the parent folder. Permissions propagation simplifies the assignment of permissions for resources.

However, there are times when you may want to prevent permission inheritance. For example, you may need to keep all sales department files in one sales folder for which everyone in the sales department has the Write permission. However, you need to limit permissions for a few files in the folder to the Read permission only. To do this, you would prevent inheritance so that the Write permission does not propagate to the files contained in the folder.

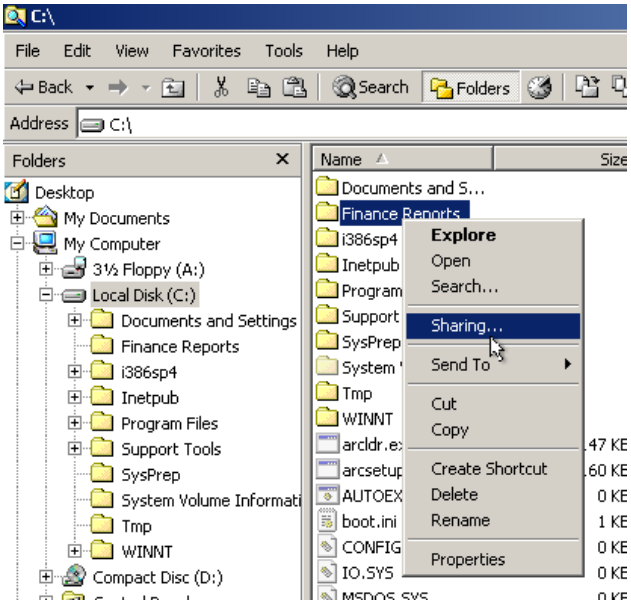
By default, subfolders and files inherit permissions that you grant for their parent folders, as shown on the **Security** tab in the **Properties** dialog box when the **Allow inheritable permissions from parent to propagate to this object** check box is selected.

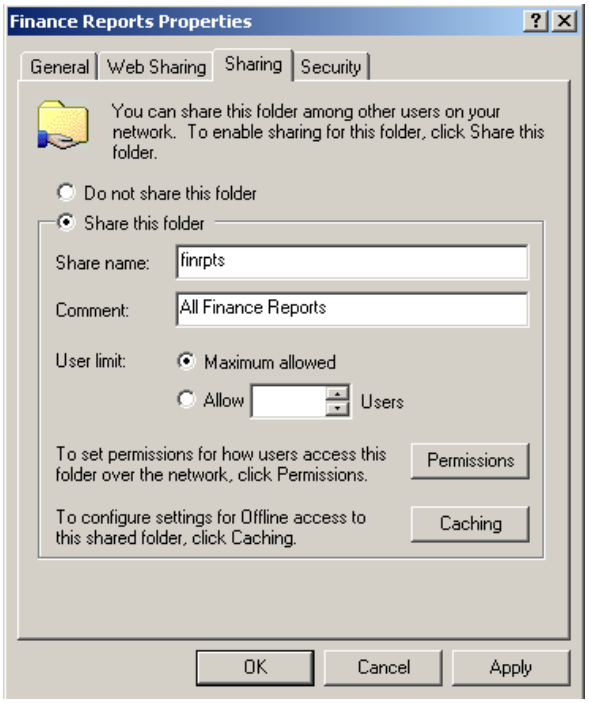
To prevent a subfolder or file from inheriting permissions from a parent folder, clear the **Allow inheritable permissions from parent to propagate to this object** check box, and then select one of the two options described in the following table.

Option	Description
Copy	Copies previously inherited permissions from the parent folder to the subfolder or file and denies subsequent permissions inheritance from the parent folder.
Remove	Removes the inherited permission that is granted for the parent folder from the subfolder or file and retains only the permissions that you explicitly grant for the subfolder or file.

4. Providing Network Access to File Resources

4.1. Sharing a Folder





When you share a folder, you give it a shared folder name, provide a comment to describe the folder and its contents, limit the number of users who have access to the folder, and grant permissions. You also have the option to share the same folder multiple times.

To create a shared folder, right-click the folder in Windows Explorer, and then click **Sharing**.

4.2. Shared Folder Permissions

Users can be granted or denied permission to shared folders. Shared folder permissions only apply to users who connect to the share over the network. They do not restrict access to users who log in locally to the computer where the files are stored and access the files locally. You can grant shared folder permissions to user accounts, groups, and computer accounts.

The Permissions

To control how users gain access to a shared folder, you use shared folder permissions. Shared folder permissions apply to folders that are shared, not to individual files. The following table describes what each of these permissions allows a user to do.

Permission	Allows the user to
Read	Display folder names, file names, file data, and attributes; run application files; and change folders within the shared folder.
Change	Create folders; add files to folders; change data in files; append data to files; change file attributes; delete folders and files; and perform actions permitted by the Read permission.
Full Control	Change file permissions; take ownership of files; and perform all tasks permitted by the Change and Read permission. By default, the Everyone group has this permission.

The default permissions of a share are that the Everyone group has Full Control. You should limit users' access to the share by using groups to assign either Change or Read permissions. Share permissions should always be used in conjunction with NTFS permissions.

Note: *Permissions are cumulative; Denying override other Permissions*

4.3. Combining NTFS and Shared Folder Permissions

When allowing access to network resources on NTFS partitions, it is recommended that you use the most secure NTFS permissions to control access to folders and files combined with the most secure shared folder permissions that allow network access.

When you share a folder on a partition formatted with NTFS, both the shared folder permissions and the NTFS permissions combine to secure file resources. NTFS permissions apply whether the resource is accessed locally or over a network. When you grant shared folder permissions on an NTFS volume, the following rules apply:

- NTFS permissions are required on NTFS volumes. By default, the Everyone groups has the Full Control permission.
- Users must have the appropriate NTFS permissions for each file and subfolder in a shared folder, in addition to shared folder permissions, in order to gain access to those resources.
- When you combine NTFS permissions and shared folder permissions, the resulting permission is the most restrictive permission of the combined shared folder permissions or the combined NTFS permissions.

5. Monitoring & Administrating Windows 2000

5.1. Overview

As an administrator, you perform a number of tasks to maintain an efficiently functioning network. These tasks include maintaining user accounts and printers, backing up and restoring data, and monitoring network activities.

To assist you in performing routine administrative tasks, Windows 2000 provides a set of administrative tools that simplifies the tasks by providing a user-friendly interface.

5.2. Administrative Tasks

As a network administrator, you provide users with access to the network, control the kind of access that each user has to network resources, and perform maintenance tasks. You create user accounts and assign permissions for users to access such resources as printers, applications, and data files.

You also manage the hardware and software installed on the computers as well as performs such tasks as creating printer shares and administering database and mail servers. Some of these routine tasks, such as backing up data on the servers, can be scheduled to run on a recurring basis automatically.

In this section, you will learn about the various routine tasks and the procedure for scheduling a task to run at a preset time.

Routine Administrative Tasks

A network administrator performs administrative tasks in the following areas: users and groups, printers, security, network events and resources, system integrity, backup and restoration, server applications, and disks.

Users and Groups

As an administrator, you assign and maintain user names and passwords for each user account. A user account enables the user to log on to a server to access network resources or to log on to an individual computer to access resources on that computer. You also create and maintain groups and define their membership. Organizing users into groups simplifies assigning permissions.

Printers

Administering printers includes setting up local and network printers and troubleshooting common printing problems, thereby ensuring that users can connect to and use printer resources easily.

Security

Maintaining network security involves planning, implementing, and enforcing a security policy for protecting data and shared network resources, including folders, files, and printers. By assigning user permissions, you can control access to resources. You determine who has access to specific resources and specify the kind of access that each user has.

Network Events and Resources

Monitoring network functioning is a very important task. Regular monitoring of the network can help detect a problem and resolve it before it causes the network to fail. Network monitoring includes evaluating resource usage and planning and implementing a policy for tracking security breaches.

System Integrity

Maintaining system integrity is critical to the network. The network administrator must regularly check the computers for the presence of computer viruses. A virus is a program that runs without your knowledge and may damage data. The administrator must safeguard the network by installing and updating anti-virus software regularly. In the event of the network being infected by a virus, the network administrator must take necessary steps to delete the virus from the network.

Backup and Restoration

One of the most important recurring tasks is backing up the data in the system. This task includes planning, scheduling, and performing regular backups to protect important data. Having a good backup system ensures that you can quickly locate and restore critical data that has been lost or damaged.

Server Applications

A system may run numerous server applications that require administration. For this purpose, there are specific tools that you use to administer application-based services, such as mail servers and database servers.

Disks

A computer's hard drive, or hard disk, is responsible for data storage. It is important to maintain these disks to ensure optimum performance and minimize the chances of data loss, while at the same time maintaining the data access speed. You verify the integrity of hard drives in terms of their reliability and configure them as part of your routine administrative tasks.

5.3. Administrative Tools

From managing user accounts and printers to monitoring resources for security purposes, the administrative tools provided by Windows 2000 help you perform a wide range of routine administrative tasks. You can access most of these tools from Control Panel.

This section discusses the most common tools used in administering a network. It dose not discuss all of the available tools.

Control Panel

Most of the administrative tools provided by Windows 2000 are available in Control Panel. Control Panel serves as a repository of tools that you can use to configure and monitor system settings. For example, using the tools in Control Panel, you can change the display on your monitor and modify security settings for a specific user.

To access Control Panel

- From the **Start** menu, point to **Settings**, and click **Control Panel**.

Registry

The registry reflects the changes that you make to the system when you use the tools in Control Panel. The registry is a database in which Windows 2000 stores configuration information pertaining to the system hardware and applications installed on the computer. Windows 2000 continually refers to this information during its operation.

Caution: *Do not make changes to the registry until you gain further knowledge and experience working with the registry.*

System Properties

System Properties is a tool you can use to view and change system properties on a local computer or on a remote computer.

Note: *To change certain system properties on a computer, you must have administrator privileges on the computer you are administering.*

To access the System Properties tool

- From **Control Panel**, open **System**.

5.4. System Properties

The System Properties tool organizes information in five areas that can be accessed from the following tabs:

General

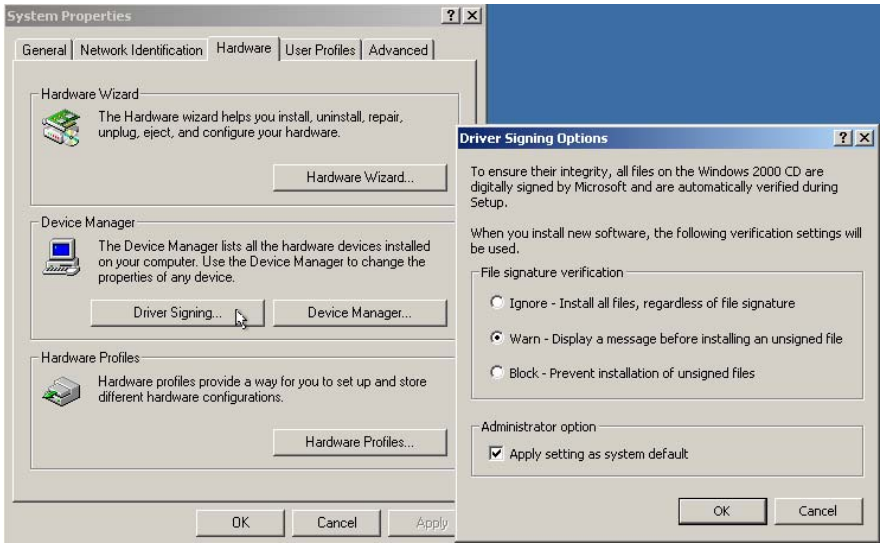
The General tab provides such information as the type of operating system running on the computer, the amount of memory installed, and to whom the computer is registered.

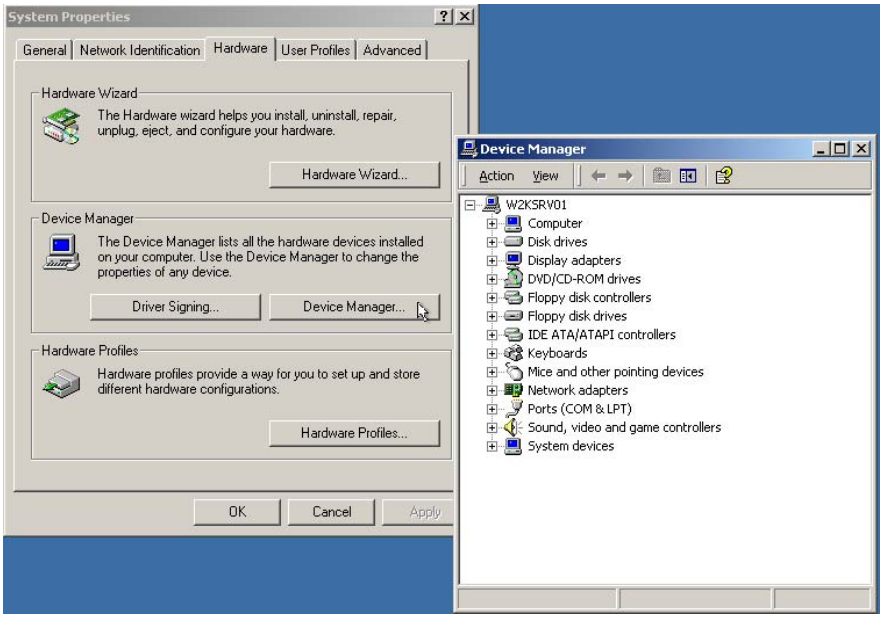
Network Identification

The Network Identification tab provides information about the name of the computer and the domain or workgroup to which it belongs. You can click Properties on the Network Identification tab to join a domain or to change the name of the computer and the domain or workgroup to which it belongs.

Hardware

The Hardware tab provides the Add/Remove Hardware wizard for installing, uninstalling, and managing computer hardware. It also provides Device Manager, a tool that you use to change the properties of any device, and Driver Signing, an option that allows you to set security levels for new software installation. Finally, Hardware Profiles enables you to set up and store different hardware configurations from which you can choose when starting the computer.



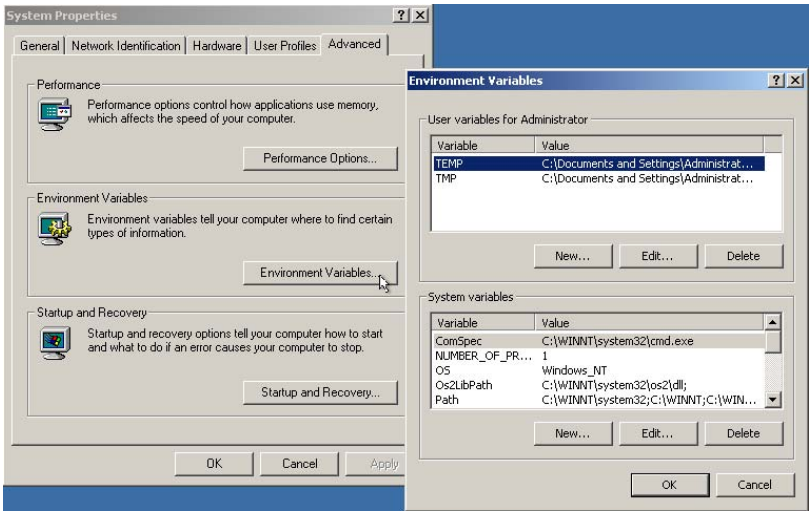


User Profiles

The User Profiles tab contains information about the different user profiles that exist on the computer. A profile contains information about a specific user's logon settings, such as desktop settings. Profiles are of two types: local and roaming. A local user profile is automatically created on each computer to which a user logs on. If the user has a roaming user profile, the same profile can be used on any other computer to which the user logs on.

Advanced

The Advanced tab provides three sets of options. Performance options control how the microprocessor is utilized when running applications, which affects the computer's speed. Environment variables assist in locating such information as the Windows system files. Startup and recovery options tell the computer how long to delay startup and what to do if an error causes the computer to stop running unexpectedly.



5.5. System Information

System Information displays a comprehensive view of the hardware, system components, and software environment.

To access System Information

- From **Control Panel**, open **Administrative Tools**, **Computer Management**, **System Tools**, and then **System Information**.

Organization of Information

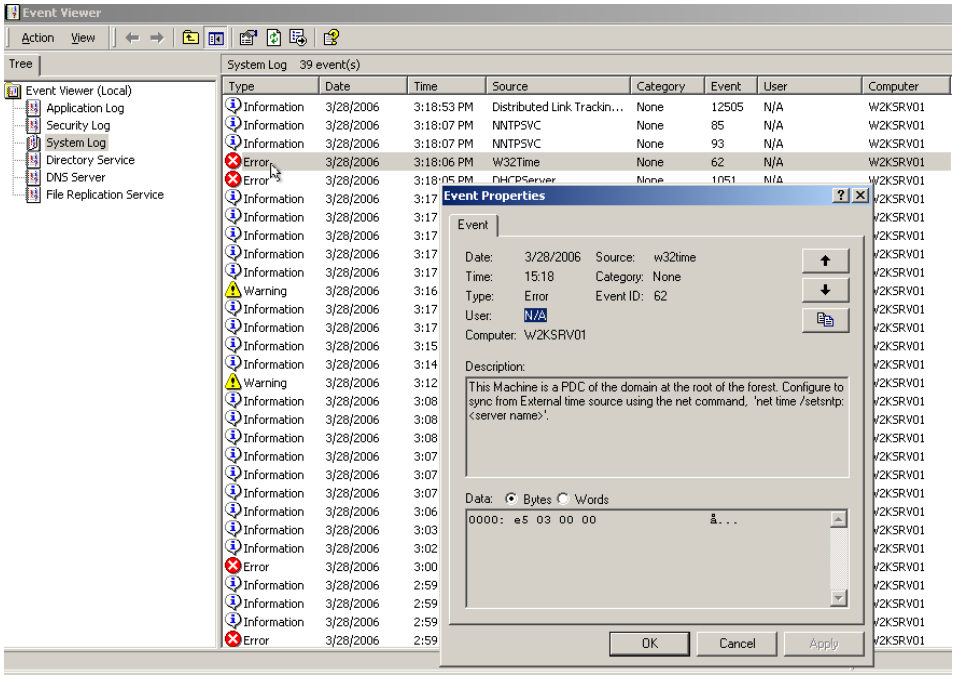
The displayed system information is organized into four top-level categories:

- **System Summary**
  System Summary folder includes information like computer name, processor name, and the version of the operating system and amount of memory installed on the computer.
- **Hardware Resources**
  The Hardware Resources folder includes subfolders that contain information about hardware settings and memory.
- **Components**
  Components folder includes subfolders that contain information about display settings, network and modem settings, and printer settings.
- **Software Environment**
  The Software Environment folder includes subfolders that contain information about currently running tasks, network connections, startup applications, and the drivers loaded in the system.

  When additional applications like Internet Explorer, are installed, the System Summary includes sections on versions and such application-specific settings as security settings for Internet Explorer.

Event Viewer

We can use Event Viewer to gathers information about hardware, software, system problems, and security events. An event is any important occurrence that happens in an application or within the operating system itself. Each time an event occurs, Windows 2000 records its occurrence in a log. Therefore, by using the event logs in Event Viewer, you can monitor the status of the system.



To access Event Viewer

- From Control Panel, open **Administrative Tools,** and then **Event Viewer**.

Types of Events

Event Viewer displays one of four types of events:

- **Error**
  Indicate a fatal problem, such as loss of data or functionality.
- **Warning**
  May indicate a possible future problem.
- **Information**
  Describe the successful operation of an application, driver, or service.
- **Auditing**
  Indicates whether an attempt to access an audited resource was a success or a failure.

Event Viewer then records the occurrences of these types of events in event logs. Different types of event logs are created depending on the additional components installed on the system. Some common event logs are the application log, the system log, and the security log.

Application Log

The application log contains events logged by applications. For example, a database application might record a file error in the application log. The application log records Error, Warning, and Information events.

System Log

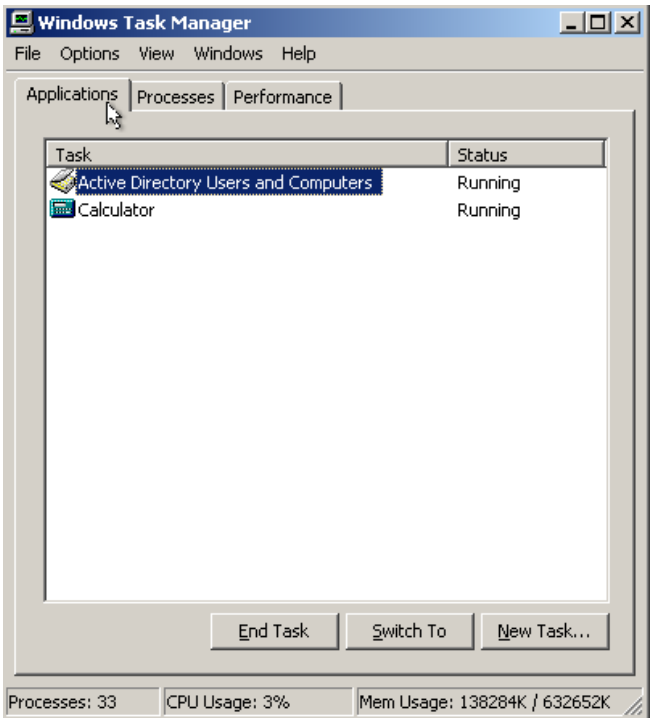
The system log contains events logged by Windows 2000 system components. For example, the system log records the failure of a system component to load during startup. The system log records Error, Warning, and Information events.

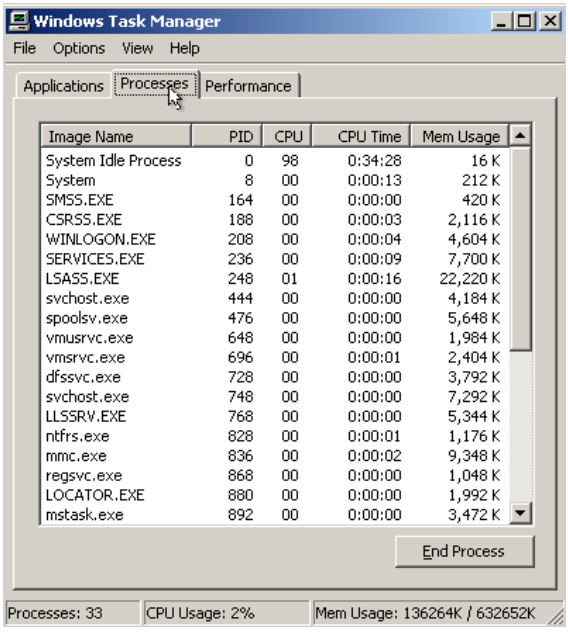
Security Log

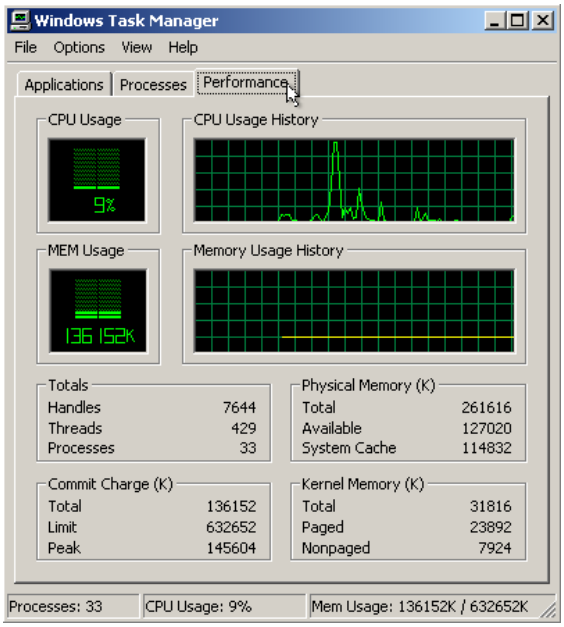
The security log records Auditing events, including valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files.

5.6. Windows Task Manager

Windows Task Manager provides information about computer performance and the applications and processes running on the computer. Using Windows Task Manager, you can start applications, end applications or processes, and view a dynamic display of your computer's performance.







To access Windows Task Manager

- Right-click an empty space on the taskbar, and then click **Task Manager**.

The information displayed by Windows Task Manager is organized into three tabs: **Applications, Processes,** and **Performance.**

- **Applications**
  Applications tab displays the status of the applications that are running on your computer. From this tab, you can end, switch to, or start an application.
- **Processes**
  The Processes tab displays information about the processes running on your computer. A process can be an application, such as Microsoft Windows Explorer, or a service, such as Event Log.

- **Performance**
  Performance tab displays a dynamic overview of your computer's performance, including the CPU and memory usage.

Performance

Monitoring system performance is an important part of maintaining and administering your Windows 2000-based installation. Windows Task Manager is a simple tool you use to monitor the performance of your computer and view general system information.

A more detailed version of Windows Task Manager is the Performance tool. This tool provides data that you use to monitor the performance of your computer or the performance of other computers on the network.

Performance Data

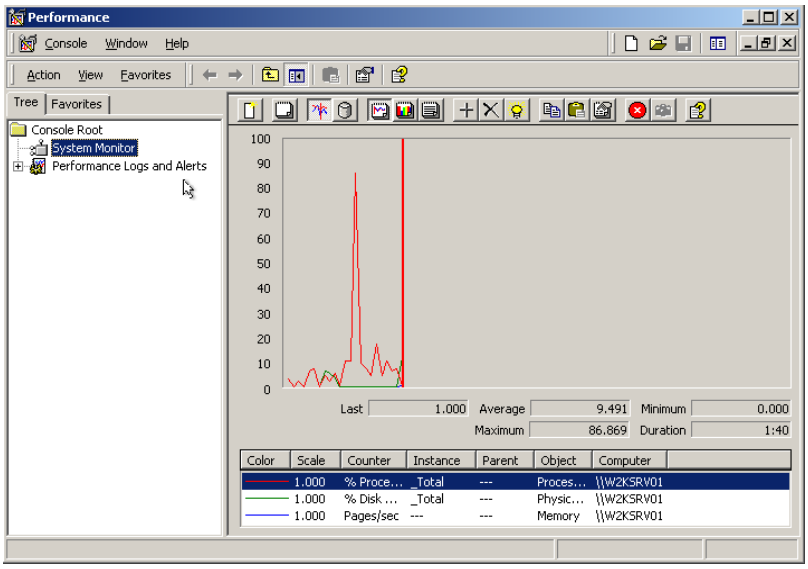
The data provided by the Performance tool is used to:

- Analyze changes in your workload and evaluate its corresponding effect on system resources.
- Observe changes and trends in workloads and resource usage so that you can plan for future system upgrades.
- Evaluate changes to system configuration by monitoring the results.
- Diagnose problems and target components or processes for improvement.

To access the Performance tool

From Control Panel, open **Administrative Tools**, and then **Performance**.

There are two tools provides by the Performance Console: System Monitor and Performance Logs and Alerts. These utilities provide detailed data about the resources used by specific components of the operating system and by other applications and services running on the system.



System Monitor

With System Monitor, you can:

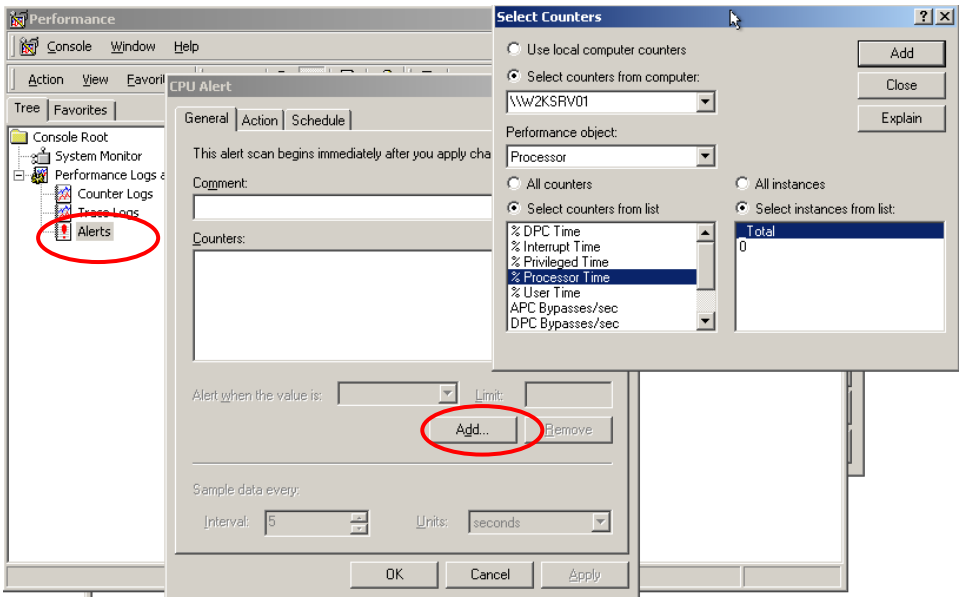
- Collect performance information on your computer and compare it with the performance of other computers on a network.

- Collect and view performance data being generated on a local computer or from several remote computers on the network.
- View data collected either currently or previously in a log file.
- Present data in a printable graph, histogram, or report view. The graph view is the default view and offers the widest variety of optional settings.
- Create a Web document from performance views.
- Create reusable monitoring configurations that can be installed on other computers.

Performance Logs and Alerts

The Performance Logs and Alerts utility:

- Supports the definition of performance objects, performance counters, and object instances.
- Sets sampling intervals for monitoring data about hardware resources and system services.
- Collects information over a period of time and archives data.
- Supports the configuration of alerts that notify you when a certain threshold is reached.



5.7. Microsoft Management Console

Most of the tools that a network administrator needs to perform day-to-day tasks are available individually. Because all of the tools are not available in one location, Windows 2000 provides the capability to create a customized tool that contains all the required utilities. In this manner, the regularly accessed tools are all available at one location.

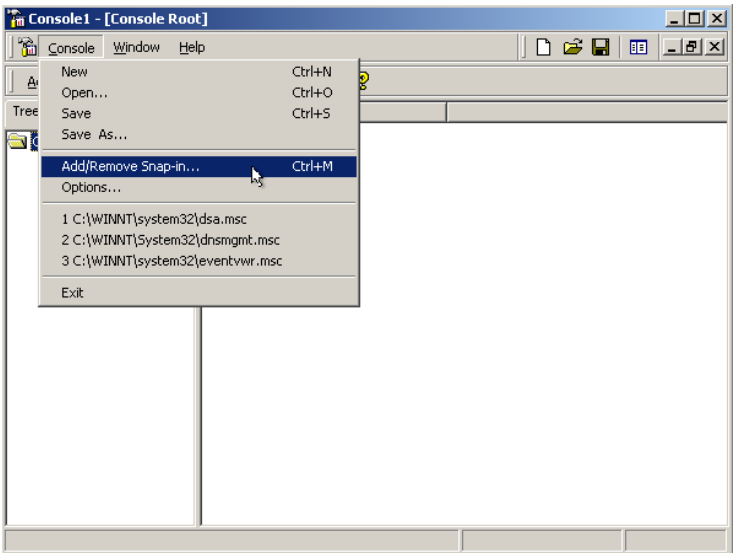
Another benefit of creating a customized tool is that an administrator can save the customized tool for later use and share the tool with other administrators and users. Also, administrators can create multiple tools of varying levels of complexity, which is useful for delegating tasks. To create a customized tool, you use the Microsoft Management Console (MMC). The customized tool that you create is called an MMC console and the primary tools that you add to it are called snap-ins. You can also add links to Web pages, folders, taskpad views, and tasks to an MMC console.

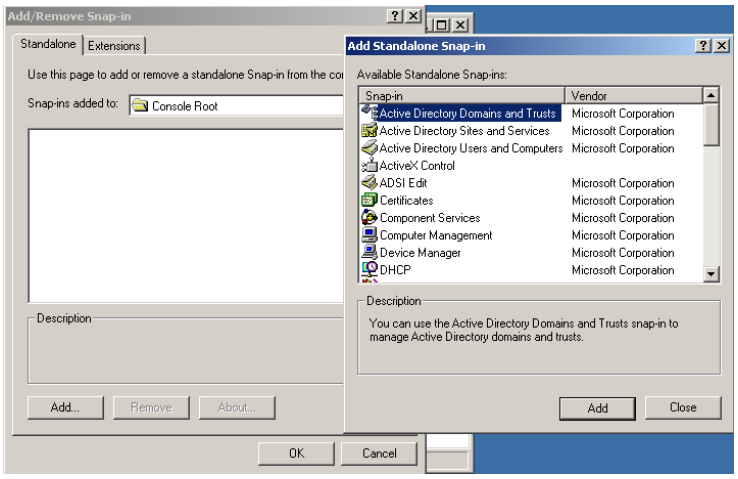
To create a customized console

- In the **Run** dialog box, type **mmc**
- On the **Console** menu, click **Add/Remove Snap-in**.

An MMC console consists of a window divided into two panes. The left pane is called the console tree and contains two tabs: **Tree** and **Favorites**. The console tree shows the items that are available in a given console. The right pane is called the details pane. The details pane shows information about the items in the console tree. The details pane can also display other types of information, including Web pages, graphics, charts, and tables.

Each console has its own set of menus and toolbars, separate from those of the main MMC window, that helps a user perform various tasks.




Add/Remove Snap-in
Standalone
Extensions
Use this page to add or remove a standalone Snap-in from the co
Snap-ins added to:
Console Root
Description
Add...
Remove
About...
OK
Cancel
Add Standalone Snap-in
Available Standalone Snap-ins:
Snap-in
Vendor
Active Directory Domains and Trusts
Microsoft Corporation
Active Directory Sites and Services
Microsoft Corporation
Active Directory Users and Computers
Microsoft Corporation
ActiveX Control
ADSI Edit
Microsoft Corporation
Certificates
Microsoft Corporation
Component Services
Microsoft Corporation
Computer Management
Microsoft Corporation
Device Manager
Microsoft Corporation
DHCP
Microsoft Corporation
Description
You can use the Active Directory Domains and Trusts snap-in to manage Active Directory domains and trusts.
Add
Close

6. Configuring Printing

6.1. Introduction to Windows 2000 Printing

Windows 2000 makes it easy for an administrator to set up network printing and configure the print resources from a central location. You can also configure client computers running Windows 95, Windows 98, or Microsoft Windows NT version 4.0, to print from the network print devices. Before you set up Windows 2000 printing, you should be aware of the terms used and the recommended system requirements for setting up a print server with a network accessible print device. For best results, keep in mind certain guidelines while planning a network-printing environment.

Windows 2000 Printing Terms

You should be familiar with the terms that are used to identify components and how these various components work together. The following list defines Windows 2000 printing terms:

Print device. The hardware device that produces printed documents. Windows 2000 supports the following print devices:

- Local print devices. Print devices that are connected to a physical port on the print server.
- Network-interface print devices. Print devices that are connected to a print server through the network instead of a physical port. Network- interface print devices require their own network adapters and have their own network address or they are attached to an external network adapter.
- Printer. The software interface between the operating system and the print device. The printer defines when and where a document will go to reach the print device (a local port, a port for a network connection, or a file).
- Print server. The computer on which the printers and client drivers are located. The print server receives and processes documents from client computers. You set up and share network printers that are associated with local- and network-interface print devices on the print servers.
- Printer driver. One or more files containing information that Windows 2000 requires to convert print commands into a specific printer language. This conversion makes it possible for a print device to print a document. A printer driver is specific to each print device model and the appropriate printer driver must be present on the print server.

6.2. Adding a Printer

When you set up and share a print device for use on the network, you make it possible for multiple users to use the same print device. You can set up a printer for a print device that is connected directly to the print server, or you can set up a printer for a network-interface print device that is connected to the print server over the network. In larger organizations, most printers point to network-interface print devices.

When you add a printer in Windows 2000, you must also verify that client computers are properly set up so that users can print their documents to the correct print device. The appropriate client drivers need to be installed on the print server for some of the client computers to be able to download them during installation.

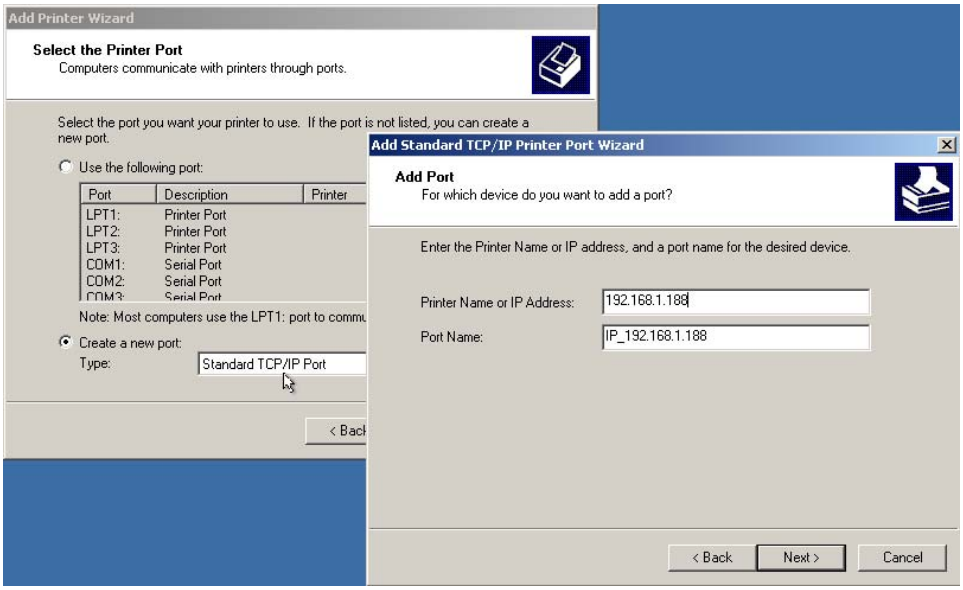
Adding and Sharing a Printer for a Local Print Device

When you add a shared printer, you must log on as Administrator on the print server. You can then add and share a printer by using the Add Printer wizard in the Printers system folder. The Add Printer wizard guides you through the steps of adding a printer for a print device that is connected to the print server. The number of local print devices that you can connect to a print server through physical ports depends on your hardware configuration.

The following table describes the options that the Add Printer wizard provides for adding a printer for a local print device.

Option	Description
Local printer	This option designates that you are adding a printer to the computer at which you are sitting (the print server).
Use the following port	The port on the print server to which you attached the print device. You can also add a port. Adding a port allows you to print to non-standard hardware ports, such as a network-interface connection.
Manufacturers and Printers	The correct printer driver for the local print device. Enter the manufacturer and the printer model for your print device. If your print device is not in the list, you must provide a printer driver from the manufacturer or select a model that uses a similar driver.
Printer name	A name that identifies the printer to the users. Use a name that is intuitive and descriptive of the print device. Some applications may not support more than 31 characters in the server and printer name combinations. This name also appears as the result of an Active Directory ™ directory service search.
Default printer	The default printer for all Windows-based applications. Select this option so that users do not have to set a printer for each application. The first time that you add a printer to the print server, this option does not appear because the printer is automatically selected as the default printer.
Shared as	A share name that users (with the appropriate permission) can use to make a connection to the printer over the network. This name appears when users browse for a printer or supply a path to a printer. Ensure that the share name is compatible with the naming conventions for all client computers on the network. By default, the share name is the printer name truncated to 8.3 characters. If you use a share name that is longer than 8.3 characters, some client computers may not be able to connect.
Location and Comment	Information about the print device. Provide information that helps users determine if the print device fits their needs. Users can search Active Directory for the information that you enter here. Because of this search capability, you need to standardize the type of information that you enter so that users can compare printers according to the search results.
Do you want to print a test page?	Verification that you have installed the printer correctly. Click Yes to print a test page.

To gain access to the Add Printer wizard, click **Start**, point **to Settings**, and then click **Printers**.



6.3. Adding and Sharing a Printer for a Network-Interface Print Device

In larger organizations, most print devices are network-interface print devices. These print devices offer several advantages. They provide greater flexibility in where you locate your printers. In addition, network connections transfer data quicker than printer cable connections.

You can add a printer for a network-interface print device by using the Add Printer wizard. The default network protocol for Windows 2000 is Transmission Control Protocol/Internet Protocol (TCP/IP), which many network-interface print devices use. If you use TCP/IP, you must provide additional port information in the Add Standard TCP/IP Printer Port wizard.

Using the Add Printer Wizard

The following table describes the options on the Select the Printer Port page of the Add Printer wizard for adding a network-interface print device.

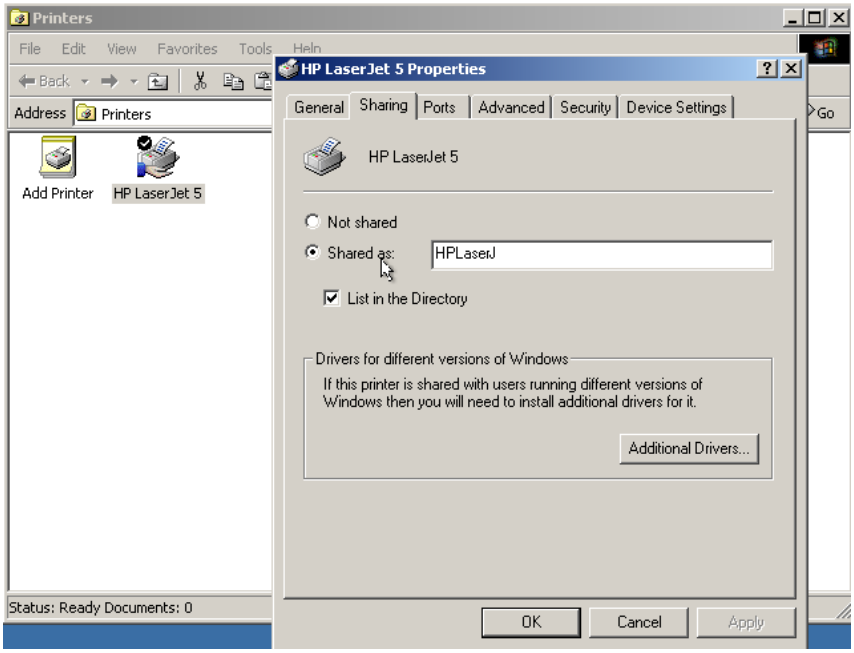
Option	Description
Create a new port	Starts the process of creating a new port for the print server to which the network-interface print device is connected. In this case, the new port points to the network connection of the print device.
Type	Determines the network protocol to use for the connection. The default protocol for Windows 2000 is TCP/IP.

6.4. Configuring a Network Printer

After you set up and share a printer for use on the network, user and organization printing needs may change and require you to configure printer settings so that your printing resources better fit these needs.

There are three common configuration changes. You can share an additional printer if your printing load increases. You can create a printer pool so that the printer automatically distributes print jobs to the first available print device and users do not have to search for an available printer. And you can set priorities between printers so that critical documents always print before noncritical documents.

Sharing an Existing Printer



If the print load increases on the shared printers and your network has an additional print device, you can share it and reduce the print load on each of the print devices.

When you share a printer on the print server:

- You must assign the printer a share name, which appears in My Network Places. Use an intuitive name to help users when they are browsing for a printer.
- You can choose to publish the printer in Active Directory if you are a member of an Active Directory network so that users can search for the printer. Publishing the printer in Active Directory enables users to search for the printer faster.
- You can add additional printer drivers for client computers running Windows 95, Windows 98, or Windows NT 4.0, on different hardware platforms.

To gain access to the **Sharing** tab, right-click the icon for the printer that you want to share in the Printers folder, and then click **Sharing**. After you have shared the printer, Windows 2000 changes the printer icon to display a hand underneath, indicating that the printer is shared.

6.5. Assigning Printer Permissions

Setting Printer Priorities

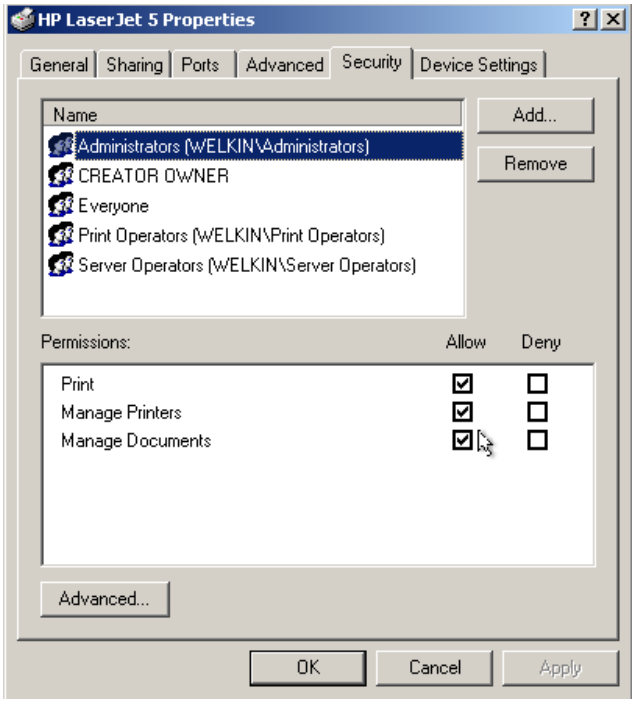
Set priorities between printers to prioritize documents that print to the same print device. To do this, create multiple printers pointing to the same print device. This allows users to send critical documents to a high-priority printer and noncritical documents to a lower priority printer. The documents sent to the high-priority printer will print first.

To set priorities between printers, perform the following tasks:

- Point two or more printers to the same print device (the same port). The port can be either a physical port on the print server or a port that points to a network-interface print device.
- Set a different priority for each printer that is connected to the print device, and then have different groups of users print to different printers. You can also have users send high-priority documents to the printer with higher priority and low-priority documents to the printer with lower priority. Notice that in the preceding illustration, User1 sends documents to a printer with the lowest priority of 1, while User2 sends documents to a printer with the highest priority of 99. In this example, User2's documents will print before User1's documents.

To set the priority for a printer, perform the following steps:

- Open the **Properties** dialog box for the printer.
- On the **Advanced** tab, change the priority in the **Priority** spin box, and then click OK.



There are three levels of printer permissions: Print, Manage Documents, and Manage Printer.

By default, administrators on a server, and print operators and server operators on a domain controller have the Manage Printer permission. The Everyone group has the Print permission, and the owner of a document has the Manage Documents permission. You can restrict access to a printer by removing Everyone and assigning the Print permission to a specific Domain Local group.

To add a user or group and assign print permissions, perform the following steps:

- In the Printers folder, right-click the icon for the printer for which you want to change permissions, and then click **Properties**.
- On the **Security** tab, in the **Properties** dialog box for the printer, click the **Everyone group**, and then click **Remove**.
- Click the **Add** button. Select the appropriate users and groups, click **Add**, and then click **OK**.
- On the **Security** tab, verify the permissions you want for the user or group, and then click **OK**.