

# Chapter 13

## Harden the Security Lifecycle



Presented by:



- Create a Business Continuity Plan
- Generate a Security Policy
- Perform Hardened Operating System Installation
- Harden Operating System, Application, and Data Protection
- Manage Changes with a Formal Change Management Program
- Be Prepared for Disaster Recovery
- Monitor and Audit

Reproduced from the book [Hardening Windows Systems](#). Copyright© 2004, The McGraw-Hill Companies, Inc.. Reproduced by permission of The McGraw-Hill Companies, Two Penn Plaza, NY, NY 10121-2298. Written permission from The McGraw-Hill Companies, Inc. is

The process of hardening systems is not a one-time job. In order to maintain a high level of information security in your organization, you must not only configure systems according to hardening recommendations, you must apply and monitor security throughout the security lifecycle. The security lifecycle of Windows operating systems is composed of the following iterative steps:

1. Business continuity planning
2. Security policy generation
3. Hardened operating system installation
4. Hardened application and data protection configuration
5. Change management
6. Disaster recovery
7. Monitoring and auditing

## Create a Business Continuity Plan

Business continuity planning is, quite simply, a plan that seeks to ensure business operation in spite of any event that may disrupt the business. Events can be natural disasters such as floods and tornadoes. Events can be fire, lack of electricity, equipment malfunction, and accidents. Events can even be digital attacks or misconfiguration. In short, any event that might interrupt business operation is something that a good business continuity plan will cover. The plan will estimate risk, recommend steps to mitigate the risk, provide disaster recovery instructions, and include a plan for bringing the business back to normal operation.

---

**TIP** The disaster recovery plan is part of the business continuity plan. Traditionally, disaster recovery planning grew out of a need to ensure that data processing could continue even if the data center was not available. In the hearts and minds of IT, disaster recovery is business continuity. To the organization, however, disaster recovery is only the immediate steps that keep the business in operation, while business continuity includes steps that bring operation back to normal and comprehends all business operations, not just IT. One example of such a distinction is that disaster recovery might include moving operations to an alternative IT site after a fire, while business continuity would go further and include the building of a new data center.

---

These are the steps involved in business continuity planning:

1. Determine the plan scope.
2. Perform business impact assessment.
3. Develop plans for continuance of each business process.

4. Test the plans.
5. Implement the plans.
6. Maintain the plans.

## Determine Plan Scope

While the goal of business continuity planning is to provide plans for all business operations, this is not always possible if no plan has ever been developed. In this case it is more likely that the organization will develop a plan based around some critical aspects of the organization. IT operations is a good candidate, but it is even more appropriate to single out specific operations such as order entry, shipping, invoicing, or other critical services and write a plan that encompasses manual operations as well as the flow of information through the network and data storage and processing.

You should determine if your organization has a business continuity plan. Next, obtain a copy to determine what has already been developed that covers IT operations. You should also research the status of disaster recovery planning at your organization. While disaster recovery is only one part of business continuity planning, you may find that disaster recovery planning exists, while business continuity planning does not, or that different groups are working at cross-purposes on these plans. From your research, you should be able to determine the scope of the current plan (or that there is no plan).

Next, determine what your role in the planning process should be. If a plan is already established, your role may be to participate in the testing and maintenance of the plan. If no plan is in operation, start by setting a scope for the plan. Pick an area that is critical and for which a plan can be developed. For example, you might start with planning for operations after a natural disaster, or of recovery after a security compromise.

### ONE STEP FURTHER

The development of intrusion detection and response activity can be considered as part of the business continuity plan. You may find management support and budget for this activity by approaching your business continuity planning team.

## Perform Business Impact Assessment

Business impact assessment (BIA) is the process of determining the impact of an event on a business process. These are the steps necessary for the assessment:

1. **Compile a list of all possible events that might have an impact on operations.** Don't forget to list every event, even if it is unlikely. Events should include not just hurricanes for coastal business and tornadoes for those in the Midwest;

each location should list all possible weather-related events. List tragedies such as fire and chemical spills. In addition, list acts of stupidity and malfeasance as well as terrorism.

2. **Identify critical services.** Critical services are those that a business cannot live without even for a short time. Examples are many of the data center operations but might not include the installation of new desktop computers. Production, order entry, shipping, and customer support of some items are critical, but vacations, renegotiation of employee benefit contracts, and the company picnic are not. You will have your own list of critical services, and you should recognize that after some time, the other operations will have to be returned to normal operation. Their replacement is also a part of business continuity planning, just not a immediately critical one in the event of a business interruption.
3. **Determine the maximum tolerable downtime (MTD) for each critical service.** The MTD is the time that is available between the cessation of operation of some critical service and the point at which the business cannot recover. The time will vary, depending on the services, the industry, the organization, and the size of the operation. Examples of MTD might be the purported two hours of downtime often quoted by major insurance companies after which they cannot survive, or the three days another company might be able to get by without shipping product. The MTD is not a number that can be pulled out of a hat; it must be arrived at by those that truly know the impact of the operation. You will have to obtain these numbers from management in the specific area. Many times, the MTD is arrived at by calculating the monetary loss that interruption of service will cause, but monetary loss is not the only factor. MTDs for IT are often determined by the operations that are performed for others. Internal IT MTDs are also important.
4. **Prepare a full report that lists all information and orders critical services by their MTDs.** Those operations that can cause the business to fail in the least amount of time are important to identify and to protect. A report on the BIA serves several purposes. Because it identifies the most critical operations over time, it is essential in the business continuity planning process. It also provides support for planning and expenses that will prevent or mitigate the impact of some disasters.
5. **Return the report to business units for validation before using in any planning.** It is important that numbers are validated, and that all parties have had the opportunity to review the information.
6. **Provide the report with recommendations for further work to senior management.** Senior management support is necessary in order to fully plan for business continuity and to implement operations that will either mitigate the impact of business interruption events or deal appropriately with them.

## Reasons for Business Failure

Many things contribute to business failure. Loss of revenue is not the only factor that should be taken into consideration during the calculation of MTD. Other items include impact on other operations, loss of sales, lost clients, increased expenses, expenses necessary to restore normal operations, fines and penalties, and additional monies expended for legal and civil obligations.

## Perform Risk Analysis

Where BIA seeks to identify how quickly operations must be operational after an interruption, risk analysis seeks to identify how likely a specific threat is to cause an interruption, and it seeks to place a cost for mitigating the risk. Risk analysis is often performed in order to develop a threat model for information systems. The rationale is that you should delegate scarce resources to develop mitigation for those threats that are most likely to occur or that may cause the most problems should they occur. Both BIA and risk analysis should be part of the preplanning phase of business continuity planning; that is why risk analysis is discussed in this section. However, risk analysis should be a part of any security evaluation of IT. Risk analysis can help you determine where to place your efforts. As in many other things, if you effectively deal with the areas that bring the most risk, you will have the most impact on security. While an organization-wide risk analysis should be undertaken as part of business continuity planning, you can perform risk analysis for the ongoing operations of IT. Risk analysis should also be a part of the planning for the implementation of new systems, and of the proposed changes to others.

Risk analysis can be broken down into several steps:

- 1. Identify assets.** Some threats are specific to a type of asset. If you do not have that asset, you are not going to experience loss as a result of a threat to that asset.
- 2. Assign value to assets.** Knowing what is at risk is important, as it influences what you might spend to protect it.
- 3. Identify risks.** All risks should be listed with no attempt to filter for probability. Probability is important, but it is only one thing to consider when preparing a response to potential threats.
- 4. Identify single loss equivalency (SLE).** For each risk and each asset, determine the loss possible if the risk became reality. This is different than determining the asset value. For example, if a sprinkler system breaks and destroys an e-commerce server, the server's replacement may be a few thousand dollars, but the loss potential should also include the money lost because orders cannot be placed at the server. This loss can be calculated by examining the amount of revenue gained during a similar time period.

5. **Identify annual loss equivalency (ALE).** This calculation multiplies the SLE by the number of times the incident might be expected to occur in a year. Determining the probability that a specific incident will happen at all, let alone how many times a year it might happen, is not easy. However, insurance companies may be able to provide some information based on history. Experienced employees and consultants can also help. For example, if no antiviral products are in use, and patches are not kept up to date, many would argue that there is a 100 percent chance that a virus or worm will infect systems within an organization of any size.
6. **Recommend countermeasures.** Countermeasures can prevent or mitigate the extent of loss. The entire reason for performing risk analysis is to determine on which assets money and efforts should be spent. This entire book has provided recommendations for hardening efforts that are countermeasures for known and unknown risks.

## Develop Plans

After information about critical operations has been compiled, proceed with the development of business continuity plans. The following actions should be considered.

- **Prevention** Preventive plans consider what can be done to prevent events such as fire or compromise of the computer system. These plans will include items such as fire and safety inspection, insurance review, equipment maintenance, and information security hardening.
- **Mitigation** Mitigation seeks to lessen the impact of events. Items include training, backups, offsite storage of backups and software, evacuation drills, and intrusion detection and response.
- **Emergency response** Emergency response includes those actions taken immediately to avoid injury and loss of life, as well as to alert authorities, notify management, prevent additional damage, and rescue critical data and equipment. It's important to establish procedures and make assignments and always emphasize that people are the most important assets to save by emergency response.
- **Recovery** Recovery is the activity that brings critical operations fully back online.
- **Normal operations** Steps taken when business operations return to normal, in addition to providing replacement facilities and equipment, can also include the return of less critical operations such as employee benefits.

## Test

Before a plan is implemented, test parts of the plan. Tests can include discussion about operations with those who will have to perform the actions designated in the plans, training on procedures, simulated walkthroughs, and full tests of recovery operations. If a plan, for example, calls for rebuilding the root CA at the offsite location, a test would encompass first rebuilding the root CA on location, and then doing the same thing at the offsite location. If recovery plans include operations that are managed by third-party organizations, then tests for contact lists should be performed at all hours. Interruption events don't always happen during business hours.

## Implement Plans

Plan implementation includes more than providing each department with a copy of the plan. In many cases, plan implementation may include obtaining contracts for offsite storage and possible temporary location or other recovery efforts; increase in or different insurance; replacement of failure-prone equipment; and improvement of operations, data centers, and equipment. Also necessary may be data systems hardening steps and implementation of incident response teams or other new operations.

Employees will have to be trained, and periodic testing and maintenance planning dates established.

## Maintain Plans

Businesses change and grow over time. The critical operations of today may not even be part of the business tomorrow. Phone number change, as do personnel. Change management processes at your organization should be followed to include updates to plans, and full reviews, including annual BIA, should be accomplished.

# Generate a Security Policy

It should come as no surprise that you must have official recognition of what constitutes a secure system. Many of these policies may exist in your organization already. Many of them need adjustments, and many may not be written yet. Information on where security policy fits into the security lifecycle can be found in Chapter 13.

# Perform Hardened Operating System Installation

Many of the recommendations made in this book can be implemented during operating system installation. For example, registry configuration and security policy items that are managed by Group Policy can be applied during system installation, as can the installation of the current service pack and all known post-service pack security patches. Doing these things during or shortly after installation but before adding the computer to the network can go a long way to protect the system from compromise. Several operations will assist you in doing so.

## Prepare Default Security Templates

Many of the hardening steps recommended in this book involve changes to security policy either via Group Policy or by applying custom security templates using Security Configuration and Analysis. These methods should not be abandoned. However, the default security configuration of the operating system is created during installation by the application of default security templates. To ensure that systems are installed in the best security configuration, modify these security templates to fit your security policy, before installation. If, for example, you install the operating system from a network share, you will be adding the contents of the i386 directory from the installation CD-ROM to the share. You can then easily replace the default templates with those designed to fulfill your policy.

The default templates are for workstations, `defltwk.inf`; for servers, `defltsv.inf`; and for domain controllers, `defltdc.inf`. Take care to thoroughly test this process before implementing it in production.

## Use Slipstreaming

*Slipstreaming* is the process of incorporating service pack files with the installation files at a network share. When a computer is installed from the share, the service pack code is incorporated and the newly installed computer is at the service pack level. To slipstream service packs for Windows NT 4.0, Windows XP, Windows 2000, or Windows Server 2003:

1. Put a copy of the I386 folder on a server. For this example, our path is `C:\I386`.
2. Assuming a service pack CD-ROM is in the D drive and the path to the `update.exe` file is `D:\i386\update\update.exe`, use the following command to slipstream the service pack:

```
D:\i386\update\update.exe -S:C:\i386
```



## Use RIS to Add Service Packs During Installation

Alternatively, you can use RIS to add service packs during installation. RIS, the Remote Installation Service, was introduced with Windows 2000. Hardware-compatible PCs can boot, locate a DHCP server to obtain an IP address, connect to the network, and contact a boot RIS server to install Windows. You must create a RIS server by installing the RIS service and configuring it. For complete information on installing and configuring RIS, see “How to Use Remote Installation Service to Install Windows Server 2003 on Remote Computers” at <http://support.microsoft.com/default.aspx?scid=kb;en-us;325862>.

When RIS is installed, it creates many folders and files for creating RIS installations, including templates for the files that you must build to support specific installations. One template, `ristndrd.sif`, is the sample RIS template for creating an unattended installation file. You can rename the file, but you must use the correct syntax and keep the `.sif` extension. To include service packs:

1. Copy `update.exe` from the service pack to the `sp` subfolder of a network share.
2. Call `update.exe` by placing two commands in the `[GuiRunOnce]` section of the `ristndrd.sif` file. (After a reboot, RIS performs an administrative logon, and these commands will run.)

```
net use n: \\server\share password /USER;username /persistent:no
```

```
N: \sp\update.exe -u
```

3. Save the file.

## Install Hotfixes During Installation

In addition to installing service packs during installation, install hotfixes. To do so, use the `cmdlines.txt` file approach, the `srvpack.inf` approach, or RIS.

### Use `Cmdlines.txt`

To install hotfixes during installation, set up an automated installation using Setup Manager. Setup Manager (`setupmgr.exe`) can be found in the `deploy cab` file of the `\support\tools` folder of the Windows Server 2003 installation CD-ROM. This file can be used for both Windows Server 2003 and Windows XP. Windows 2000– and Windows NT 4.0–specific Setup Manager files must be used to prepare automated installations.

1. Create a folder to be used for distribution.
2. Use the Setup Manager tool to create the answer file, and name it `unattend.txt`. This file can be used to contain computer-specific information that might be needed by commands in the `cmdlines.txt` file. Instructions for creating the answer file are located at [www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/all/deployguide/en-us/acicb\\_ui\\_dmof.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/all/deployguide/en-us/acicb_ui_dmof.asp).

3. Use the Setup Manager tool to create `cmdlines.txt`. Command lines placed in this file will run during the GUI part of Windows installation. This is where you will place commands to install hotfixes. Help in using `cmdlines.txt` can be found at [www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/all/deployguide/en-us/acicb\\_ui\\_yext.asp](http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/Default.asp?url=/resources/documentation/windowsserv/2003/all/deployguide/en-us/acicb_ui_yext.asp).
4. Add hotfix command lines to the [commands] section of the `cmdlines.txt` file. An example hotfix command line that would install the Q123456 hotfix is  

```
"Q123456 /q"
```
5. Add the I386 folder from the installation CD-ROM to the folder.
6. Add `cmdlines.txt` and `unattend.txt` to the `i386\%OEM%` subfolder
7. Add hotfix executable files to the `\i386\%oem%` subfolder.

### Use `svcpack.inf`

Another way to install Windows and include current hotfixes is to use the `svcpack.inf` file. You must have a service pack- integrated Windows version.

---

**TIP** The `/Q` switch, when used with the **update** command, does not provide information during file extraction. The `/N` switch prevents backup of older files, and therefore the hotfix cannot be uninstalled. The `/Z` switch prevents a reboot after the install.

---

1. Prepare a distribution share.
2. Create an I386 folder within the share.
3. Xcopy files and folders from the installation CD-ROM to the i386 folder.
4. Open `i386\dosnet.inf` in Notepad.
5. Find the `uniproc` line in the [OptionalSRCDirs] section of the file.
6. Add a line right after this that contains the word **svcpack**. The section will look like  

```
[OptionalSRCDirs]
uniproc
svcpack
```
7. Save the file and close it.
8. Create the `i386\svcpack` folder.
9. Copy hotfix executables to the `i386\svcpack` folder.
10. Rename the files using the 8.3 naming format. The files should have the form `Qxxxxxx.exe`.

11. Use the *filename* `-x` command to expand each hotfix to a unique temporary location.
12. Hotfixes provide new files and replacement files. For each replacement file, delete the original file from the I386 folder.
13. Copy the sp3.cat catalog file to the distribution folder if the sp3.cat file is later than the one in the distribution folder. (Use the catver.exe tool to determine the versions of the sp3.cat files.)
14. For each hotfix, copy hotfix files from the temporary folders to the distribution folder. If any of the hotfix files are in a subfolder, copy the folder and its contents to the distribution folder. (Do not copy symbols subfolders or the hotfix.exe, hotfix.inf, update.exe, update.inf, spcustom.dll, spuninst.exe, update.ver, or spmsg.dll files.)
15. Delete the i386\svcpack.inf file.
16. Create a new svcpack.inf file with Notepad and include these lines:

```
[version]
signature="Windows NT$"
MajorVersion=5
MinorVersion=0
BuildNumber=2195
[SetupData]
CatalogSubDir="I386\svcpack"
[ProductCatalogsToInstall]
Qxxxxxx.cat
[SetupHotfilesToRun]
```

17. Note the Qxxxxxx.cat entry under ProductCatalogsToInstall. Add a line for each catalog file provided with a hotfix.
18. Add a line in the [SetupHotfixesToRun] section of the file using the following format:

```
Qxxxxxx /q /n /z
```

19. If hotfixes include replacement drivers, edit dosnet.inf and add the following lines:

```
[OptionalSrcDirs]
svcpack
```

20. Force the use of new drivers by adding the driver name to the ForceCopyDriverCabFiles section as shown here for the usbhub.sys driver:

```
[ForceCopyDriverCabFiles]
usbhub.sys
```

21. Run Windows (2000, Server 2003, XP) setup.
22. Verify that hotfixes install by looking for them in the Add/Remove Programs tool in the Control Panel, as well as in the uninstallation folders for each hotfix in the %systemroot% folder.

### Use RIS

To use RIS to install hotfixes:

1. Put patches on an accessible network share.
2. Configure RIS to install the most current service pack.
3. Add script lines to the [GuiRunOnce] section of the unattended installation file.

## Harden Operating System, Application, and Data Protection

The first 12 chapters of this book outline the steps to harden Windows networks. In addition to these steps, you should learn and use appropriate steps to harden the other operating systems that you use, your network infrastructure, and the other components of your information systems. You will find a wealth of information in other books in this series, including these:

- *Hardening Network Infrastructure* by Wesley Noonan (McGraw-Hill/Osborne, 2004)
- *Hardening Linux* by Paul Love, Ronald P. Reck, John Terpstra (McGraw-Hill/Osborne, 2004)
- *Hardening Enterprise Security* by the Kansas City Five (McGraw-Hill/Osborne, 2004)

## Manage Changes with a Formal Change Management Program

You will never secure your Windows network. Never. There are three reasons for this:

- **There is no such thing as perfect security.** There will always be a way that a determined attacker can compromise a system. We can only harden systems against known vulnerabilities and use standard security practices that *may* protect systems from as-yet unknown vulnerabilities.

- **New applications, new hardware, new systems, new infrastructure, and new people are constantly being added.** Each one of these brings the potential of introducing a new vulnerability.
- **The best security plans are worthless if they are not enforced.** Security policy may be disregarded, or temporary changes may be made that weaken security.

But there is hope. Everything that you do to increase the security of your Windows systems sets speed bumps and roadblocks in the way of those who would attack your systems. To keep these stumbling blocks enforced, you must implement a formal change management program. A *change management program* forces a review and approval process whenever changes are made to any aspect of information systems. These changes include software updates, hardware replacement and repairs, configuration changes, and anything that means something will be different.

Windows configuration changes (including scripts and Group Policy changes) and patching are two small parts of the program and represent two types of changes that must and can be handled by change management. Upgrades, migration, new installations, and change management programs are usually handled by committees composed of representatives from different areas of the organization, not just IT, and that may have a temporary membership when a specific area is being addressed. Typically, the change management program moves slowly and deliberately to weigh the impact and cost of proposed changes. If changes are approved, the exact procedures used for making them may be detailed along with the testing process and an audit of their correct installation and the actual impact.

Many Group Policy configuration changes will not suffer from an exhaustive review; in fact, a comprehensive examination of what they mean, how they relate to other settings already in place, and what their impact will be is a good thing. As you may have discovered, improper or untested changes to Group Policy can destroy the operation of your network just as surely as any directed attack. On the other hand, some changes to systems must be made quickly. A good change management program will have a separate procedure for things such as patching and emergency security configuration changes.

Change management offers the following benefits for security:

- Proposed changes are studied for their impact on existing systems. Current hardware, software, and wetware (people) systems are studied.
- A discussion of proposed security changes presents an opportunity for educating management about the need for security and for specific security initiatives.
- Changes that would weaken security are also subject to intensive review and may be thwarted.

## Upgrades, Migration, Replacements, and New Installations

The earlier section “Perform Hardened Operating System Installation” details the steps to be used to ensure that new installations join the network already secured. An established plan for providing replacement systems and new installations of currently

approved versions of Windows is not part of the change management program except as change management approves service packs and hotfixes, and installation practices must be in sync with this process.

Upgrades and/or migration to newer versions of the operating system, should, however, be considered by the change management process.

## Security Configuration Change

As you attempt to institute changes to the security practices of your organization, you may feel frustrated by formal change management processes. You should, instead, champion the process. Yes, change management can delay the implementation of practices that you and I deem imperative for good security. But this same careful consideration and lumbering progress can also mean that once implemented, good security will not be lightly tossed aside.

Still, there will be times when a security configuration change must be made immediately in order to secure the network. You may find that a service pack has re-enabled a service deemed risky for your organization, or implemented a default action that now must be turned on if you are to maintain your current security status. The trick is to understand the change management process and obtain a procedure that pre-approves changes that perform maintenance, and fast-tracks emergency changes.

An important thing that should be established is the “how” of security configuration change. The approval of the actual change should be a different decision. For example, if Group Policy is used to apply security configuration changes, then once a change is approved, no discussion is required on how the change will be made.

## Patch

It was not that long ago that common wisdom was “If it’s not broke, don’t fix it.” In other words, even if Microsoft produced a patch or a service pack, no one got excited about implementing it. It is hard to realize that the patching process has become a major part of network administration in only the last couple of years. Any network administrator who does not understand that she must implement a sound patching program condemns her network to at least massive worm and virus attacks on a periodic basis and at worst gives up systems to attackers for the asking. You must patch, what’s the best way?

Patching is a process that is best served by developing a procedure in concert with change management that gives systems administrators the responsibility for testing and approving each patch in concert with areas of the organization that may be impacted by the patch or lack of a patch. The patching process procedure should include the following steps:

1. Filter.
2. Order.
3. Obtain.

4. Test.
5. Apply.

## Filter

First consider, which patches may impact which computers? Some patches are issued for products that are not used in your organization. They do not have to be considered, but all patches should be reviewed.

## Order

Putting the current patches in order means determining which are the most critical to apply, which are next most important, and so on. Microsoft's rating can assist you in this determination, but other resources should be used as well. If you subscribe to security lists, the discussions in these lists can help you determine how to rate the vulnerabilities that the patches fix. If, for example, there is discussion or evidence attack code that seeks to leverage the flaw, then you might rate the patch as more important. Two types of security lists can help. The first lists are primarily notices of vulnerability and patch availability. These are lists such as

Microsoft's Security Bulletin Notification Service ([www.microsoft.com/technet/security/bulletin/notify.msp](http://www.microsoft.com/technet/security/bulletin/notify.msp))

Microsoft's Security Newsletter ([www.microsoft.com/technet/security/secnews/default.msp](http://www.microsoft.com/technet/security/secnews/default.msp))

CERT Coordination Center ([www.cert.org/](http://www.cert.org/))

You can also read Microsoft's security bulletins online at [www.microsoft.com/technet/security/default.msp](http://www.microsoft.com/technet/security/default.msp). Security discussion lists are a second type of list. Many of these also copy the Microsoft security bulletins, or provide pointers to them. In addition, you will find other, nonofficial vulnerability notices, discussion of problems installing patches and service packs, and other security topics.

- For a Windows-specific security list, sign up for ntbugtrac at [www.ntbugtraq.com/](http://www.ntbugtraq.com/).
- A moderated list for security information, bugtrac can be read or subscribed to at [www.securityfocus.com/archive/1](http://www.securityfocus.com/archive/1).
- Subscribe to an unmoderated vulnerability list, full-disclosure at <http://lists.netsys.com/mailman/listinfo/full-disclosure>.

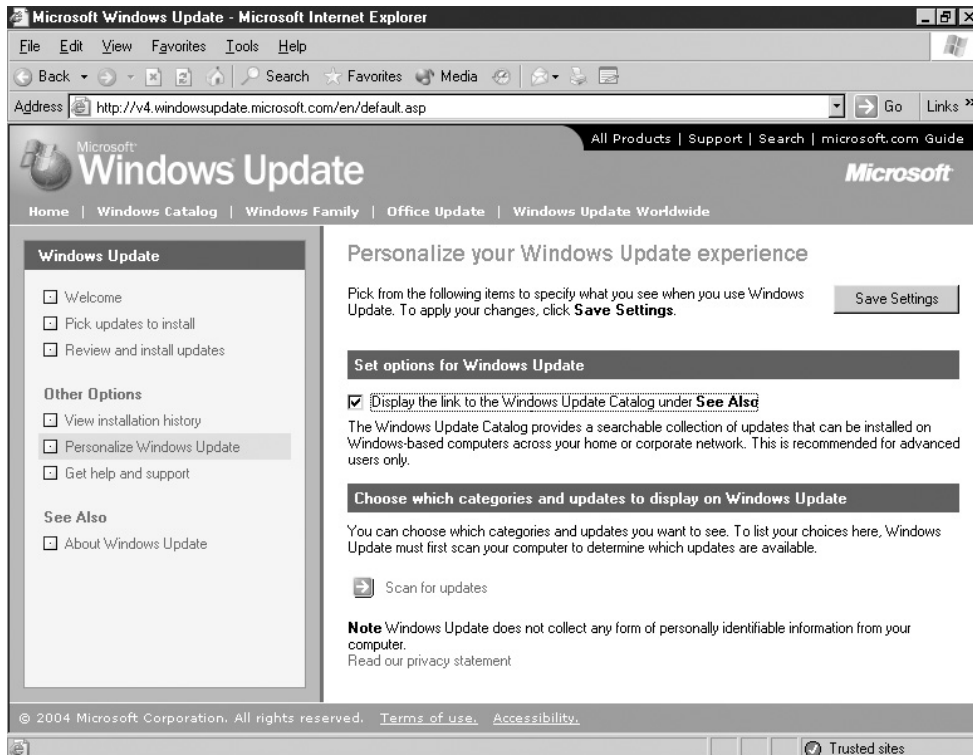
You will also need to determine your own network's needs. The requirements for isolated environments will be very different from mobile systems and those directly exposed to the Internet. Deciding which systems to apply patches to in what order may also be part of your planning.

## Obtain Patches Directly

Service packs and patches should be obtained only by downloading directly from Microsoft. Several methods are available, including using the Windows Update catalog, direct downloading from the Microsoft download site, or taking advantage of the automatic downloads made possible by Windows Software Update Services (SUS).

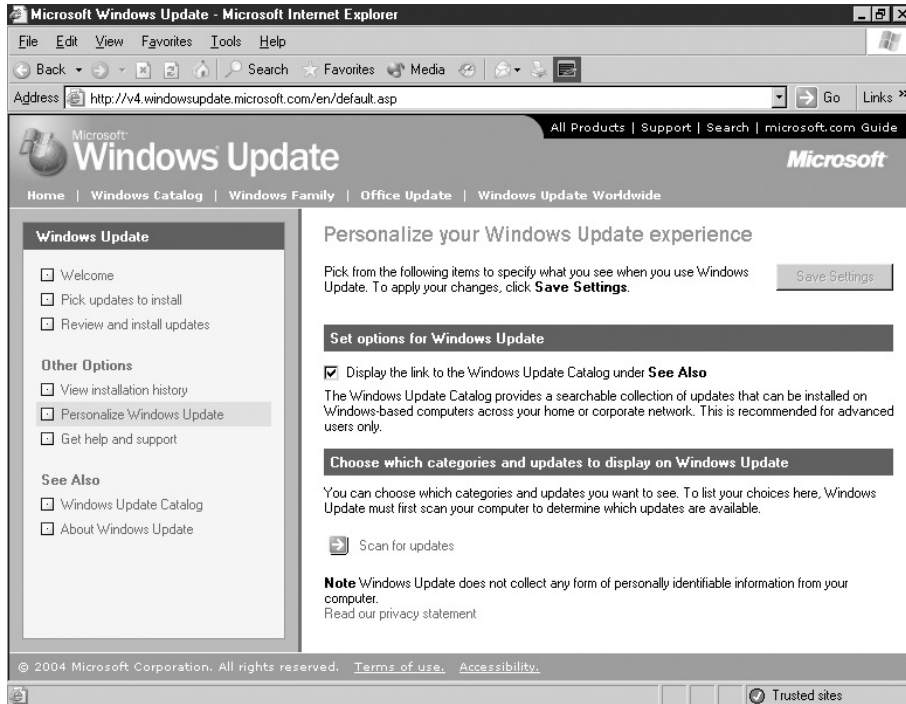
To obtain patches using the Windows Update Catalog:

1. Browse to Windows Update (<http://v4.windowsupdate.microsoft.com/en/default.asp>) or select Windows Update from the Tools menu of Internet Explorer.
2. In the Other Options section, click Personalize Windows Update.
3. Under the Personalize Your Windows Update Experience section, check Display the Link to the Windows Update Catalog under See Also as shown here:

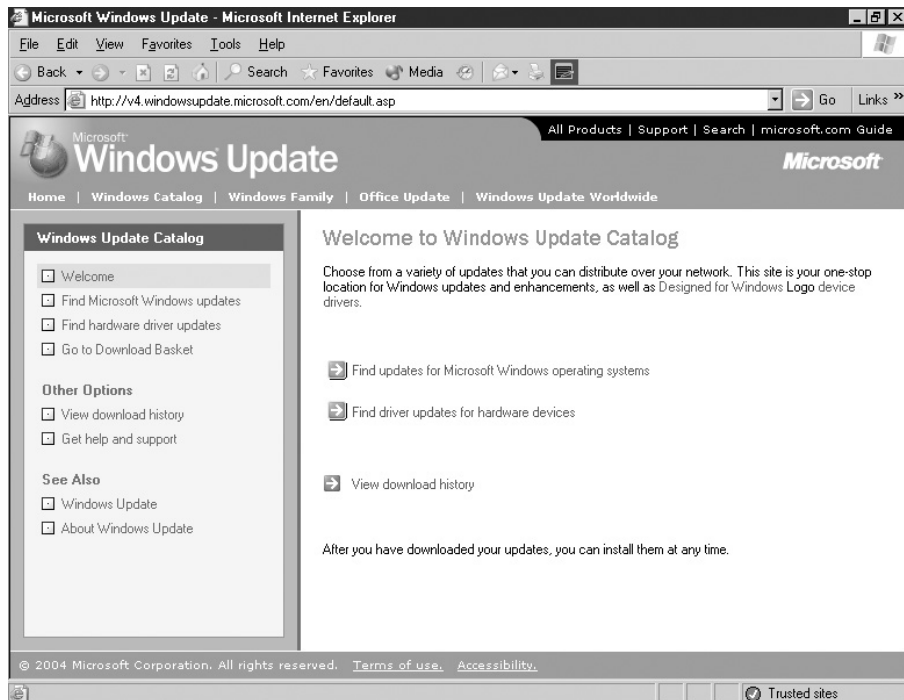


4. In the upper right-hand corner of the window, click Save Settings.
5. Click the Windows Update Catalog listing now displayed under the heading See Also in the left pane as shown here:

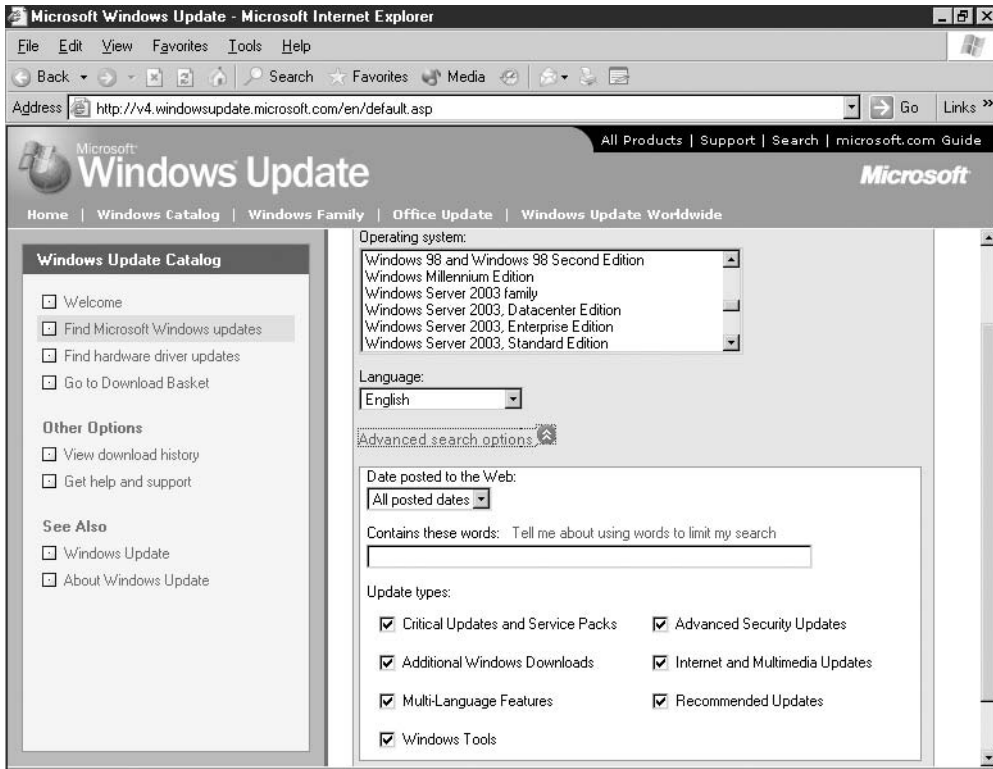




6. Select Find Updates for Microsoft Windows Operating Systems as shown here:



7. Select the operating system from the Operating System drop-down list. (Note that you can find updates for Windows 98 as well as for more recent versions of the OS.)
8. Click the Advanced Search options and set as necessary as shown here:



9. Click Search.
10. When the search is complete, select from the list presented to display brief descriptions of the available patches.
11. Click the Add button adjacent to each patch in order to select it for download.
12. When you have selected all updates, click Go to Download Basket as shown here:

The screenshot displays the Microsoft Windows Update website interface. The browser window title is "Microsoft Windows Update - Microsoft Internet Explorer". The address bar shows the URL "http://v4.windowsupdate.microsoft.com/en/default.asp". The page header includes the Microsoft logo, "Windows Update", and navigation links: "All Products | Support | Search | microsoft.com Guide". Below the header, there are links for "Home | Windows Catalog | Windows Family | Office Update | Windows Update Worldwide".

The main content area is titled "Your search returned 38 results" and includes a sub-header "Select from the list below to see updates found in each category." Below this, there are three categories: "Critical Updates and Service Packs (31)", "Multi-Language Features (1)", and "Recommended Updates (6)". A "Go to Download Basket" button is present, along with a "Total items in Download Basket: 1" indicator. A "Sort by: Title" dropdown menu is also visible.

The detailed view of a "Security Update for Windows Server 2003 (KB8830352) - (Posted Date: February 09, 2004)" is shown. It includes a description: "A security issue has been identified that could allow an attacker to compromise a computer running Microsoft Windows Internet Naming Service (WINS) and gain control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer. Read More..." and an "Add" button.

13. Enter or browse to the location where you want to store updates.

14. Click Download Now.

## HEADS UP!

Other methods for downloading patches exist. The Windows Update site can be used to scan a local computer and recommend necessary patches as well as provide a way to download and install them. Automatic Update can be configured to notify users that patches are available for download and then provide the means to carry out the downloads. However, these methods do not allow testing of the patch, nor are they reasonable methods in an enterprise environment, since it would be difficult to get users to use Windows Update and Automatic Update would unnecessarily consume bandwidth. These methods may be okay in smaller environments or as emergency measures for mobile systems. A list of recommended and tested patches could be prepared by administrators, and mobile users could be taught how to use other means to select, download, and apply patches.

## Obtain Patches Using SUS

SUS is a free tool that can be used to create the backbone of an automated patch download and application service for Windows 2000 SP3 and above, Windows XP SP1 and above, and Windows Server 2003. While downloading is automated, it can be configured to require an administrator request. What's more, downloaded patches must be approved before they can be distributed and applied, and clients must be configured before any patches will reach servers and desktops.

SUS must be installed on a Windows 2000 or Windows Server 2003 domain member computer. (SUS can be installed on a domain controller, though this is not recommended.) To install and configure SUS:

1. Download SUS from [www.microsoft.com/downloads/details.aspx?FamilyID=a7aa96e4-6e41-4f54-972c-ae66a4e4bf6c&DisplayLang=en](http://www.microsoft.com/downloads/details.aspx?FamilyID=a7aa96e4-6e41-4f54-972c-ae66a4e4bf6c&DisplayLang=en).
2. Make sure to read the requirements for installation, including the requirement for IIS. (You must allow Active Server Pages.)
3. Double-click the executable, and then Next at the welcome screen.
4. Accept the license agreement and click Next.
5. Click Custom Installation.
6. Select Save the Updates to This Local Folder in order to have clients update from the computer on which SUS is installed. Click Next. (Alternatively, you can direct SUS clients to the Microsoft Windows Update Server.)
7. Check English Only, or accept the default of all languages (or select specific languages), and then click Next. (This is an important step, as the time for downloading patches in a language you don't need, and the disk space for storing them, is a waste.)
8. Leave the default I Will Manually Approve New Versions of Approved Updates and click Next.
9. Click Install.
10. When installation is complete, it will attempt to take you to the <http://localhost/susadmin> site so that you can configure the system. You can, of course, administer SUS from your administrative workstation.
11. Use the susadmin pages to configure SUS.

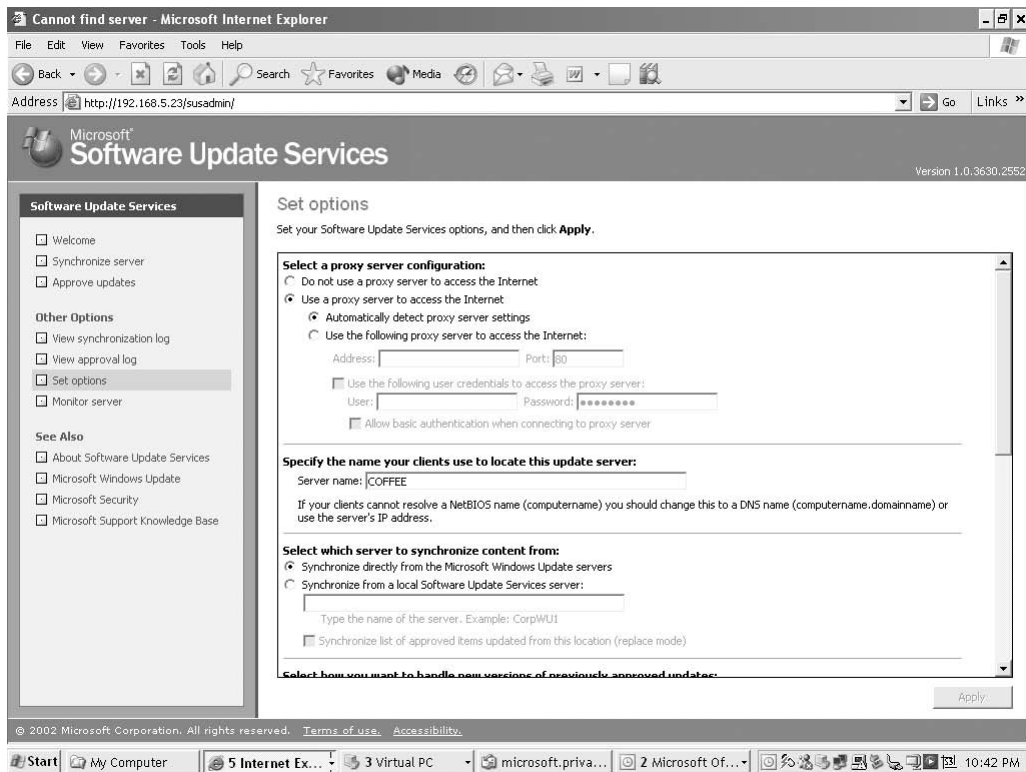
---

**NOTE** Internet Explorer on Windows Server 2003 is configured by default in a restricted mode, and you may not be able to immediately access the SUS administration site.

---

To configure SUS:

1. Open the SUS administration page at `http://server_name/susadmin`.
2. In the left pane, click Synchronize Server.
3. Configure synchronization. Click Synchronization Schedule. The server can be set to automatically synchronize with Windows Update (download new patches and service packs), or you can choose to synchronize manually. If you choose this option, make sure to sign up to be notified when new software has been added for download.
4. Click OK.
5. In the left pane, click Set Options as shown next. Options are to configure the proxy server, choose the server name used by clients to access the server, point the SUS server to another server for updates, decide which language updates should be downloaded, and so forth.



6. Synchronize the server. Click Synchronize Now to download the most recent service pack and hotfixes.

7. Once you have tested updates, use the View Approval Log option to approve service packs and hotfixes for distribution as shown here:

Cannot find server - Microsoft Internet Explorer

Address <http://192.168.5.23/susadmin/>

Microsoft  
**Software Update Services**  
Version 1.0.3630.2552

**Software Update Services**

- Welcome
- Synchronize server
- Approve updates

**Other Options**

- View synchronization log
- View approval log
- Set options
- Monitor server

**See Also**

- About Software Update Services
- Microsoft Windows Update
- Microsoft Security
- Microsoft Support Knowledge Base

**Approve updates**

Choose the updates that you would like to distribute to your clients, and then click **Approve**.

**Available Updates** Sort by: Status

<input checked="" type="checkbox"/>	<b>Critical Update for Microsoft Windows XP Media Center Edition Infrared Receiver (KB832418)</b> , 3/8/2004 (New)
	Download size: <b>328 KB</b> This driver update contains the latest firmware for the hardware and the required functionality of the latest version of Windows XP Media Center Edition. It supports all versions of the infrared receiver (IR) through Microsoft Windows XP Media Center Edition 2004. After you install this item, you may have to restart your computer. Once you have installed this item, it cannot be removed. Details...
	Applies to: Windows XP SP1
<input checked="" type="checkbox"/>	<b>811493: Security Update (Windows 2000)</b> , 3/5/2004 (New)
	Download size: <b>5.2 MB</b> A security issue has been identified that could allow an attacker to compromise a computer running Microsoft® Windows® 2000 and gain complete control over it. An attacker would need the ability to log onto the computer locally to carry out an attack. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer. Details...
	Applies to: Windows 2000 SP2, Windows 2000 SP3
<input checked="" type="checkbox"/>	<b>Critical Update for Windows Media Player Script Commands (KB828026)</b> , 3/5/2004 (New)
	Download size: <b>2.8 MB</b> This update contains a change to the behavior of Windows Media Player's ability to launch URLs in the local computer zone from other zones. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer. Details...
	Applies to: Windows 2000 Professional SP3, Windows 2000 Professional SP4, Windows 2000 Server SP3, Windows 2000 Server SP4, Windows Server 2003 Family, Windows XP RTM, Windows XP SP1, Windows 2000 Advanced Server SP3, Windows 2000 Advanced Server SP4
<input checked="" type="checkbox"/>	<b>Flaw In Windows Media Player May Allow Media Library Access (819639)</b> , 3/5/2004 (New)
	Download size: <b>2 MB</b> An identified security issue in Windows Media Player 9 could allow an attacker to see certain information on your computer after you viewed a Web page. For instance, this issue could allow an attacker to view information about your media library and modify it. By installing this update, you can help protect your computer. After you install this item, you may have to restart your computer. Details...
	Applies to: Windows Server 2003 Family

Approve

© 2002 Microsoft Corporation. All rights reserved. [Terms of use](#). [Accessibility](#).

Start My Computer 5 Internet Ex... 3 Virtual PC microsoft.priv... 2 Microsoft Of... 10:35 PM

## ONE STEP FURTHER

Your test environment for patches should be large enough to test different configurations. You can simplify the distribution of patches to a large test environment by providing a SUS server specifically for the test systems. To avoid having multiple downloads of the same patches, you can chain the production SUS server and the test SUS server so that one gets new updates from the other instead of making its own requests from Microsoft. Since patches must be approved before they are distributed to clients, you can delay application to the production network until patches pass testing. Simply delay approval of any patch on the production SUS server until your testing is complete.

## Test

You can find anecdotal evidence that supports whatever you want to believe about the problems that hotfixes can cause. Horror stories about machines that crashed and required operating system installation abound, as do testimonials that in five years only one hotfix caused a problem and that was with one machine with special hardware.

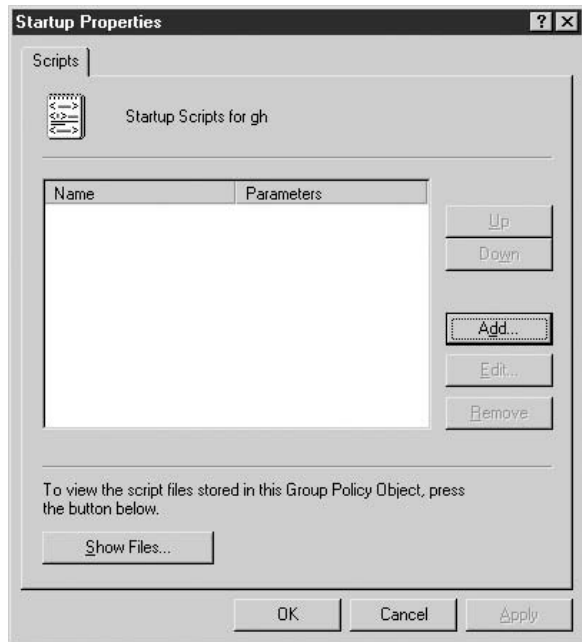
The reality, of course, is that both situations can occur, and the proper response is to test all hotfixes before adding them to production machines. Ideally, tests should be run on systems as close to those in production as possible, though even this is no guarantee. After testing, automated installation to most desktops and less critical servers should be scheduled. For critical servers, updating should be approached with caution and you should be prepared to deal with the unexpected.

## Apply Updates Using Group Policy

If your organization has more than a few seats, you will need some automated way to apply approved patches. Many third-party solutions are available. Two easy ways to automate updating of approved patches using native tools are to use a logon or startup script or to use SUS.

To use Group Policy, create a script that checks for file versions and installs patches if they have not been installed.

1. Determine which OUs contain computers on which the update should be applied.
2. Create a GPO and link it to these OUs.
3. Open the GPO in the editor and navigate to Computer Configuration, Windows Settings, Scripts.
4. Double-click Scripts and then Startup.
5. Use the Add button on the Scripts page as shown in the illustration.
6. Browse to the script file, add any parameters in the Script Parameters box, and click OK twice.
7. Allow Group Policy to replicate.
8. Reboot computers. The patch is applied on reboot.



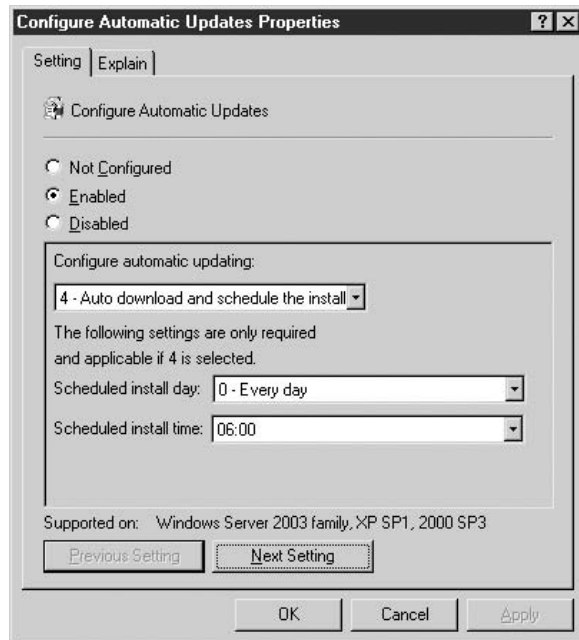
## Apply Updates Using a Script

Using Group Policy is not the only way to use a script to apply patches. You may wish to provide an IP address file of computers to update, a network patch location, and a script that uses both to apply patches to multiple computers. A detailed explanation and example script can be found in the article “How to Use a Visual Basic Script to Install the 824146 (MS-03-039) or 823980 (MS03-026) Security Patch on Remote Host” at <http://support.microsoft.com/default.aspx?scid=kb;en-us;827227>.

## Apply Updates Using SUS

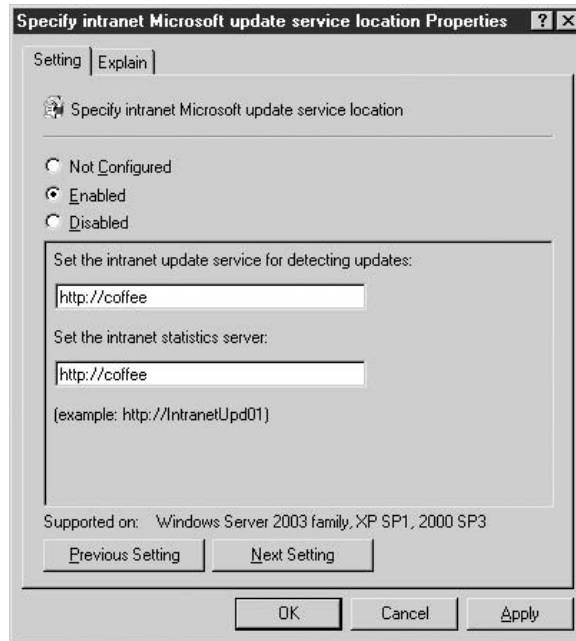
SUS can be used to apply updates if SUS clients are configured. (Windows XP SP1 and above, Windows 2000 SP3 and above, and Windows Server 2003 can be SUS clients.) SUS clients are configured through Group Policy. For Windows 2000 domains, add the wuau.adm template to the Computer Configuration, Administrative Templates node. The wuau.adm template is provided with the SUS download. The template is already installed in Windows Server 2003.

1. Expand the Computer Configuration, Administrative Templates, Windows Components node and select Windows Update.
2. Double-click Configure Automatic Update Properties.
3. Click Enabled.
4. Select number 4, Auto Download and Schedule the Install. (Under Configure Automatic Updating, Notify for Download and Notify for Install will prompt users to request updates and to install updates at their leisure. Auto Download and Notify for Install requires the user to request the install.)
5. Use the scheduling day and time boxes to select the time for installation as shown in the illustration.



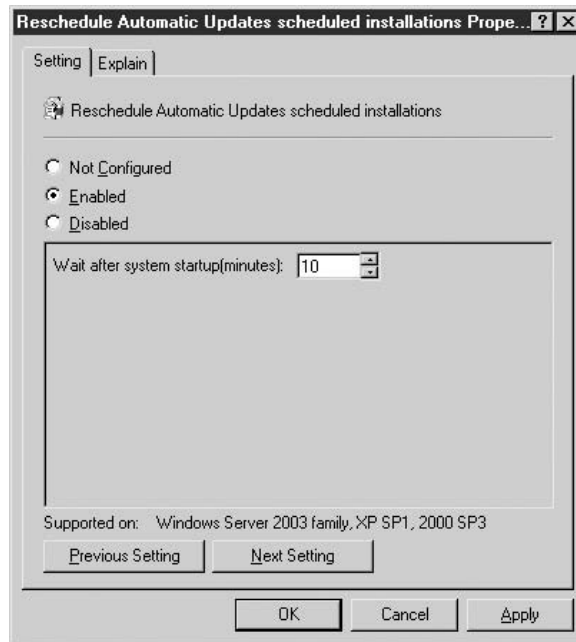


6. Click Next Setting to move to the Specify Intranet Microsoft Update Service Location.
7. Click Enabled.
8. Enter URLs for the update server and intranet statistics server as shown next. (If you have one SUS server, these will be the same.)



9. Click Next Setting to move to the Reschedule Automatic Updates Scheduled Installations page.
10. Click Enabled.
11. Enter a number in the box for Wait After System Startup (minutes) as shown next. This number is the number of minutes after computer startup that the system will wait before installing a missed scheduled install. A missed scheduled install could happen if, for example, the schedule to install updates is set for 5 P.M., an update is awaiting installation, and the user turns off their computer at 4 P.M. If the Reschedule Automatic Updates Scheduled Installation

setting is enabled, once the system is rebooted, the system will wait the set number of minutes and then install the update.



12. Click Next Setting to move to the No Auto-Restart for Scheduled Automatic Updates Installations.
13. Click Enabled. This setting prevents the system from restarting automatically even though the update requires it. Those patches that require a restart will not be fully installed until the system is rebooted.

## HEADS UP!

Automatic restart after patch application is a problematic option. If desktops are left on all the time and patches are never applied except when no user will be using them, then you've solved one problem by introducing another. When desktops are left on all the time, they may be more easily targeted for attack. However, if desktops are rebooted at an arbitrary time, when users may be working, there may be loss of data or other problems. Yet to allow users to be in control of when and whether updates are installed is unacceptable. It seems the best solution is to schedule updates but prevent automated reboots and ensure that reboots do occur. Similar issues affect servers; however, the problem is that many servers today must be operational 24 × 7, so reboots must be planned and administrators will have to understand which patches require reboots and which ones don't so that they can schedule reboots to ensure patch application.

---

---

# Be Prepared for Disaster Recovery

All systems will eventually fail. Whether the failure is due to hardware, software, malicious attack, improper configuration, user mistake, or any other reason, the most important thing is to restore service. You cannot do so if you are not properly prepared.

---

**TIP** KB article 287061, “Windows NT 4.0 and Windows 2000 Disaster Recovery and Backup and Restore Procedures,” contains links to articles on disaster recovery. Go to <http://support.microsoft.com/default.aspx?scid=kb;en-us;287061>.

---

## Use Fault-Tolerant Configurations

Many fault-tolerant devices are available that can prevent hardware meltdown from becoming network meltdown. Use RAID drives to prevent drive failure from requiring a restore. Investigate, test, and use other hardware devices that work in tandem—when one fails, the other takes over or continues on. Use clustering to provide fault tolerance for database and other cluster-aware applications. Use load balancing to link multiple servers such as firewalls. When one server fails, the load is automatically redirected to other servers. Use duplicate servers and configure network devices or software applications to use either. DNS is a good example of this; client TCP/IP protocol configuration provides the ability to list two DNS servers. If one is not available, the system will automatically attempt to use the other.

## Schedule and Perform Backups

In order to properly prepare for recovery, you must back up data and system configurations. The procedures for actually performing backups are simple. However, the creation of a complete backup plan and its management is not.

### Create Backup Data Plans

Some data may be disposable, such as documents downloaded from web sites for browsing, statistics downloaded from a central server on a daily basis, temporary files, and other information. However, to ensure the recovery of data that is not, you must have a plan for backing up data that includes

- When to back up
- When to do full backups vs. system configuration backups vs. data backups
- What media are used
- Whether backups will be automated
- How long backups are kept

- How many times backup media will be reused
- What type of backup media will be used
- Where will offsite storage be and how often will backups be moved offsite
- Who will have access to backups
- Where will backups be stored locally
- Who can restore systems
- Which data will be backed up

---

**NOTE** In many organizations, users must store all data on network drives. It is easier to back up this data, and it is easier to restore desktop systems. When data is stored on the network, recovering a user system is usually accomplished by simply doing a reinstall. Since the standard desktop systems can be imaged, quick recovery is possible once any necessary hardware repairs or replacements are complete.

---

## Do Full System Backups

Windows provides a native tool for performing backups. While the capabilities of the tool vary depending on the operating system, the basics of its operation are very similar from version to version.

---

**TIP** System State backup can be performed only locally. You cannot back up system state to the network using the built-in tool. System state backup is not available for Windows NT 4.0.

---

To do a full system backup for Windows NT 4.0, you will need to install and configure a tape drive. Windows Server 2003, Windows 2000, and Windows XP can back up to additional media types. A member of the Backup Operators group, or a user granted the backup files and directories user right, can back up data. The local Administrators group can back up system state. To back up:

1. Open the Backup program via Start | Program Files | Accessories | System Tools.
2. Select the Backup tab.
3. Select the Drives in the left pane.
4. Select System State. (System State backup backs up boot files, the COM+ Class Registration Database, and the Registry. If the server is a domain controller, Active Directory is also backed up. If IIS is installed, the metabase will be backed up. If certificate services are installed, then their configuration is backed up. )
5. Select the backup destination (file, tape).

6. Select the backup media or filename (if a file will be used, enter the path).
7. Click Start Backup.

## Schedule Backups

Backups must be done on a regular basis. There are no set rules for frequency, but many organizations follow a daily backup plan. When the amount of data to back up prohibits backing up all data every day, a weekly full backup is supplemented by a daily partial backup that either backs up those files that have changed since the full backup (differential) or those that have changed since the last partial backup (incremental). Another type of backup that can be used backs up only those files that were created or modified on the current day. This, however, does not ensure complete recovery.

These are the important things to remember about partial backups:

- Using a differential backup will increase the amount of time needed to back up each day a differential backup is performed, as all new and changed files since the full backup will need to be backed up.
- If differential backups are made, and a computer must be restored, you will need only two backups, the full backup and the last differential created.
- Using an incremental backup will reduce the amount of time needed to back up.
- If incremental backups are made and a computer must be restored, you must use the full backup and all of the incremental backups made since the full backup.

To perform an immediate backup:

1. Open the Backup program via Start | Program Files | Accessories | System Tools.
2. Select the Backup tab.
3. Select the Scheduled Jobs tab.
4. Click Add Job.
5. Follow the wizard to configure what to back up and create a schedule.

## Regularly Back Up Configurations

In addition to performing full backups, regularly back up system state data. For Windows XP, Windows Server 2003, and Windows 2000, back up the system state and any configuration files not backed up with system state. For Windows NT 4.0, back up the registry and any configuration files and create a Windows NT 4.0 boot disk. Create an emergency repair disk for Windows NT 4.0; this process gives you the opportunity to back up the registry. (Creating an emergency repair disk does not back up the registry for Windows XP, Windows Server 2003, and Windows 2000.)

## HEADS UP!

In order to restore system state on a Windows 2000 or Windows Server 2003 domain controller, the backup must not be older than the Active Directory tombstone lifetime. The *tombstone lifetime* is the amount of time for which deleted objects remain as deleted objects in the Active Directory. (When you delete an Active Directory object, the deletion event must somehow be transmitted to all copies of the AD so that it can be deleted there as well. The tombstone is the record of a deletion event, as it is the object “marked” for deletion.) When the time is up, the tombstone is deleted. If a backup of system state older than the tombstone lifetime (by default, 60 days) is restored, all data will be rejected as out-of-date. It is simple to avoid this issue—make regular backups.

### Keep a Log of Backup Activity

When backups are made, a log is created. Print and keep backup logs. They are records of backups and may also be helpful during restore operations in locating files.

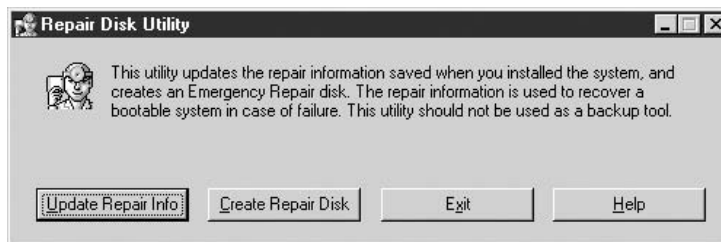
Create a manual log to record when different systems were backed up and the backup media removed. Keep details of how the media are labeled, who removed them for storage, and where they were stored. When tapes are reused, record that as well.

### Make Emergency Repair Disks

Windows 2000, Windows XP, and Windows Server 2003 emergency repair disks can be created by using the native backup tool. Making the disk also places current setting information in the systemroot\repair folder. This information may be necessary when attempting to restore the system; it might also be used to compromise the system. Manage the permissions on this folder and provide full access to only the system and Administrators.

To create an emergency repair disk for Windows NT 4.0:

1. Open a command prompt and enter `rdisk /r`.
2. In the Repair Disk Utility dialog, select Create Repair Disk as shown here:



The `/r` switch copies the information to the repair folder as well. If the data becomes too large for a single floppy, you can use the Update Repair Info button and then copy the contents of the repair folder to other backup media.

## Use Restore Points

Windows XP automatically takes snapshots of the system configuration and provides the ability to return the system to a state prior to the installation of a new driver, or a configuration change. Restore points can also be manually requested and are a good practice before making major system changes. To make a restore point:

1. Click Start | Accessories | System Tools | System Restore.
2. Click Create a Restore Point and then click Next.
3. Enter a descriptive name for the restore point and click Create.
4. Click the Home button to return to the System restore page, or close the window.

To restore the system to the restore point:

1. Click Start | Accessories | System Tools | System Restore and then click Next.
2. Use the Select a Restore Point page to select a date and then select the desired restore point.

## Plan and Perform Special Backup Operations

If you completely back up entire servers and their data, you can do a complete system restore, but what if it's simply some component of the server that fails? Or what if you simply need to move some service from a crashed server to one that is already operational?

An example of such operations would be recovery of DNS. Of course, if you have followed best practices, you have more than one DNS server. In Windows NT 4.0, you've configured a secondary DNS server. If zone transfers are a frequent part of your maintenance, then the loss of a single DNS server is not the end of networking as you know it. But what if you have only two DNS servers and both fail? Can you quickly get up and running on an existing Windows NT 4.0 server? Sure, if you've a backup of the `winnt\system32\dns` folder's file, and you have prepared a boot file or backed up the DNS registry keys.

In addition to making full backups and system state backups, you must consider the special needs of various services and applications running in your environment. Areas to consider are

- Active Directory
- DNS

- DHCP
- RIS
- Certificate services
- EFS
- Exchange Server
- SQL Server

## Practice Recovery Operations

How do you know that your backups are good? How do you know if you'll be able to recover from a disk crash or other failure? Practice. While you cannot take every backup and attempt to use it to restore every computer, you can do periodic restores and you can keep ready the information necessary to perform restores. Test this list by doing practice restores.

### Practice Restoring Active Directory

Restoring Active Directory can be a complex process. To understand the process and to be able to determine the exact steps for each situation requires detailed knowledge. The information that follows should not be used without such understanding. Many of the steps and much of the knowledge required to perform Active Directory restores is in the white paper "Active Directory Disaster Recovery" at [www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/support/adrecov.msp#XSLTsection126121120120](http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/support/adrecov.msp#XSLTsection126121120120).

Do a nonauthoritative restore to provide a basis from which to update the newly restored operating system via replication. This approach also reduces the amount of time necessary to restore the system and prevents unnecessary replication traffic. If the Active Directory is not large, this process may be forgone and the replication process will update the local copy.

1. Boot into Directory Services Restore Mode to take AD offline.
2. Select the Windows AD operating system and log on using the local administrator account and Directory Services Restore password you created during dcpromo. Then click OK.
3. Start the backup utility.
4. Click Restore Wizard and then click Next.
5. Check the System State Entry and click Next.
6. Click Finish.
7. Reboot.



Do an authoritative restore if the backup copy contains the correct Active Directory data, in other words, if you need to restore Active Directory to a state prior to that currently on the network. The authoritative restore process designates the restored AD as the copy all other domain controllers should synchronize their database with.

1. Nonauthoritatively restore AD.
2. Open a command prompt.
3. Enter **ntdsutil**.
4. Enter **authoritative restore**.
5. At the prompt, enter **restore database**.
6. Enter Quit as many times as necessary to exit ntdsutil.
7. Reboot.

Do a primary restore if you must rebuild the domain from scratch using a backup. The first DC will need a primary restore; all other DCs should be nonauthoritatively restored.

1. Use the backup utility.
2. Select System State.
3. Click the Advanced option.
4. From the Advanced Restore Options dialog box, select When Restoring Replication Data Sets, Mark the Restored Data as the Primary Data for All Replicas.

### Practice Restore Operations for Services

System state backup data, once restored, may not complete the restoration process for all services. Several services need additional steps in the restore process.

- The WINS database is restored but may be out of date. If WINS data is supported by multiple WINS databases, update WINS by performing a WINS replication; otherwise, WINS will update itself over time.
- The DHCP database is restored but may be out of date. Reconcile the restored database by selecting the scope in the DHCP snap-in, and then using the Action menu and selecting Reconcile. DHCP will operate in safe mode, querying the network to see if an address it is about to assign already exists. Quit this mode after one-half of the lease duration has expired.

### Establish and Practice Using Emergency Management Services

Windows Server 2003 introduces the ability to use Emergency Management Services (EMS) to restore a server that cannot be restored by any other means. EMS can be used

via out-of-band connections such as a null modem cable, a modem, or a service processor. EMS might also be used to disrupt server operation. Limit the ability of users to access out-of-band services by physically protecting the server and any out-of-band connections, and by selecting equipment with and using secure access mechanisms. Consider a separate management interface for out-of-band connections.

### Practice Using the Recovery Console

The recovery console is a tool provided for Windows 2000, Windows Server 2003, and Windows XP computers to assist in the recovery. You can use the recovery console to view files, change drivers, and use powerful commands to do such operations as fixing the boot sector.

Evaluate the need for and practicality of installing the recovery console. The recovery console can be used to compromise a system if its security configuration is not used. You can use the recovery console by booting from the installation CD-ROM.

To install the recovery console, you will need the Windows installation CD-ROM. If the CD-ROM is placed in the D drive, the command to install the recovery console is

```
D:\i386\winnt32.exe /cmdcons
```

## Monitor and Audit

Information systems do not escape the natural process of decay. We recognize that and monitor hardware for signs of wear. But the hardening process and its product can also decay over time. Security can also be accidentally or maliciously adjusted. The purpose of monitoring and auditing is to find those areas where this has or is occurring, prompt action to recover from any harm, and return systems to their hardened state.

### HEADS UP!

It has become common to identify the words “Perform an audit” with doing a pentest. Even more disturbing, there are those who think the first thing that should be done when building a security program is to have internal and external penetration tests performed. This is *not* the way to audit the security status of your organization. Just as security is much, much more than understanding the latest hack attack, auditing is much more than simulating attacks in order to test defenses. The proper way to establish and maintain security is to harden the network according to security principles, best practices, and the use of tested solutions to known attack vectors, and then, to test these defenses.

Monitoring encompasses periodic checking of configuration settings and regular activity review and action when something exceeds the norm. Auditing is the process of formal review of policy compliance, forensic review of collected data, and penetration testing (pentesting) of controls. Many of the same tools can be used during both activities. This book describes how to use commonly available native Windows tools, but there are many third-party tools that you may find valuable.

## Configure System Auditing

You must record activity in order to have it for review or to use in intrusion detection. To configure auditing, you must set audit processes at the system level, and to audit object level activity, you must set audit requirements on the object. In both the following examples, most, if not all, auditing choices are selected. You determine the settings to match your requirements. It is imperative to set system auditing; however, you probably will not want to set object auditing for every object. Instead, use object auditing to monitor critical or sensitive data, or to track the activity of suspects.

Windows NT 4.0 auditing settings can be set for domain controllers using User Manager for Domains and for domain members or stand-alone computers using User Manager. For other post-Windows NT 4.0 systems based on Windows NT technologies, use Group Policy. The local Group Policy may be used for stand-alone computers and to set auditing for domain members if auditing is not set at the domain level. Best practices are to set auditing for domain members by setting it in a GPO linked to the OU within which the computer account resides.

## Configure Auditing for Windows NT 4.0

Table 13-1 lists and describes audit categories for Windows NT 4.0. To configure system auditing for Windows NT 4.0:

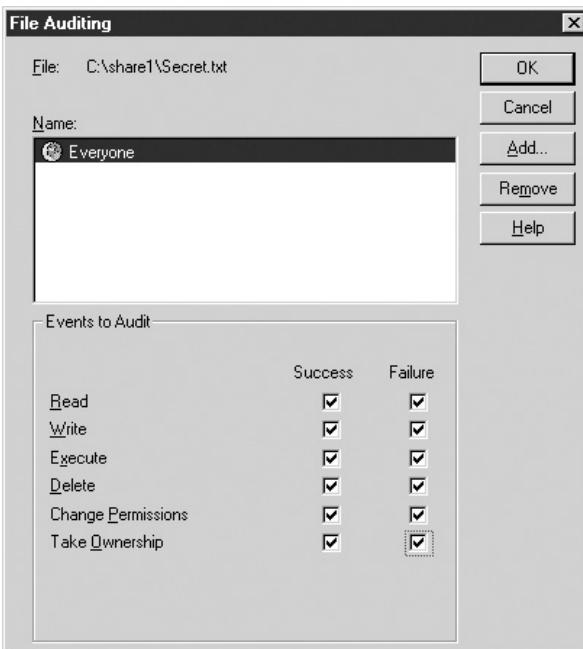
1. Select Programs | Administrative Tools | User Manager | Policies and then click Audit.
2. Select all events except Process Tracking as shown here:



3. Click OK.

Audit Selection	Description	Success	Failure
Logon and Logoff	Records user logon and logoff at the computer whose console the user is using.	Y	Y
File and Object Access	Turns on the ability to set auditing at the object level. Does <i>not</i> begin recording information until object auditing is configured on objects.	Y	Y
Use of User Rights	Records use of a right.	Y	Y
User and Group Management	Records changes to users and groups.	Y	Y
Security Policy Changes	Records changes to audit settings.	Y	Y
Restart, Shutdown, and System	Records typical system events.	Y	Y
Process Tracking	Creates an event for every action a process takes. Does not provide useful information except where software is being tested. Set on test systems only.	N	N

**Table 13-1.** Audit Policy for Window NT 4.0



To set object auditing on files:

1. Right-click the file in Windows Explorer and select Properties.
2. Click the Security tab.
3. Click Auditing.
4. Click Add to add user groups you want to monitor.
5. Select Events to audit as shown in the illustration.
6. Click OK to close.

## Configure Auditing for Windows XP and Windows 2000

Auditing is set for Windows XP and Windows 2000 using group policy. On stand-alone computers, the Audit policy can be set either in the local group policy or by configuring Local Security Policy. For computers joined in a domain, audit settings can vary according the policy configured in the GPO linked to the OU in which the computer account exists.

**TIP** When a domain account is used from a workstation, the account logon events are recorded on the domain controller, but the logon events are recorded on the workstation. The use of two types of logon events solves the problem often cause by Windows NT 4.0 logon/logoff audit events, which were recorded only where the interactive event occurred. Logon and logoff records were present only on the computer used by the user interactively. In order to audit these events, audit logs from all workstations need to be collected and filtered. By using two different types of events, the records on the domain controller can provide domain logon records.

The Audit Policy is part of the Windows Settings, Security Settings, Local Policies node. To set or modify audit policy, select the Audit Policy container and then change policy settings by double-clicking the settings in the details pane. Table 13-2 lists the Audit Policy choices for Windows XP, Windows 2000, and Windows Server 2003.

## Review Windows Server 2003 Audit Settings

Windows Server 2003 audit settings are set by default. This is a major departure from previous Windows system defaults. Review these settings and modify to meet the preceding recommendations. Windows Server 2003 default audit settings are displayed in Figure 13-1.

Audit Policy	Description	Success	Failure
Audit Account Logon Events	Records logon and logoff records where accounts reside.	Y	Y
Audit Account Management	Records changes to accounts.	Y	Y
Audit Directory Service Access	Enables the recording of configured directory object audit settings.	Y	Y
Audit Logon Events	Records activity where the user logs on interactively.	Y	Y
Audit Object Access	Enables the recording of configured audit settings on file, folder, printer, and registry objects.	Y	Y
Audit Policy Change	Records policy changes.	Y	Y
Audit Privilege Use	Records use of user rights.	Y	Y
Audit Process Tracking	Records every action a process takes.	N	N
Audit System Events	Records system events such as shutdown and startup.	Y	Y

**Table 13-2.** Audit Categories for Windows Server 2003, Windows XP, and Windows 2000

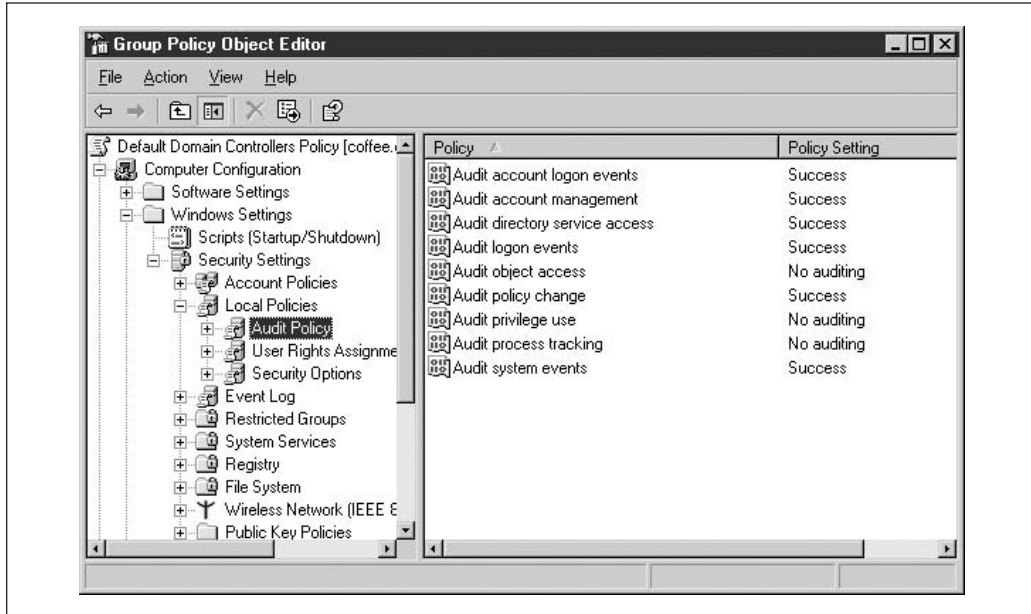


Figure 13-1. Windows Server 2003 default audit settings

## Configure Audit Logs

Audit logs must be configured both to provide enough room to record events and to dictate the retention policy of audit events.

### Configure Logs for Windows NT 4.0

To configure logs in Windows NT 4.0, use the Event Viewer Administration tool and select Log Settings from the Log menu as shown in Figure 13-2. The defaults are displayed in the figure; the following changes should be made.

- **Expand the log size.** Unlike normal Windows files, the security log cannot expand ad infinitum or until the disk is full. All Windows event log files are restricted and may only reach the limit set for them. The size required will depend on the amount of activity on the computer, which may also be a function of the role it plays on the network. Set the file size large and monitor its growth. Size is also a function of how frequently you archive the logs.
- **Set Event Log Wrapping to Overwrite Events as Needed.** If you allow events to be overwritten after some number of days, you risk losing events. If you prevent any event overwrites and the log becomes full, the log will simply stop recording events. By setting as needed, at least the most current events will still be in the log. You should, however, audit the log growth to prevent any overwrites. If the log will reach its limits before your normal archival time, either change the archive frequency or make the log file size larger.

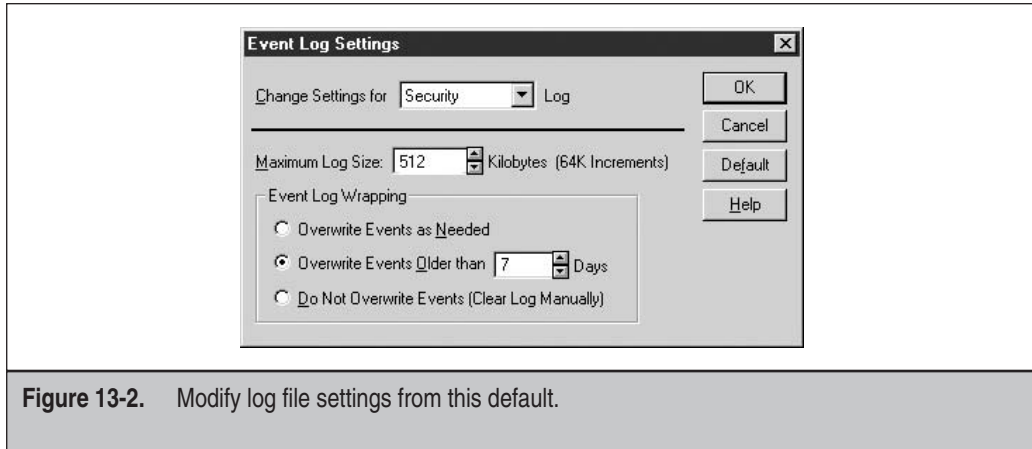


Figure 13-2. Modify log file settings from this default.

## Configure Logs for Windows 2000, Windows XP, and Windows Server 2003

Event log settings in Windows 2000, Windows XP, and Windows Server 2003 are configured in Group Policy in the Security Settings, Event Log section. Make the following adjustments:

- Change the Maximum Security Log Size to meet the requirements of your systems.
- Enable Prevent Local Guests Group from Accessing the Application Log, the Security Log, and the System Log (three settings).
- Set the Retention Method for Security Log to Overwrite Events as Needed.

## ONE STEP FURTHER

Three additional audit settings are available in the Windows Server 2003 Security Options and via registry entries for other Windows systems based on NT technologies. Configure these settings for critical systems, but be aware what they mean. Shut Down System Immediately if Unable to Log Security Audits will prevent remote access to the computer if the event log is full. This setting should be set only on systems for which you supply real-time monitoring. The event log must be manually cleared and the setting reset in order to regain remote access to the computer.

Audit the Access of Global System Objects records of the use of semaphores (locking objects), mutexes (mutually exclusive controls), and DOS devices. This setting enables powerful audit resources for the review of software but simply records too much information in a production environment.

Audit the Use of Backup and Restore Privileges records each file accessed during a backup and probably provides more information than is needed for most production computers.

## Archive Audit Logs

Log files should be periodically archived. Logs can be manually archived by using the Save Log File As menu selection. Archived logs should be stored at a location other than the computer on which they were recorded. Log files should be consolidated for review. Each entry in the log includes the computer on which the log entry was recorded, so identification of the log entry origination is always possible.

A script can be written, for example, using the Resource Kit tool `dumpel`, to dump log data to a text file. Schedule the script to run using the built-in Scheduler program or the `AT` command. Consolidate the log files and use appropriate tools for filtering. The text file is easily imported into a database such as Access or SQL Server. Queries and reports can then be written to filter events.

## Use Security Events for Intrusion Detection and Forensics

Audit policy is configured so that security events will be collected. Then what? The events can be used to discover what happened after a security breach. They can also be used to aid in the detection of intrusions. To do either of these things, you must find a way to filter event logs. Again, two types of filters are needed. To forensically examine a specific event, you will need to be intimately familiar with the normal events recorded for security, system, and applications. This knowledge can help you understand which events to look for when tracking activity. To detect intrusions, you filter on events that are likely to indicate abnormal activity. Keep in mind, however, that some normal events, if recorded in unusual circumstances, may indicate intrusion, and some abnormal events may simply be the result of something other than intrusion. Often, it is a combination of events that provides a clearer picture. Table 13-3 lists authentication events that should be monitored. All security events should be monitored; for a comprehensive list, see the Knowledge Base articles 299475 (<http://support.microsoft.com/?id=299475>) and 301677 (<http://support.microsoft.com/default.aspx?scid=kb;EN-US;301677>).

Event ID	Description
529	Unknown username or known username with bad password.
530	Account logon time restriction violation.
531	Account currently disabled.
532	Account expired.
533	User not allowed to log on this computer.
534	Logon type restricted; user has not been granted requested logon type at this machine.

**Table 13-3.** Track Security Log Authentication Events



Event ID	Description
535	Specified account password has expired.
537	Unsuccessful logon.
539	Account locked out.
544	IPSec association establishment failed because peer could not authenticate.
545	IPSec peer authentication failed.
614	IPSec policy agent disabled.
615	IPSec policy agent changed.
616	IPSec policy agent encountered a potentially serious flaw.
617	Kerberos policy changed.
643	Domain policy changed.
675	Account logon preauthentication failed.
676	Authentication ticket failed.
677	Service ticket request failed.
681	The logon to account <client name> by <source> from <workstation> failed; the error code was <error>.
682	A user reconnected to a disconnected Terminal Services session.
683	A user disconnected a Terminal Services session without logging off.

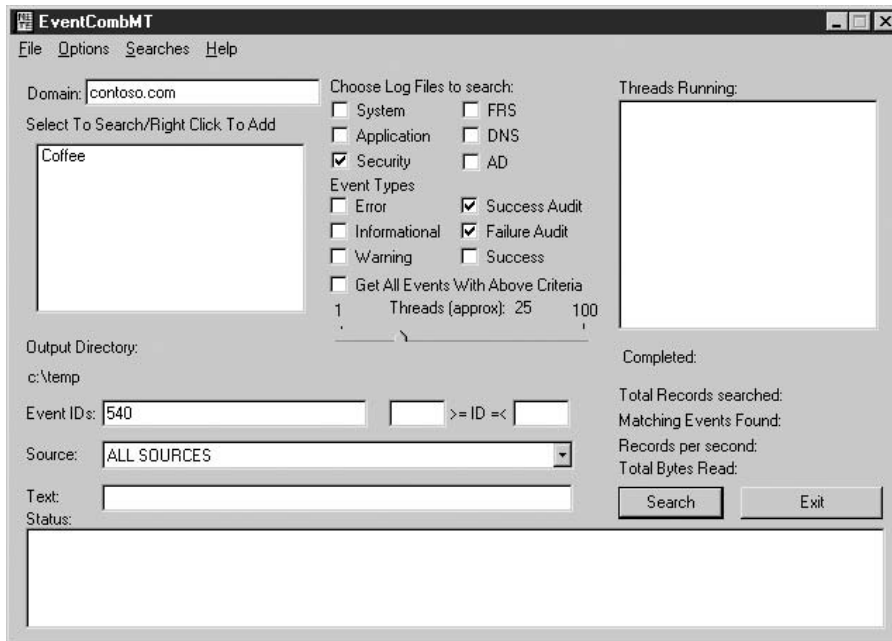
**Table 13-3.** Track Security Log Authentication Events (*continued*)

To examine and filter events, you can create queries to use with an Access or SQL database developed from archived logs. To perform more current examinations, the tool EventCombMT can be used to consolidate current security log information and filter by specific events. EventCombMT can be downloaded from the Security Guide Scripts Download page [www.microsoft.com/downloads/details.aspx?FamilyID=9989d151-5c55-4bd3-a9d2-b95a15c73e92&DisplayLang=en](http://www.microsoft.com/downloads/details.aspx?FamilyID=9989d151-5c55-4bd3-a9d2-b95a15c73e92&DisplayLang=en).

After downloading the EventCombMT tool:

1. Double-click the executable to open the tool; then click OK.
2. Set the domain box entry to the domain to review.
3. Right-click the box Select to Search/Right Click to Add.
4. Add servers to search. All server can be added, or all DCs.
5. Select the Security Log file.

6. Select the Event type (either Success Audit or Failure Audit, or both).
7. Enter the event IDs to search for as shown here:



8. Click Search to start the search.
9. A temporary file, eventcombmt.txt, is created in the temp folder to record the search process. The results of the search are recorded in a text file named for the server and type of event log and are displayed in the window.

## Audit Security Configuration

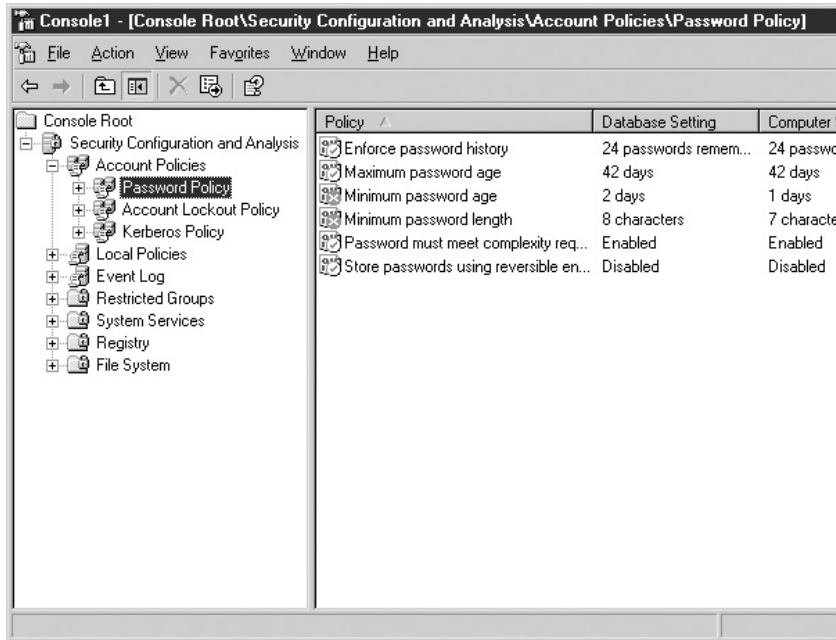
To ensure that security configuration remains in force, the settings should be audited. This means that both Group Policies should be checked for compliance and computers should be checked to determine if settings are being applied. Two free tools can be used for this purpose, Security Configuration and Analysis, and Resultant Set of Policy.

### Audit Configuration Compliance with Security Configuration and Analysis

The Security Configuration and Analysis snap-in can be used to audit Security settings on a single computer. To use the tool:

1. Have available a security template that is composed of the settings that are correct for this computer.
2. Add the Security Configuration and Analysis tool to an MMC console.
3. Open a new database by selecting Open Database, typing a filename, and then pressing ENTER.

4. Browse to and select the security template in step 1 and click Open.
5. Right-click the Security Configuration and Analysis node and select Analyze Computer Now.
6. Click OK to approve the log file path.
7. When the process completes, review each policy, looking for red and white xs. The xs indicate variances from the approved policy as shown here:



## ONE STEP FURTHER

The command-line tool `secdit.exe` can be used in a script to perform an analysis. A script could be written to perform an analysis of multiple computers. You can review the results using the Security Configuration and Analysis tool.

### Audit Configuration Compliance with Resultant Set of Policy

Windows XP and Windows Server 2003 offer a new tool, Resultant Set of Policy, that can be used to validate security settings for a specific purpose. To use the tool:

1. Add the snap-in to an MMC console.
2. Right-click the Resultant Set of Policy node and select Generate RSoP Data. Then click Next.

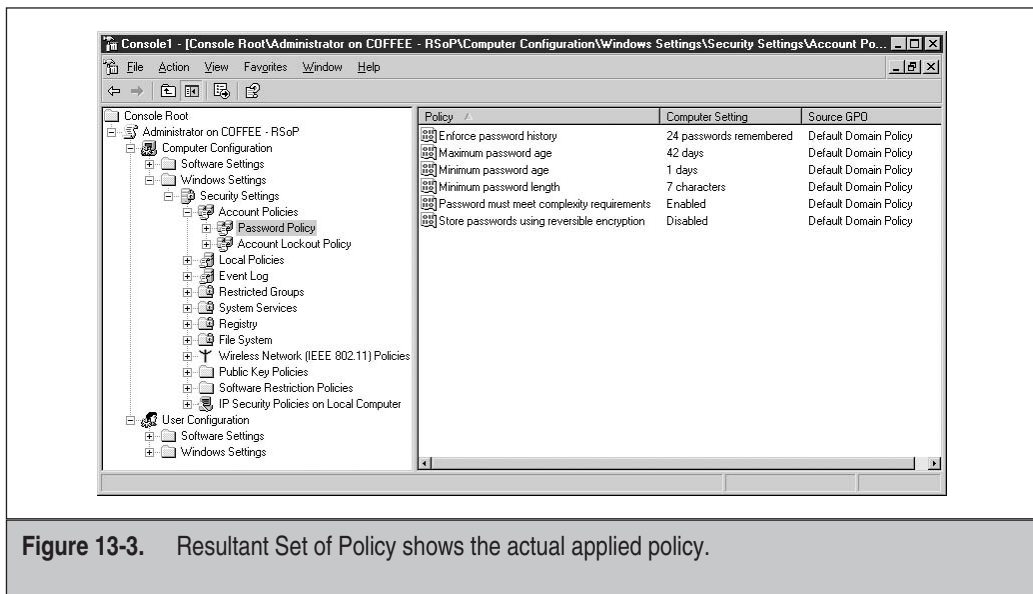
3. Select Logging Mode and click Next. Logging mode will perform a test by connecting to a specific computer and checking the results of Group Policy application for a specific user on that computer. Planning mode can be used to see the results of different combinations of GPOs. It does not connect to a specific computer to complete the test.
4. Select a specific computer to test and click Next. The local computer may be used. You may also restrict the scan to user settings only.
5. Select a specific user account to test and click Next. You can restrict the scan to computer settings only.
6. Review choices and then click Next.
7. When the scan is complete, click Finish.

View the results by selecting nodes in the console as shown in Figure 13-3. Note that RSoP does not compare the settings with those set by policy; it merely reports what is. It does indicate the source of the settings by listing the Source GPO.

---

**TIP** A downloadable tool, the Group Policy Management Console, can be used to run these tests and show more information.

---

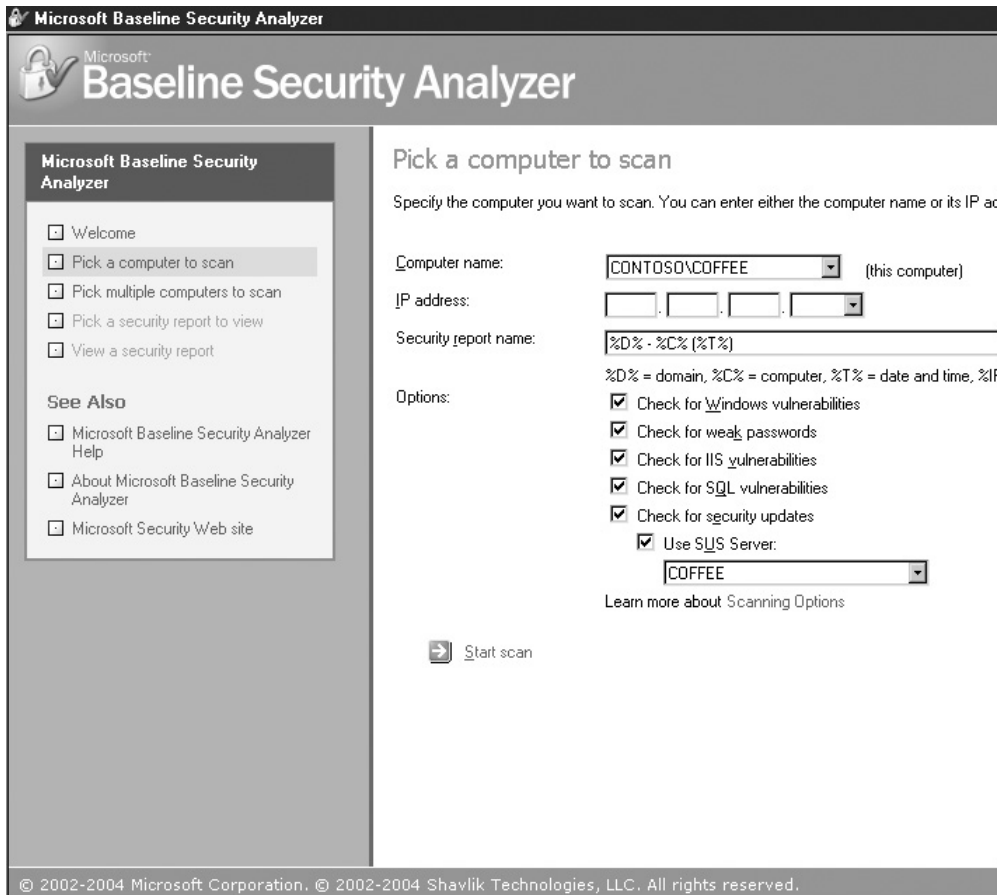


**Figure 13-3.** Resultant Set of Policy shows the actual applied policy.

## Audit Patch Status

It's not enough to schedule and apply patches; you must determine if patches are actually being applied. A tool that can assist you in these efforts is the Microsoft Baseline Security Analyzer. Download the tool from [www.microsoft.com/downloads/details.aspx?FamilyID=8b7a580d-0c91-45b7-91ba-fc47f7c3d6ad&DisplayLang=en](http://www.microsoft.com/downloads/details.aspx?FamilyID=8b7a580d-0c91-45b7-91ba-fc47f7c3d6ad&DisplayLang=en). To use the tool:

1. Run the tool from the Programs menu.
2. Click Scan a Computer.
3. Configure the scanner as shown next. You can prevent it from scanning specific types of vulnerabilities and point it to a SUS server. (Using your SUS server requires the tool to indicate only patches missing that you have approved for installation.)



**Microsoft Baseline Security Analyzer**

Microsoft  
**Baseline Security Analyzer**

**Microsoft Baseline Security Analyzer**

- Welcome
- Pick a computer to scan
- Pick multiple computers to scan
- Pick a security report to view
- View a security report

**See Also**

- Microsoft Baseline Security Analyzer Help
- About Microsoft Baseline Security Analyzer
- Microsoft Security Web site

**Pick a computer to scan**

Specify the computer you want to scan. You can enter either the computer name or its IP address.

**Computer name:**  (this computer)

**IP address:**

**Security report name:**

**Options:**

- Check for Windows vulnerabilities
- Check for weak passwords
- Check for IIS vulnerabilities
- Check for SQL vulnerabilities
- Check for security updates
- Use SUS Server:

[Learn more about Scanning Options](#)

© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.

4. Click Start Scan.
5. When the scan is complete, a number of security vulnerabilities may be indicated along with the patch status of this system as shown here:

**Microsoft Baseline Security Analyzer**

Microsoft Baseline Security Analyzer

View security report

Sort Order:

**Computer name:** CONTOSO\COFFEE  
**IP address:** 192.168.5.23  
**Security report name:** CONTOSO - COFFEE (3-13-2004 4-21 PM)  
**Scan date:** 3/13/2004 4:21 PM  
**Scanned with MBSA version:** 1.2.3316.1  
**Security update database version:** 2004.3.9.0  
**Office update database version:** 11.0.0.6303  
**Security assessment:** Severe Risk (One or more critical checks failed.)

**Security Update Scan Results**

Score	Issue	Result
X	Windows Security Updates	10 security updates are missing or could not be confirmed. What was scanned    Result details    How to correct this
X	Windows Media Player Security Updates	1 critical security updates are missing. What was scanned    Result details    How to correct this
X	MDAC Security Updates	1 critical security updates are missing. What was scanned    Result details    How to correct this
✓	Office Security Updates	No critical security updates are missing. What was scanned
✓	IIS Security Updates	No critical security updates are missing. What was scanned
✓	MSSQL	No critical security updates are missing.

Previous security report

© 2002-2004 Microsoft Corporation. © 2002-2004 Shavlik Technologies, LLC. All rights reserved.

## ONE STEP FURTHER

You can use a command-line version of MBSA, `mbsacli.exe`, to script scans. The results can be placed in a database for analysis. An article that provides simple instructions for doing so can be found in my article "Auditing Patch Management" at <http://mcpmag.com/columns/article.asp?EditorialsID=531&whichpage=2&pagesize=10>.