

# Backing Up and Recovering Data

## On This Page

- ↓ [Introduction](#)
- ↓ [Before You Begin Using Backup](#)
- ↓ [Before You Begin Using Shadow Copies of Shared Folders](#)
- ↓ [Backing Up Your Servers](#)
- ↓ [Enabling Shadow Copies of Shared Folders on a File Server](#)
- ↓ [Restoring Data from Backup](#)
- ↓ [Restoring Previous Versions of Files and Folders](#)
- ↓ [Related Information](#)

## Introduction

This document will walk you through how to protect your servers and data using two technologies: Backup and Shadow Copies of Shared Folders.

Use Backup to help protect data from accidental loss if your server's hardware or storage media fails. For example, you can use Backup to create a duplicate copy of the data on your hard disk and then archive the data on another storage device. If the original data on your hard disk is accidentally erased or overwritten, or becomes inaccessible because of a hard disk malfunction, you can easily restore the data from the archived copy.

Shadow Copies of Shared Folders is a file-storage technology that provides user access to snapshots of files that are located on a shared network resource, such as a file server. With Shadow Copies of Shared Folders, users can quickly recover deleted or changed files that are stored on the network without administrator assistance, which can increase productivity and reduce administrative costs.

The tasks that are covered in this document are:

- Creating an Automated System Recovery (ASR) set
- Backing up your file and print servers
- Backing up the Active Directory directory service
- Enabling Shadow Copies of Shared Folders on a file server
- Restoring files from Backup
- Restoring your computer using an ASR set
- Restoring Active Directory
- Restoring Previous Versions of files and folders

**IMPORTANT:** All the step-by-step instructions included in this document were developed by using the Start menu that appears by default when you install your operating system. If you have modified your Start menu, the steps might differ slightly.

↑ [Top of page](#)

## Before You Begin Using Backup

The recommendations in this document are only for file and print servers running Microsoft Windows Server 2003. The following sections cover the options that you should consider before creating backups of your

servers.

## Select a Type of Backup Storage

The backup storage can be a hard disk drive, a separate storage device such as a tape drive, or an entire library of disks or tapes organized and controlled by a robotic changer.

Backing up to a tape is preferable because you can create a backup and store the tape in a different location from the computer. This protects against hard disk failure as well as loss from a fire or other catastrophic event.

If you choose to back up to a hard disk, make sure that it is a hard disk separate from your primary hard disk in case your primary hard disk fails. Backing up to a hard disk drive is convenient, but does not protect against a catastrophic event such as a fire or earthquake.

## Select a Schedule

It is best to perform backups late at night, on weekends, or whenever the server is not being used. You can back up files that are open or in use, but it is safer to back up your server during a slow use period.

You should schedule a weekly normal backup of all of your data, including the System State data for the server. A normal backup will copy all the files you select and mark each file as having been backed up. In addition, you can also schedule a daily differential backup. A differential backup copies files that have been created or changed since the last normal backup (the "differences"). It does not mark files as having been backed up so the changed file will also be backed up as part of the next normal backup. If you are performing a combination of normal and differential backups, restoring data requires that you have the last normal as well as the last differential backup.

## Backup Permissions

Certain permissions and user rights are required to back up files and folders. As part of scheduling backups, you will be asked for information about who is running the backup. If you are a member of the Administrators or Backup Operators group on the local computer, you can back up any file and folder on the local computer to which the local group applies. Likewise, if you are a member of the Administrators or Backup Operators group on a domain controller, you can back up any file and folder locally on any computer in the domain with which you have a two-way trust relationship. However, if you are not a member of either the Administrator or Backup Operators group for the domain, and you want to back up files, then you must be the owner of the files and folders that you want to back up, or you must have one or more of the following permissions for the files and folders you want to back up: Read, Read & Execute, Modify, or Full Control.

## Creating an ASR Set

In addition to regular backups of your data, you should use Backup to create an Automated System Recovery (ASR) set when you first place your server into production and again before and after any major changes to the system such as software and hardware upgrades. An ASR set contains a backup of your operating system files and a bootable floppy disk that can be used to start your computer if it will not start normally. Before creating an ASR set, make sure that you have a 3.5-inch floppy disk available to make the boot disk.

[↑ Top of page](#)

## Before You Begin Using Shadow Copies of Shared Folders

Shadow Copies of Shared Folders should be used in conjunction with a regular backup plan on file servers that use shared folders to provide users access to files. Shadow Copies for Shared Folders will allow users to recover their own files without costly intervention from a backup administrator. It is not a replacement for regular backups-shadow copies cannot be used for permanent archives and may be deleted depending on the storage limits and the number of shadow copies that exist on the server.

## Default Schedule

When you enable Shadow Copies of Shared Folders, a default schedule is created. If you keep the default settings, shadow copies of the volume will be taken at 7:00 A.M. and noon, Monday through Friday. This schedule might work for your users, but it is important to consider the particular work habits of your users

before using this default schedule. You might want to consider the following questions:

- Do most of your users work from 9 A.M. to 5 P.M., Monday through Friday, in the same time zone?
- Are users spread out across time zones Does this mean that you need more copies throughout the day to cover all of the work hours?
- How much work time can your users afford to lose Will the default schedule of copies twice a day (7:00 A.M. and noon, Monday through Friday) provide adequate coverage?
- How often can copies be taken without needing to add additional storage?
- How many days of history can be retained before reaching the limit of 64 shadow copies?

You might want to create an initial schedule and deploy to a small group to test whether your scheduled shadow copies stay within the storage limits you set. Also, consider polling your users to find out their work habits and when they think that a shadow copy would be beneficial. This kind of information can help you determine the best schedule for your specific users.

## Default Storage Settings

You can only enable Shadow Copies of Shared Folders on a per-volume basis; that is, you cannot select specific shared folders and files on a volume to be copied or not copied. By default, the shadow copies will be stored on the volume that is being copied (the source volume). If you have more than one drive available on your server, you should use a separate volume on another disk to store the shadow copies. This eliminates the possibility that high input/output (I/O) load will cause shadow copies to be deleted. This is the recommended configuration for heavily used file servers.

The default storage size is 10 percent of the source volume (the volume being copied). The minimum amount of storage space that you can specify is 100 megabytes (MB). If the shadow copies are stored on a separate volume, change the default to reflect the space available on the storage volume instead of the source volume. Remember that when the storage limit is reached, older versions of the shadow copies will be deleted and cannot be restored.

When determining the amount of space to allocate for storing shadow copies, you must consider both the number and size of files that are being copied, as well as the frequency of changes between copies. For example, 100 files that only change monthly require less storage space than 10 files that change daily.

There is a limit of 64 shadow copies that can be stored on a volume. When this limit is reached, the oldest shadow copy is deleted and cannot be retrieved.

## Installing Client Software

In order for client computers to use Shadow Copies of Shared Folders, the Previous Versions client software must be installed on the client computers in your organization. It is recommended that you download and place the installation package on a shared resource and send an e-mail to users about what the client does and how to install it. See "Sample E-mail" later in this section.

If your organization only has client computers running Windows XP, the Previous Versions client software can be found on a computer running Windows Server 2003 in the following location:

```
%systemroot%\system32\clients\twclient directory
```

If your organization has client computers running Windows 2000 and Windows XP, download the installation package (ShadowCopyClient.msi) from the [Microsoft Web site](http://go.microsoft.com/fwlink/?LinkId=22346) at <http://go.microsoft.com/fwlink/?LinkId=22346>. In addition, you will need to run the same installation package on Windows Server 2003. This sets a registry setting that allows access to the server from client computers running Windows 2000.

## Sample E-mail

Organization members:

There is a new feature called **Previous Versions** that is available for employees who use shared folders for documents. If you work with files that are located in shared folders on your network, you may be able to access previous versions of your files. Accessing previous versions of your files is useful because you can:

- Recover files that were accidentally deleted. If you accidentally delete a file, you can open a previous

version and copy it to a safe location.

- Recover from accidentally overwriting a file. If you accidentally overwrite a file, you can recover a previous version of the file.
- Compare versions of file while working. You can use previous versions when you want to check what has changed between two versions of a file.

This feature has been enabled on the following file server: `\\NameOfServer\SharedResource`. Copies are scheduled to be taken at 7:00 A.M. and noon, Monday through Friday. Remember that these are copies of the files that were taken at these times. If you have worked on the file since the copy was taken and you need to revert or recover a previous version, you will lose all the work you have done since the copy was taken. Saving your work frequently is still the best way to ensure your work is not lost.

To install the software for accessing previous versions on your desktop, go to:  
`\\NameOfServer\InstallationFolder` and double-click **ShadowCopyClient.msi**.

[↑ Top of page](#)

## Backing Up Your Servers

The following section describes the step-by-step procedures for:

- Creating an Automated System Recovery (ASR) set
- Backing up your file and print servers
- Backing up Active Directory

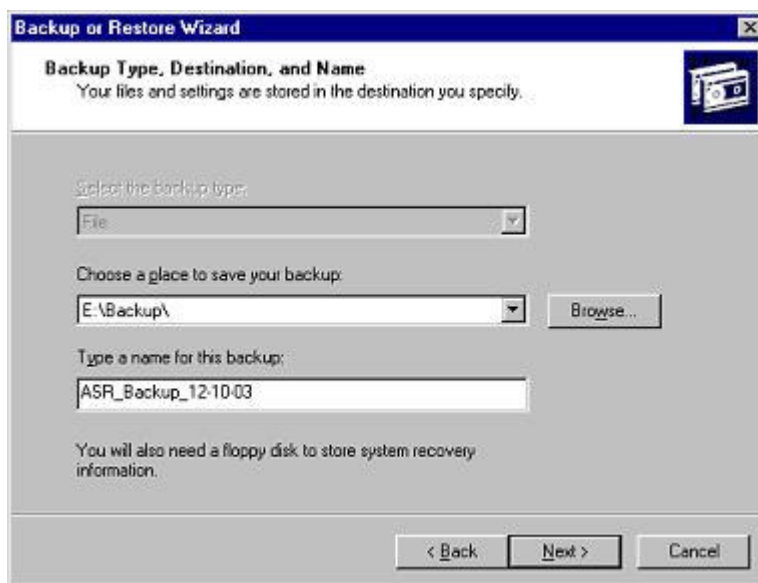
### Creating an Automated System Recovery (ASR) Set

You should use Backup to create an ASR set when you first place your server into production and again before and after any major changes to the system such as software and hardware upgrades. An ASR set is used as a last resort in system recovery, only after you have exhausted other options such as the startup options Safe Mode and Last Known Good Configuration.

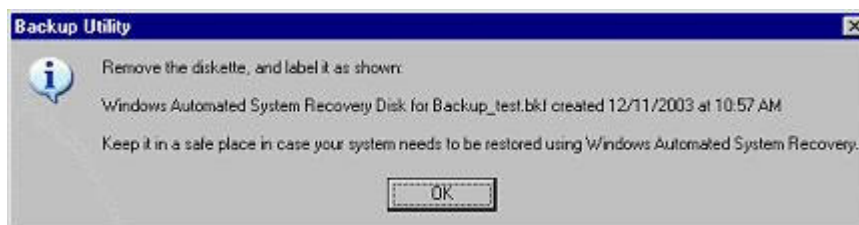
### Requirements

- **Credentials:** To perform this procedure, you must be a member of the Administrators or Backup Operators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure.
- **Tools:** Backup
- **To create an ASR set**
  1. Click **Start**, click **Run**, type **ntbackup**, and then click **OK**.
  2. The **Backup or Restore Wizard** will appear. Click **Next**.
  3. On the **Backup or Restore** wizard page, ensure **Back up files and settings** is selected, and then click **Next**.
  4. On the **What to Back Up** page, ensure **All information on this computer** is selected, and then click **Next**.
  5. On the **Backup Type, Destination, and Name** page, under **Choose a place to save your backup**, click the drop-down menu or click **Browse** to choose a location to save your backup. Under **Type a name for this backup**, type a descriptive name for the backup, and then click **Next**.

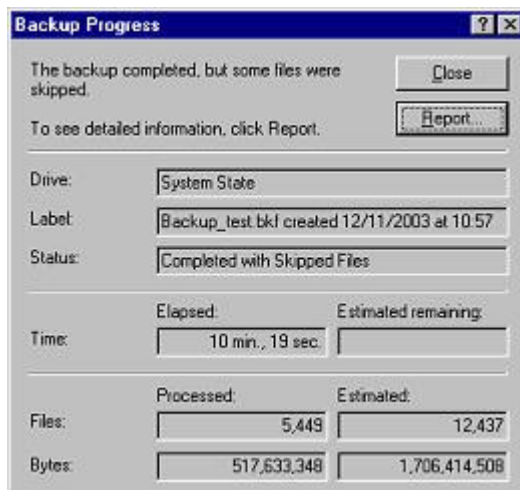
**Note:** Screenshots in this document reflect a test environment and the information might differ from the information displayed on your screen.



6. On the **Completing the Backup or Restore Wizard** page, verify that all of the information is correct, and then click **Finish** to start creating the ASR set.
7. When the **Backup Utility** message appears, follow the directions and insert a .44 megabyte (MB) floppy disk into drive A, and then click **OK**.
8. When the **Backup Utility** message appears letting you know you can remove the floppy disk, make sure you label the disk with the information given.



9. When the backup is complete, the **Backup Progress** dialog box will indicate that the backup is finished. To view additional information about what happened during the backup process, click **Report** to open the backup report in Notepad. When you are finished, click **Close**.



10. Store the floppy disk in a safe place near the computer. Remember, this disk can be used along with your installation CD to start and restore the computer but you must have both the boot disk and the backup files that were created.

## Backing Up Your File and Print Servers

To protect your servers, schedule regular backups of all of the data. We recommend that you schedule a

weekly normal backup of all of your data, including the System State data for the server. A normal backup will copy all the files you select and mark each file as having been backed up. In addition, we recommend you schedule a daily differential backup. A differential backup copies files that have been created or changed since the last normal backup (the "differences").

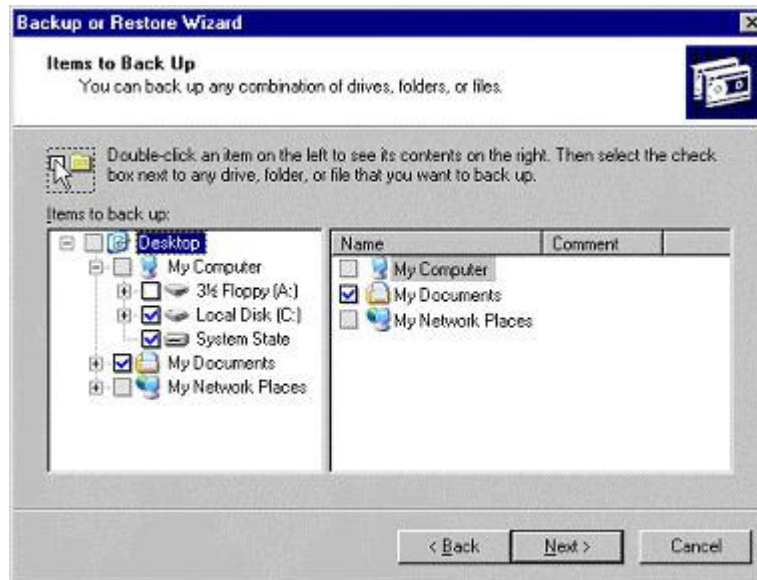
## Requirements

- **Credentials:** To perform this procedure, you must be a member of the Administrators or Backup Operators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure.

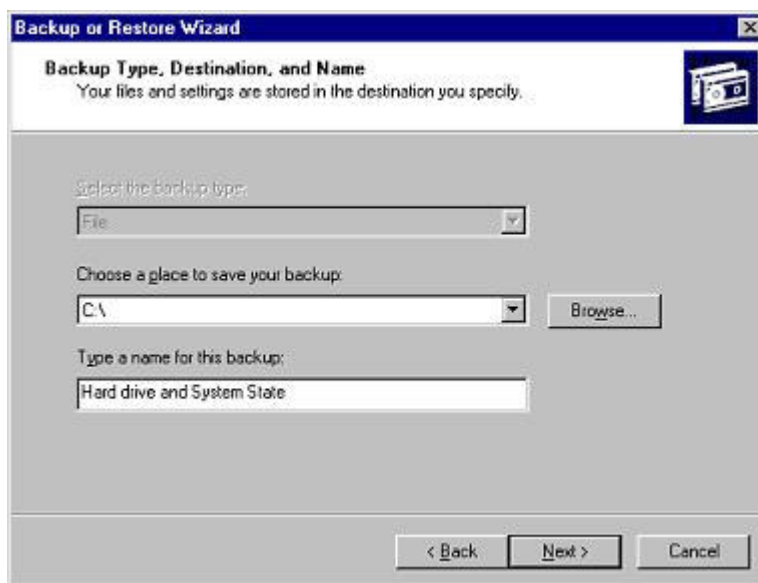
- **Tools:** Backup

### ● To schedule a weekly normal backup

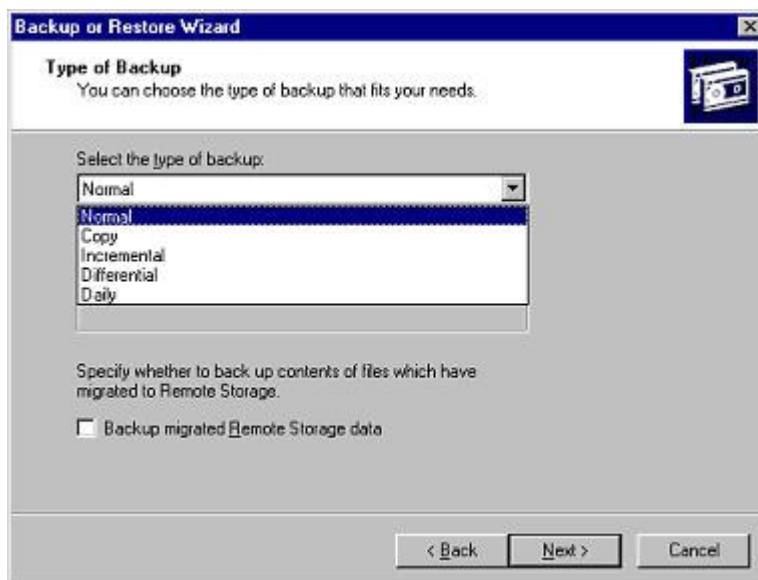
1. Click **Start**, click **Run**, type **ntbackup**, and then click **OK**.
2. The **Backup or Restore Wizard** will appear. Click **Next**.
3. On the **Backup and Restore** wizard page, make sure **Back up files and settings** is selected, and then click **Next**.
4. On the **What to Back Up** page, click **Let me choose what to back up**, and then click **Next**.
5. On the **Items to Back Up** page, click the items to expand their contents. Select the **System State** check box and select other check boxes for any drives or folders that contain data that should be backed up on a regular basis, and then click **Next**.



6. On the **Backup Type, Destination, and Name** page, under **Choose a place to save your backup**, click the drop-down menu or click **Browse** to choose a location to save your backup. Under **Type a name for this backup**, type a descriptive name for the backup, and then click **Next**.



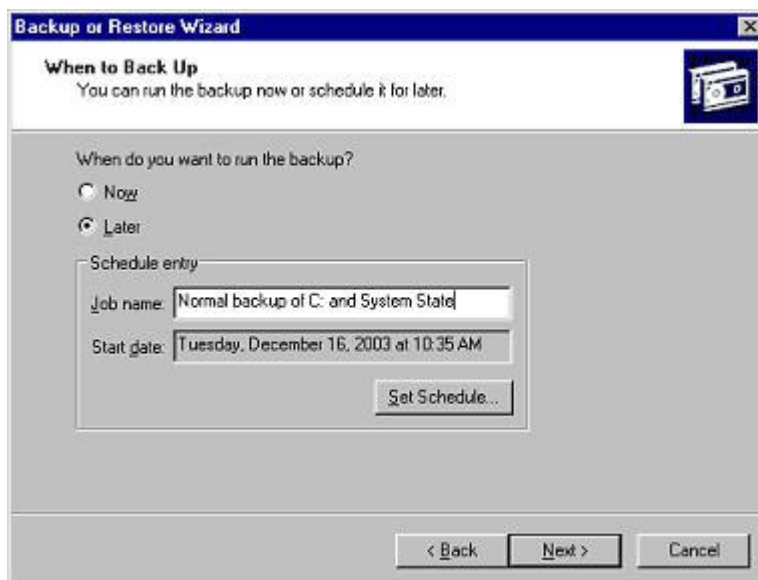
7. On the **Completing the Backup or Restore Wizard** page, click **Advanced**.
8. On the **Type of Backup** page, in the drop-down menu, click **Normal**, and then click **Next**.



9. On the **How to Back Up** page, select the **Verify data after backup** check box, and then click **Next**.
10. On the **Backup Options** page, ensure the **Append this backup to the existing backups** option is selected, and then click **Next**.



11. On the **When to Back Up** page, under **When do you want to run the backup**, click **Later**.
12. In **Schedule entry**, type a descriptive name in **Job name**, and then click **Set Schedule**.



13. In the **Schedule Job** dialog box, under **Schedule Task**, click **Weekly** in the drop-down menu.
14. In **Start time**, use the up and down arrows to select the appropriate time for the backup to start.
15. In **Schedule Task Weekly**, select one or more days when you would like to have a backup created, and then click **OK**.



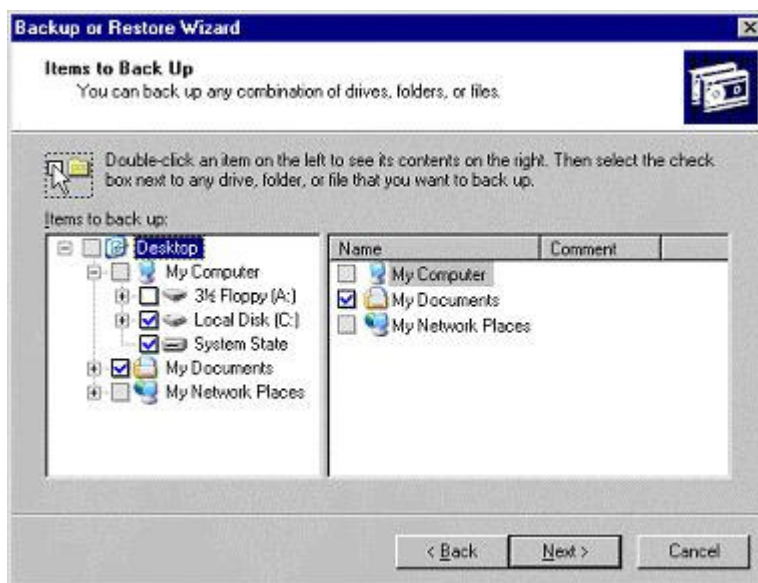
16. In the **Set Account Information** dialog box, in **Run as**, type the domain or workgroup and user name in the format *domain\username* or *workgroup\username*. In **Password**, type the password for the user account. Retype the password in **Confirm password**, and then click **OK**.



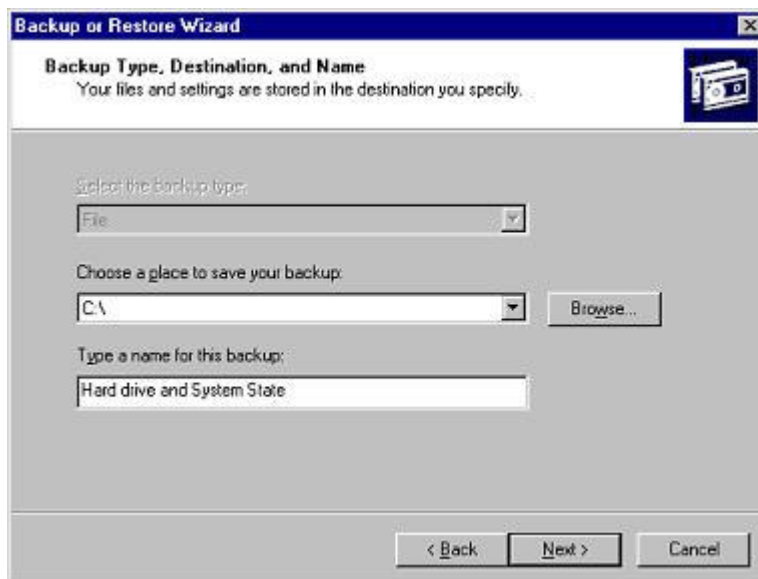
17. On the **Completing the Backup or Restore Wizard** page, confirm the settings, and then click **Finish**.

- **To schedule a daily differential backup**

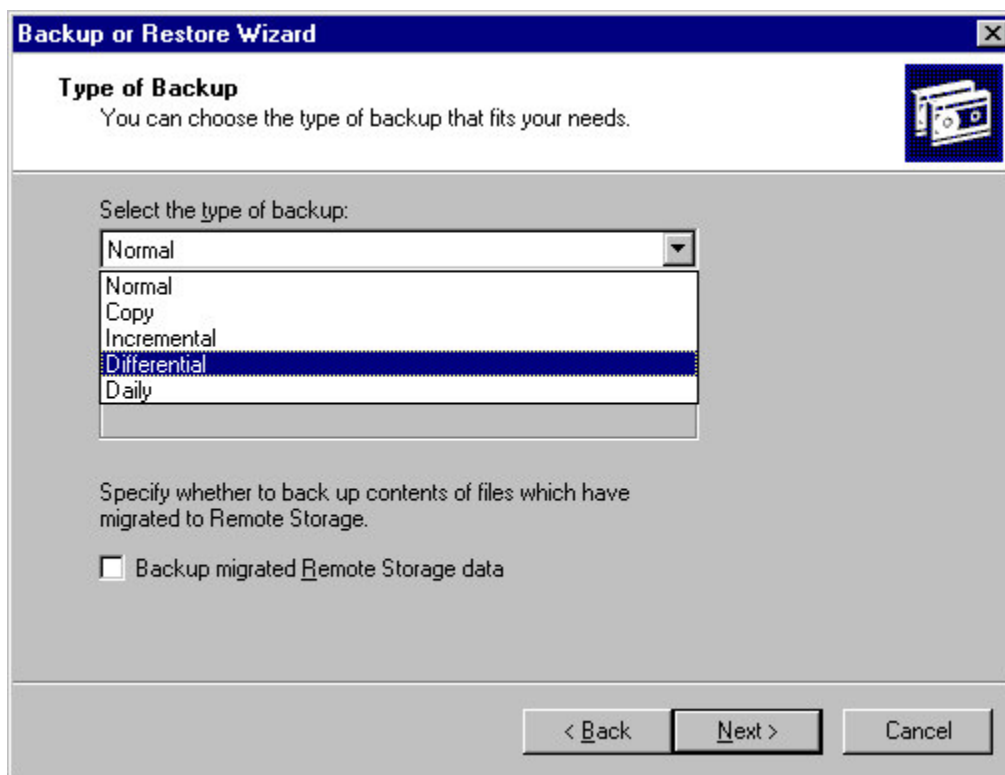
1. Click **Start**, click **Run**, type **ntbackup.exe**, and then click **OK**.
2. The **Backup or Restore Wizard** will appear. Click **Next**.
3. On the **Backup and Restore** wizard page, ensure **Back up files and settings** is selected, and then click **Next**.
4. On the **What to Back Up** page, click **Let me choose what to back up**, and then click **Next**.
5. On the **Items to Back Up** page, click the items to expand their contents. Select the **System State** check box and select other check boxes for any drives or folders that contain data that should be backed up on a regular basis, and then click **Next**.



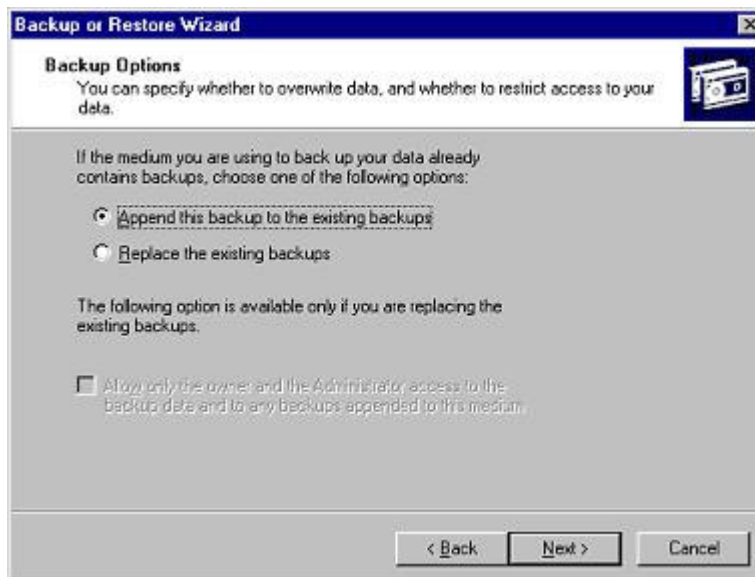
6. On the **Backup Type, Destination, and Name** page, in **Choose a place to save your backup**, click the drop-down menu or click **Browse** to choose a location to save your backup. In **Type a name for this backup**, type a descriptive name for the backup, and then click **Next**.



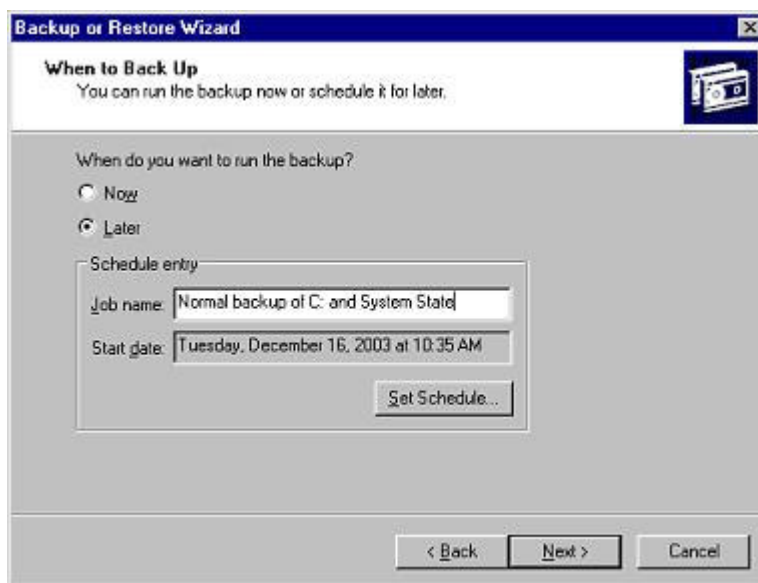
7. On the **Completing the Backup or Restore Wizard** page, click **Advanced**.
8. On the **Type of Backup** page, under **Select the type of backup**, click **Differential**, and then click **Next**.



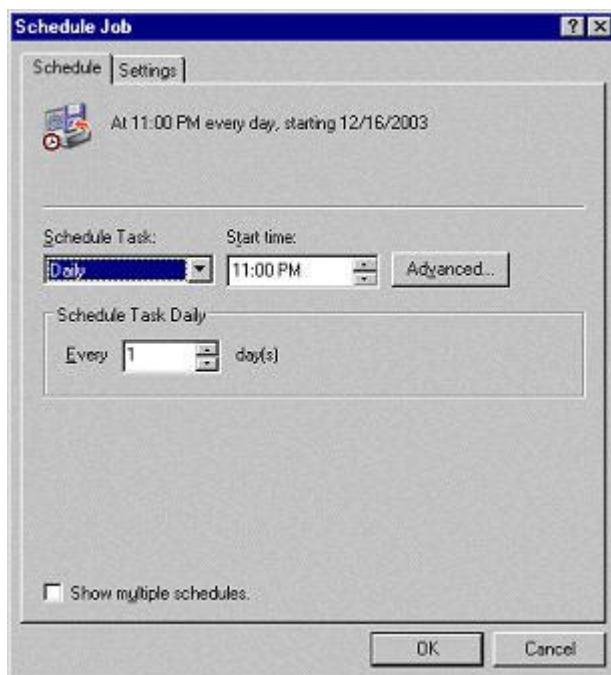
9. On the **How to Back Up** page, select the **Verify data after backup** check box, and then click **Next**.
10. On the **Backup Options** wizard page, ensure the **Append this backup to the existing backups** option is selected, and then click **Next**.



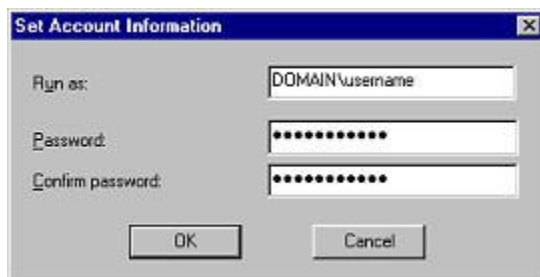
11. On the **When to Back Up** page, under **When do you want to run the backup**, click **Later**. Under **Schedule entry**, type a descriptive name in **Job name**, and then click **Set Schedule**.



12. In the **Schedule Job** dialog box, under **Schedule Task**, select **Daily** from the drop-down menu.
13. Under **Start time**, use the up and down arrows to select the appropriate time for the backup to start, and then click **OK**.



14. In the **Set Account Information** dialog box, in **Run as**, type the domain or workgroup and user name in the format *domain\username* or *workgroup\username*. In **Password**, type the password for the user account. Retype the same password in **Confirm password**, and then click **OK**.



15. On the **Completing the Backup or Restore Wizard** page, confirm your settings, and then click

**Finish.**

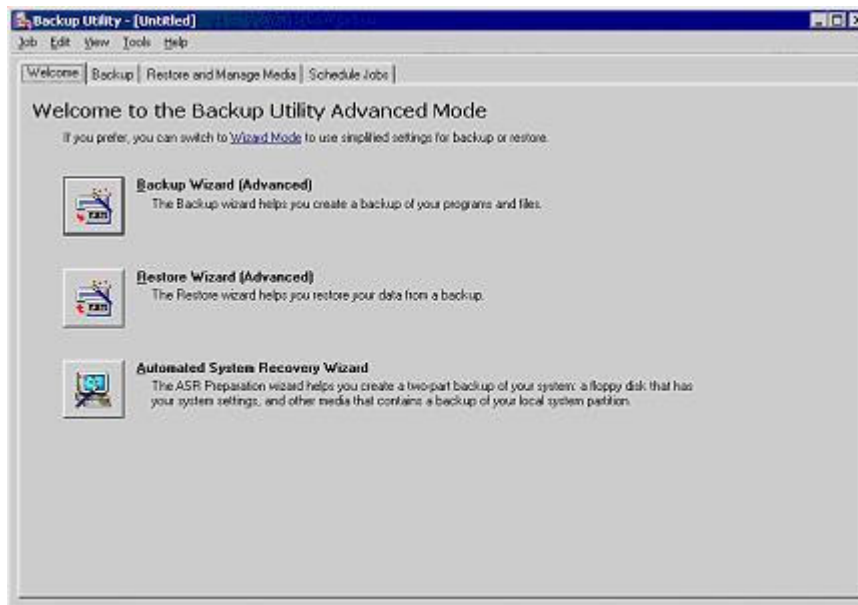
## Backing Up Active Directory

Back up the Active Directory directory service to ensure the recoverability of your Active Directory data in the event of a security breach that corrupts or destroys your Active Directory installation. You can back up Active Directory by performing a system state backup.

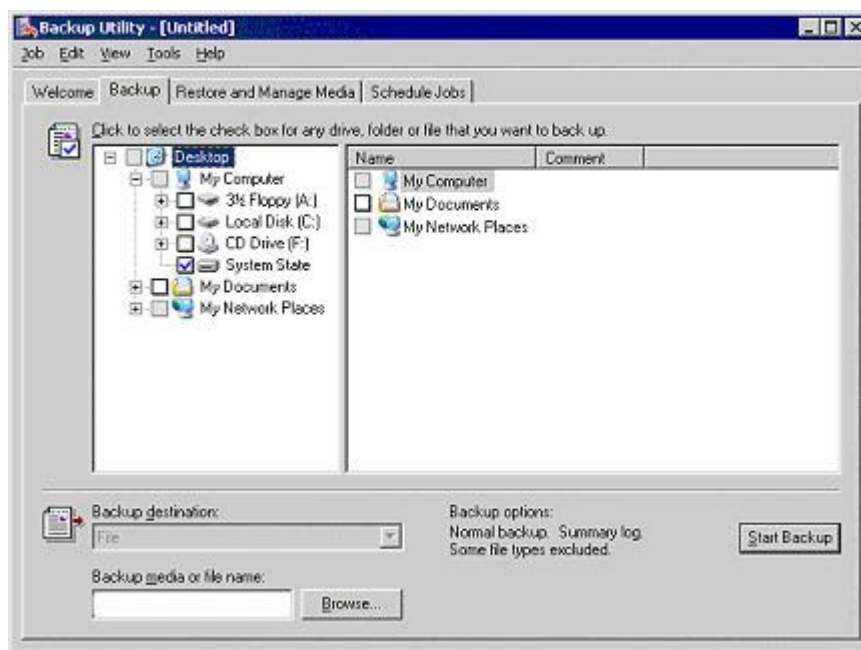
You should perform this procedure on a regular basis on each of your domain controllers. In the event of a loss or corruption of Active Directory data, you can use this backup to restore Active Directory to a known, good state. For more information about backing up and restoring Active Directory, see "Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part II" in Related Information later in this document.

## Requirements

- **Credentials:** To perform this procedure, you must be a member of the Administrators or Backup Operators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure.
- **Tools:** Backup Utility
- **To back up Active Directory**
  1. Log on to a domain controller using an account (such as Administrator) that is a member of the Domain Admins group.
  2. Click **Start**, click **Run**, in **Open**, type **ntbackup**, and then click **OK**.
  3. On the Welcome page of the Backup or Restore Wizard, click the **Advanced Mode** link to open the **Backup Utility**. Click **Backup Wizard (Advanced)**.



4. On the **Backup** tab, select the **System State** check box. In **Backup media or file name**, specify the backup media location, and then click **Start Backup**.



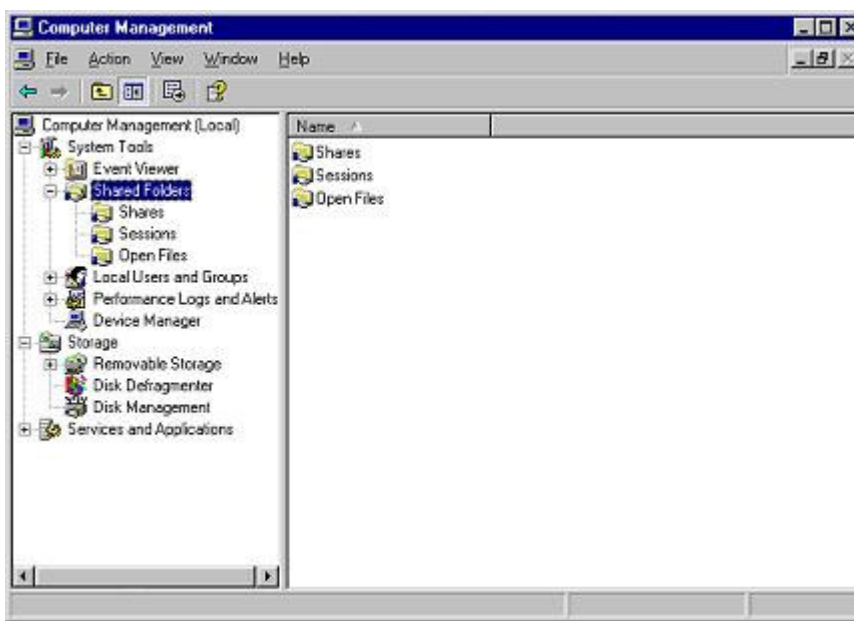
[↑ Top of page](#)

## Enabling Shadow Copies of Shared Folders on a File Server

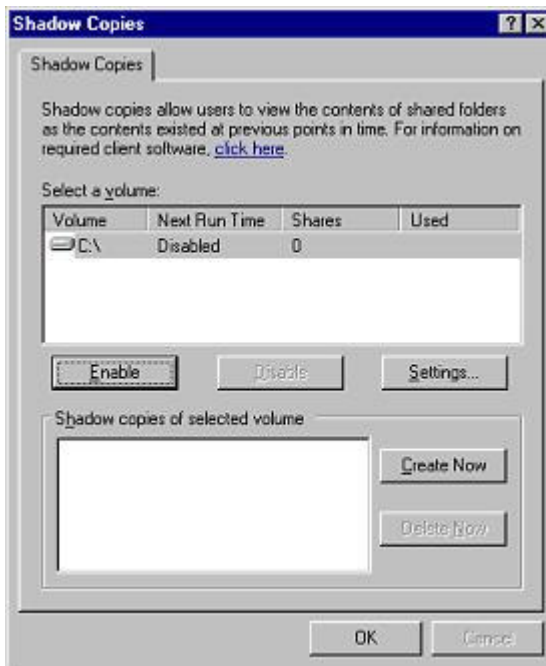
When you enable Shadow Copies of Shared Folders on your file server, snapshots of the content of shared files and folders will be taken. These snapshots can then be accessed using the Previous Versions client. By enabling Shadow Copies of Shared Folders, you also create a default schedule that will create shadow copies at 7:00 A.M. and noon, Monday through Friday. There will also be a limit set on the amount of space that can be used to store the shadow copies. The default storage size is 10 percent of the source volume (the volume being copied). When the storage limit is reached, older versions of the shadow copies will be deleted and cannot be restored.

### Requirements

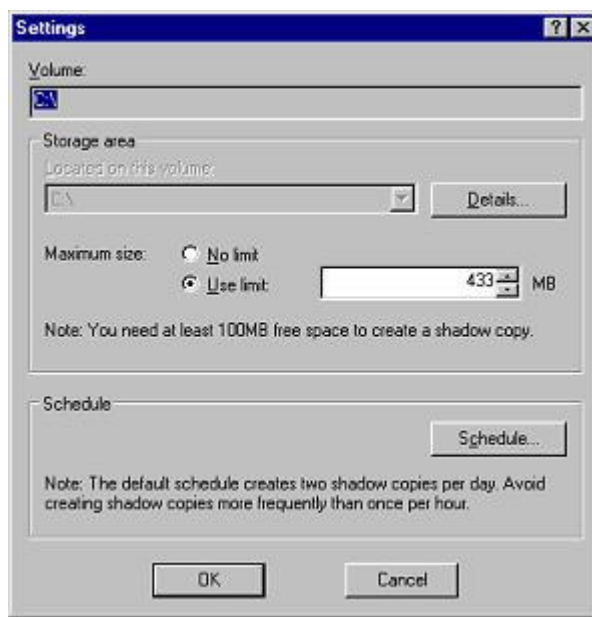
- **Credentials:** To perform this procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure.
- **Tools:** Computer Management
- **To enable Shadow Copies of Shared Folders**
  1. Click **Start**, point to **All Programs**, point to **Administrative Tools**, and then click **Computer Management**.
  2. In the console tree, right-click **Shared Folders**, select **All Tasks**, and click **Configure Shadow Copies**.



3. In the **Shadow Copies** dialog box, click the volume where you want to enable **Shadow Copies of Shared Folders**, and then click **Enable**. The **Enable Shadow Copies** dialog box will appear. Click **Yes** to confirm that you want to enable shadow copies on the volume.



**Note:** To change default schedule settings, click **Settings** .



[↑ Top of page](#)

## Restoring Data from Backup

There are several ways to restore your server depending on what files need to be restored and whether your system will start normally. The following procedures are covered in this section:

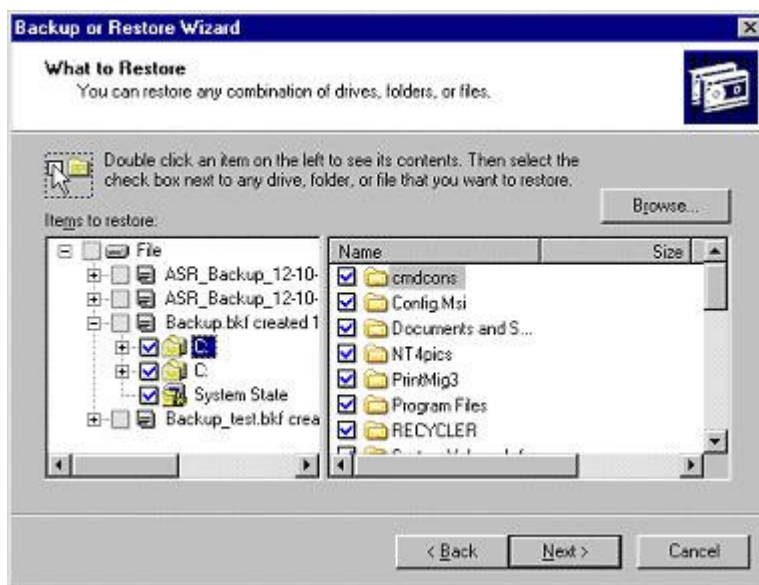
- Restoring files from Backup
- Restoring your computer using an ASR set
- Restoring Active Directory

### Restoring Files from Backup

If the original data on your hard disk is accidentally erased or overwritten, or becomes inaccessible because of a hard disk malfunction, the data may be restored from the back up copy.

### Requirements

- **Credentials:** To perform this procedure, you must be a member of the Administrators or Backup Operators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure.
- **Tools:** Backup. If you are performing a combination of normal and differential backups, restoring files and folders requires that you have the last normal as well as the last differential backup.
- **To restore files from backup**
  1. Click **Start**, click **Run**, type **ntbackup**, and then click **OK**.
  2. The **Backup or Restore Wizard** will appear. Click **Next**.
  3. On the **Backup and Restore** wizard page, click **Restore files and settings**, and then click **Next**.
  4. On the **What to Restore** page, click the items to expand their contents. Select any drives or folders that contain data that should be restored, and then click **Next**.



5. On the **Completing the Backup or Restore Wizard** page, verify that all of the settings are correct, and then click **Finish**.

### Restoring Your Computer Using an ASR Set

ASR should be used as a last resort in system recovery, only after you have exhausted other options such as the startup options Safe Mode and Last Known Good Configuration. For more information about these and other recovery options, see "Repair overview" in Related Information later in the document.

### Requirements

- Tools: Your previously created ASR set, your previously created backup media, and the original Windows Server 2003 installation CD.
- **To restore your computer from an ASR set**
  1. Insert the original Windows Server 2003 installation CD into your CD drive.
  2. Restart your computer. If you are prompted to press a key to start the computer from CD, press the appropriate key.
  3. Press **F2** when prompted at the beginning of the text-only mode section of Setup. You will be prompted to insert the ASR floppy disk you have previously created.
  4. Follow the directions on the screen.

**Note:** Automated System Recovery will not restore your data files. For more information, see "Restoring Files from Backup" earlier in this document.

### Restoring Active Directory

In the event that your domain controller is corrupted or destroyed, you can recover your data using the **Directory Services Restore Mode** startup option.

### Requirements

- Credentials: To perform this procedure, you must be a member of the Administrators or Backup Operators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure.
- Tools: Directory Services Restore Mode
- **To restore Active Directory**
  1. Restart the domain controller, press the **F8** key during the text-mode portion when starting

Windows Server 2003 to reach the Windows Advanced Options Menu.

2. Choose **Directory Services Restore Mode** from the **Windows Advanced Options Menu**, and then press ENTER.
3. Select the operating system to start, and then press ENTER.
4. Press CTRL+ALT+DELETE to log on.
5. At the logon prompt, supply the Directory Services Restore mode credentials you supplied during the Active Directory installation process (dcpromo).
6. Click **OK** to acknowledge that you are using **Safe** mode.
7. Click **Start**, point to **All Programs**, point to **Accessories**, point to **System Tools**, and then click **Backup**.
8. On the **Backup or Restore Wizard** dialog box, click **Advanced Mode**.
9. On the **Restore and Manage Media** tab, click **System State** to restore from the appropriate backup media item.
10. In **Restore Files to**, select **Original Location**.
11. Click **Start Restore**.
12. Click **OK** to acknowledge the warning regarding restoring the System State to the original location.
13. In the **Confirm Restore** dialog box, click **OK**.
14. After the restore process is finished, click **Close**, and then click **Yes** to restart the computer.

[↑ Top of page](#)

## Restoring Previous Versions of Files and Folders

With the Previous Versions client, you may be able to access previous versions of your files that are located in shared folders on your network. This feature is available when Shadow Copies of Shared Folders is enabled on the server.

Accessing previous versions of your files is useful because you can:

- View previous versions to compare versions of file while working. You can use previous versions when you want to check what has changed between two versions of a file.
- Recover files that were accidentally deleted. If you accidentally delete a file, you can open a previous version and copy it to a safe location.
- Recover from accidentally overwriting a file. If you accidentally overwrite a file, you can recover a previous version of the file.

### Requirements

**Credentials:** You must at least have Read permissions on the file to view or copy a previous version and Read & Execute permissions in order to restore the file.

**Tools:** Previous Versions client. The client is installed by default on computers running Windows Server 2003. For more information about installing the Previous Versions client, see "Before you Begin Using Shadow Copies of Shared Folders" earlier in this document.

#### ● To view a previous version of a file or folder

1. Locate the file that you want to view a previous version of (on the network), right-click the file, and then click **Properties**.
2. On the **Previous Versions** tab, click the version you want to view, and then click **View**.

**Notes:** If there are no previous versions listed, the file has not changed since the oldest copy was taken.

If you do not see the **Previous Versions** tab, the client is not installed.

Previous versions are read-only. You cannot make changes to the previous version of the file as it exists on the server.

- **To copy a previous version of a file to a new location**

1. Locate the file that you want to copy (on the network), right-click the file, and then click **Properties**.
2. On the **Previous Versions** tab, click the version of the file that you want to copy, and then click **Copy**.
3. In the **Copy Items** dialog box, click a new location to place the file, and then click **Copy**.

**Notes:** If there are no previous versions listed, the file has not changed since the oldest copy was taken.

If you do not see the **Previous Versions** tab, the client is not installed.

When you use **Copy**, the file permissions will be set to the default permissions for the directory where the copy of the file is placed.

- **To restore a previous version of a file**

1. Locate the file that you want to restore (on the network), right-click the file, and then click **Properties**.
2. On the **Previous Versions** tab, click the version of the file that you want to restore, and then click **Restore**. A warning message about restoring a previous version will appear. Click **Yes** to complete the procedure.

**Notes:** Restoring a previous version will delete the current version. If you choose to restore a previous version of a folder, the folder will be restored to its state at the date and time of the version you selected. You will lose any changes that you have made to files in the folder since that time. If you do not want to delete the current version of a file or folder, use **Copy** to copy the previous version to a different location.

If there are no previous versions listed, the file has not changed since the oldest copy was taken.

If you do not see the **Previous Versions** tab, the client is not installed.

When you restore a previous version of a folder, files in the current folder that were not contained in the previous version of the folder will not be erased.

When you restore a file, the file permissions will not be changed; permissions will remain the same as they were before the restore. When you copy a previous version of a file, the permissions will be set to the default permissions for the directory where the copy of the file is placed.

Restoring a large directory puts a heavy load on the file server and can result in previous versions being deleted. Try to restore individual files instead of entire directories whenever possible.

- **To recover a file that was accidentally deleted**

1. Locate the folder where the deleted file was stored (on the network), right-click the folder, and then click **Properties**.
2. On the **Previous Versions** tab, double-click the most recent version of the folder that contains the file that you want to recover. A list of files that are stored in that previous version will appear.
3. Right-click the file that was accidentally deleted, and then click **Copy**.
4. Right-click the location where you want to place the file, and then click **Paste**.

**Notes:** When you copy a file, file permissions will be set to the default permissions for the directory where the copy of the file is placed.

When you recover a file that was accidentally deleted, you are copying a previous version. You will lose any

changes made to the file after the last previous version was created.

To recover a deleted folder, go to a previous version of the parent folder to view and select the folder to copy.

[↑ Top of page](#)

## Related Information

For more information about backing up and restoring data, see the following:

- "[Backing up and recovering data](http://go.microsoft.com/fwlink/?LinkId=22347)" on the Microsoft TechNet Web site at <http://go.microsoft.com/fwlink/?LinkId=22347>.
- "[Repair overview](http://go.microsoft.com/fwlink/?LinkId=22448)" on the Microsoft TechNet Web site at <http://go.microsoft.com/fwlink/?LinkId=22448>.
- "[Checklist: Recovering a system that will not start](http://go.microsoft.com/fwlink/?LinkId=22449)" on the Microsoft TechNet Web site at <http://go.microsoft.com/fwlink/?LinkId=22449>.

For more information about Shadow Copies of Shared Folders, see the following:

- "[Shadow Copies of Shared Folders](http://go.microsoft.com/fwlink/?LinkId=22349)" on the Microsoft TechNet Web site at <http://go.microsoft.com/fwlink/?LinkId=22349>.
- "[Introduction to Shadow Copies of Shared Folders](http://go.microsoft.com/fwlink/?LinkId=22350)" on the Microsoft Web site at <http://go.microsoft.com/fwlink/?LinkId=22350>.
- "[Shadow Copies of Shared Folders: Frequently Asked Questions](http://go.microsoft.com/fwlink/?LinkId=2235)" on the Microsoft Web site at <http://go.microsoft.com/fwlink/?LinkId=2235>.

For more information about Backup technologies, see the following:

- "[Understanding Backup](http://go.microsoft.com/fwlink/?LinkId=22348)" on the Microsoft Web site at <http://go.microsoft.com/fwlink/?LinkId=22348>.  
For more information about backing up and restoring Active Directory, see the following:
- "[Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part II](http://go.microsoft.com/fwlink/?LinkId=22447)" on the Microsoft Web site at <http://go.microsoft.com/fwlink/?LinkId=22447>.

[↑ Top of page](#)

---

[Manage Your Profile](#)

© 2008 Microsoft Corporation. All rights reserved. [Contact Us](#) | [Terms of Use](#) | [Trademarks](#) | [Privacy Statement](#)

**Microsoft**