



# Windows Security Reference

This document is a checklist of the security options with reference material (provided by Microsoft) for a Windows server implementation. The options are based on Windows 2003 functionality, but many of the checks are also valid for Windows 2000.

## Table of Contents

Password Policy .....	1
Account lockout policy .....	4
Kerberos Policy .....	5
Audit Policy .....	5
User Rights Assignments .....	8
Security Options .....	8
Event Log .....	8
System Services .....	8
Administrative Templates .....	8
Registry Settings .....	8
NTFS .....	8
Configure SNMP Community Name .....	8
IIS Configuration .....	8

## Password Policy

Password policy settings control the complexity and lifetime for passwords. This section discusses each specific password policy setting

Password Policy	Default	Member Server	High Security	Domain Controller
Enforce password history	24	≥ 10	≥ 10	≥ 10
Maximum password age	42 days	<ul style="list-style-type: none"> <li>• ≤ 30 days for administrator accounts</li> <li>• ≤ 90 days for Faculty and staff accounts</li> <li>• ≤ 180 days for student accounts</li> </ul>	<ul style="list-style-type: none"> <li>• ≤ 30 days for administrator accounts</li> </ul>	<ul style="list-style-type: none"> <li>• ≤ 30 days for administrator accounts</li> <li>• ≤ 90 days for Faculty and staff accounts</li> <li>• ≤ 180 days for student accounts</li> </ul>
Minimum password age	1 day	≥ 1 day	≥ 1 day	≥ 1 day
Minimum password length	7 characters	≥ 8 characters	≥ 8 characters	≥ 8 characters
Password must meet complexity requirements	Disabled	Enabled, but use custom passfilt.dll to require alpha & numeric	Enabled, but use custom passfilt.dll to require alpha & numeric	Enabled, but use custom passfilt.dll to require alpha & numeric
Store password using reversible encryption for all	Disabled	Disabled	Disabled	Disabled



users in the domain				
---------------------	--	--	--	--

## Enforce password history

The **Enforce password history** setting determines the number of unique new passwords that have to be associated with a user account before it is possible to reuse an old password. The value must be set between 0 and 24 passwords.

## Maximum password age

You can configure the **Maximum password age** setting so that passwords expire as often as necessary for your environment. The default values for this setting range from 1 to 999 days. This policy setting defines the period in which an attacker who has cracked a password may use it to access a computer on the network before the password expires. Changing passwords regularly is one way to prevent passwords from being compromised. The default value for this setting is 42 days.

## Minimum password age

The **Minimum password age** setting determines the number of days that a password must be used before a user changes it. The range of values for this setting is between 0 and 999 days. Setting this to 0 allows you to change the password immediately. The default value for the setting is 1 day.

The **Minimum password age** setting must be less than the **Maximum password age** setting, unless the **Maximum password age** setting is set to 0, indicating that passwords will never expire. In this case, the **Minimum password age** can be set to any value between 0 and 999.

Set the **Minimum password age** to be greater than 0 if you want **Enforce password history** to be effective. Without a minimum password age, users can cycle through passwords repeatedly until they get to an old favorite.

The **Minimum password length** setting ensures passwords have at least a specified number of characters. Long passwords — eight or more characters — are usually stronger than short ones. With this policy setting, users cannot use blank passwords, and they must create passwords that are a certain number of characters long.

## Minimum password length

The default value for this setting is 7 characters, but an eight-character password is recommended as it is long enough to provide some level of security, but still short enough for users to easily remember. This setting will provide a great deal of defense against the commonly used dictionary and brute force attacks.

A dictionary attack is a method of obtaining a password through trial and error in which an attacker uses all items in a word list. A brute force attack is a method of obtaining a password or other encrypted text by trying every possible value. The feasibility of a brute force password attack depends on the length of the password, the size of the potential character set, and the computational power available to the attacker.



## **Password must meet complexity requirements**

The Passwords must meet complexity requirements setting determines whether passwords must meet a series of guidelines that are considered important for a strong password.

Enabling this policy requires passwords to meet the following requirements:

- The password is at least six characters long.
- The password contains characters from three of the following four categories:
  - English uppercase characters (A - Z)
  - English lowercase characters (a - z)
  - Base 10 digits (0 - 9)
  - Non-alphanumeric (For example: !, \$, #, or %)
- The password does not contain three or more characters from the user's account name. If the account name is less than three characters long then this check is not performed because the rate at which passwords would be rejected would be too high. When checking against the user's full name several characters are treated as delimiters which separate the name into individual tokens: commas, periods, dashes/hyphens, underscores, spaces, pound-signs and tabs. For each token that is three or more characters long, that token is searched for in the password and if it is present the password change is rejected. For example, the name "Erin M. Hagens" would be split into three tokens: "Erin," "M," and "Hagens." Since the second token is only one character long it would be ignored. Therefore this user could not have a password that included either "erin" or "hagens" as a substring anywhere in the password. All of these checks are case insensitive.

The rules that are included in the Windows Server 2003 policy cannot be directly modified. However, you can create a new version of passfilt.dll to apply a different set of rules. For the source code for passfilt.dll see the Microsoft Knowledge Base article 151082: "HOW TO: Password Change Filtering & Notification in Windows NT" at: <http://support.microsoft.com/default.aspx?scid=151082>.

## **Store password using reversible encryption for all users in the domain**

The Store password using reversible encryption for all users in the domain setting determines whether Microsoft Windows Server 2003, Windows 2000 Server, Windows 2000 Professional, and Windows XP Professional store passwords using reversible encryption.

This policy provides support for applications that use protocols requiring knowledge of the user's password for authentication purposes. By definition, storing encrypted passwords in a way that is reversible means that the encrypted passwords can be decrypted. A knowledgeable attacker who was able to break this encryption could then log into network resources using the compromised account. For this reason, never enable this setting unless application requirements outweigh the need to protect password information.

Using CHAP authentication through remote access or Internet Authentication Service (IAS) services requires enabling this setting. Challenge Handshake Authentication Protocol (CHAP) is



an authentication protocol used by Microsoft remote access and Network Connections. Digest Authentication in Microsoft Internet Information Services (IIS) also requires enabling this setting.

### ***Account lockout policy***

More than a few unsuccessful password tries during an attempt to log on to your system might represent an attacker attempting to determine an account password by trial and error. Windows Server keeps track of logon attempts, and the operating system can be configured to respond to this type of potential attack by disabling the account for a preset period of time. Account lockout policy settings control the threshold for this response and the actions to be taken once the threshold is reached.

<b>Account Lockout Policy</b>	<b>Default</b>	<b>Member Server</b>	<b>High Security</b>	<b>Domain Controller</b>
Account lockout duration	Not Defined	≥ 1 hour	≥ 1 hour	≥ 1 hour
Account lockout threshold	0 invalid login attempts	Between 5 and 10 invalid login attempts	Between 5 and 10 invalid login attempts	Between 5 and 10 invalid login attempts
Reset account lockout counter after	Not Defined	Between 15 minutes and 1 hour	Between 15 minutes and 1 hour	Between 15 minutes and 1 hour

### **Account lockout duration**

The Account lockout duration setting determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from 1 to 99,999 minutes. You can specify that the account will be locked out until an administrator explicitly unlocks it by setting the value to 0. If an account lockout threshold is defined, the account lockout duration must be greater than or equal to the reset time.

### **Account lockout threshold**

The Account lockout threshold determines the number of failed logon attempts that causes a user account lock out. A locked -out account cannot be used until it is reset by an administrator or until the lockout duration for the account expires. You can set a value between 1 and 999 failed logon attempts, or you can specify that the account will never be locked out by setting the value to 0. If you define an Account lockout threshold, then the Account lockout duration must be greater than or equal to the reset time.

Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE or password - protected screen savers do not count as failed logon attempts unless the group policy Interactive logon: Require Domain Controller authentication to unlock workstation is enabled. If Interactive logon: Require Domain Controller authentication to unlock workstation is enabled then repeated failed password attempts to unlock the workstation will count against the Account lockout threshold.

### **Reset account lockout counter after**

The Reset account lockout counter after setting determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon



attempts. If an Account lockout threshold is defined, this reset time must be less than or equal to the Account lockout duration.

### ***Kerberos Policy***

Kerberos policies are used for domain user accounts. These policies determine Kerberos version 5 protocol – related settings, such as ticket lifetimes and enforcement. By reducing the lifetime of Kerberos tickets, the risk of a legitimate user's credentials being stolen and successfully used by an attacker decreases. However, authorization overhead increases. In most environments, these settings should not need to be changed. These settings are applied at the domain level, the default values are configured in the Default Domain Policy GPO in a default installation of a Windows 2000 or Windows Server 2003 Active Directory domain.

### ***Audit Policy***

An audit policy determines the security events to report to the network administrators so that user or system activity in specified event categories is recorded. The administrator can monitor security – related activity, such as who accesses an object, if a user logs on to or off from a computer, or if changes are made to an auditing policy setting. If no auditing is configured, it will be difficult or impossible to determine what took place during a security incident. However, if auditing is configured so that too many authorized activities generate events, the security event log will fill up with useless data. Therefore, the following recommendations help balance the decisions on what to monitor so that the data collected is relevant.

<b>Audit Policy</b>	<b>Default</b>	<b>Member Server</b>	<b>High Security</b>	<b>Domain Controller</b>
Audit account logon events	Success	Success, Failure	Success, Failure	Success, Failure
Audit account management	No Auditing	Success, Failure	Success, Failure	Success, Failure
Audit directory service access	No Auditing	Success, Failure	Success, Failure	Success, Failure
Audit logon events	Success	Success, Failure	Success, Failure	Success, Failure
Audit object access	Success	Success, Failure	Success, Failure	Success, Failure
Audit policy change	No Auditing	Success	Success	Success
Audit privilege use	No Auditing	Failure	Success, Failure	Failure
Audit process tracking	No Auditing	No Auditing	No Auditing	No Auditing
Audit system events	No Auditing	Success	Success	Success

### **Audit account logon events**

The **Audit account logon events** setting determine whether to audit each instance of a user logging on to or off another computer that validates the account. Authenticating a domain user account on a domain controller generates an account logon event. The event is logged in the domain controller's security log. Authenticating a local user on a local computer generates a



logon event. The event is logged in the local security log. There are no Account logoff events logged.

### **Audit account management**

The **Audit account management** setting determines whether to audit each account management event on a computer. Examples of account management events include:

- A user account or group is created, changed, or deleted.
- A user account is renamed, disabled, or enabled.

A password is set or changed.

### **Audit directory service access**

The **Audit directory service access** setting determines whether to audit the event of a user accessing a Microsoft Active Directory® directory service object that has its own system access control list (SACL) specified. Setting **Audit directory service access** to **No Auditing** makes it difficult or impossible to determine what Active Directory objects may have been compromised during a security incident. There will be no audit record evidence available for analysis after a security incident if the values for this setting are not set to **Success** and **Failure**.

Configuring **Audit directory service access** to **Success** generates an audit entry each time that a user successfully accesses an Active Directory object with a specified SACL. Configuring this setting to **Failure** generates an audit entry each time that a user unsuccessfully attempts to access an Active Directory object with a specified SACL.

### **Audit logon events**

The **Audit logon events** setting determine whether to audit each instance of a user logging on to or off of a computer. Records are generated from the **Account logon events** setting on domain controllers to monitor domain account activity and on local computers to monitor local account activity.

Configuring the **Audit logon events** setting to **No auditing** makes it difficult or impossible to determine which user has either logged on or attempted to log on to computers in the enterprise. Enabling the **Success** value for the **Auditing logon events** setting on a domain member will generate an event each time that someone logs on to the system regardless of where the accounts reside on the system. If the user logs on to a local account and the **Audit account logon events** setting is **Enabled**, the user logon will generate two events.

There will be no audit record evidence available for analysis after a security incident takes place if the values for this setting are not configured to **Success** and **Failure** for all three security environments defined in this guide.

### **Audit object access**

By itself, this setting will not cause any events to be audited. The **Audit object access** setting determines whether to audit the event of a user accessing an object — for example, a file, folder,



registry key, printer, and so forth — that has a specified SACL. A SACL is comprised of access control entries (ACEs). Each ACE contains three pieces of information:

- The security principal (user, computer, or group) to be audited.
- The specific access type to be audited, called an access mask.
- A flag to indicate whether to audit failed access events, successful access events, or both.

Configuring this setting to **Success** generates an audit entry each time that a user successfully accesses an object with a specified SACL. Configuring this setting to **Failure** generates an audit entry each time that a user unsuccessfully attempts to access an object with a specified SACL.

Corporations should define only the actions they want enabled when configuring SACLs. For example, you might want to enable the **Write and Append Data auditing** setting on executable files to track the replacement or changes to those files, which computer viruses, worms, and Trojan horses will commonly cause. Similarly, you might want to track changes to or even the reading of sensitive documents.

## Audit policy change

The **Audit policy change** setting determines whether to audit every incident of a change to user rights assignment policies, audit policies, or trust policies. This includes making changes to the audit policy itself.

Configuring this setting to **Success** generates an audit entry for each successful change to user rights assignment policies, audit policies, or trust policies. Configuring this setting to **Failure** generates an audit entry for each failed change to user rights assignment policies, audit policies, or trust policies.

The recommended settings would let you see any account privileges that an attacker attempts to elevate — for example, by adding the **Debug programs** privilege or the **Back up files and directories** privilege. Policy change auditing also includes making changes to the audit policy itself as well as to trust relationships.

## Audit privilege use

The **Audit privilege use** setting determines whether to audit each instance of a user exercising a user right. Configuring this value to **Success** generates an audit entry each time that a user right is exercised successfully. Configuring this value to **Failure** generates an audit entry each time that a user right is exercised unsuccessfully. Audits are not generated when the following user rights are exercised, even if the **Audit privilege use** settings is configured to **Success** or **Failure**. This is because auditing these user rights generates many events in the security log, which may constrain the performance of your computers. To audit the following excluded rights, you must enable the **Audit: Audit the use of Backup and Restore privilege** security option in Group Policy:

- **Bypass traverse checking**
- **Debug programs**
- **Create a token object**



- **Replace process level token**
- **Generate security audits**
- **Back up files and directories**
- **Restore files and directories**

Enabling privilege auditing generates a very large number of event records. For this reason, each security environment defined in this guide has unique recommendations for these settings. Failed use of a user right is an indicator of a general network problem and often can be a sign of an attempted security breach. Corporations should set the **Audit privilege use** setting to **Enable** only if there is a specific business reason to do so.

### **Audit process tracking**

The **Audit process tracking** setting determines whether to audit detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access. Configuring this setting to **Success** generates an audit entry each time the process being tracked succeeds. Configuring this setting to **Failure** generates an audit entry each time the process being tracked fails.

Enabling **Audit process tracking** will generate a large number of events, so typically it is set to **No Auditing**. However, these settings can provide a great benefit during an incident response from the detailed log of the processes started and the time when they were launched.

### **Audit system events**

The **Audit system events** setting determines whether to audit when a user restarts or shuts down a computer or when an event occurs that affects either the system security or the security log. Configuring this setting to **Success** generates an audit entry when a system event is executed successfully. Configuring this setting to **Failure** generates an audit entry when a system event is attempted unsuccessfully.

## ***User Rights Assignments***

User Rights Assignments determine which users or groups have logon rights or privileges on the computers in your organization. Logon rights and privileges govern the rights that users have on the target system. They are used to grant the right to perform certain actions, such as logging on from the network or locally, as well as administrative tasks, such as generating new logon tokens.

**Note:** Throughout the following section, User Rights Assignments, "Not defined" means Administrators still have the privilege for every right not defined. Local administrators can make changes, but any domain-based Group Policy settings will override them the next time that the Group Policies are refreshed or reapplied.

<b>User Rights Assignments</b>	<b>Default</b>	<b>Member Server</b>	<b>High Security</b>	<b>Domain Controller</b>
--------------------------------	----------------	----------------------	----------------------	--------------------------



User Rights Assignments	Default	Member Server	High Security	Domain Controller
Access this computer from the network	Administrators, Backup Operators, Everyone, Power Users, and Users	Depending on your requirements <ul style="list-style-type: none"> <li>• Defaults settings (Not Defined)</li> <li>• Administrators, Backup Operators, Power Users, and Users</li> </ul>	Administrators, Authenticated Users	Administrators, Backup Operators, Power Users, and Users
Act as part of the operating system	Not Defined	Not Defined	No One	Not Defined
Add workstations to domain	Not Defined	Not Defined	Administrators	Depending on your requirements: Administrators
Adjust memory quotas for a process	Administrators, NETWORK SERVICE, LOCAL SERVICE	Not Defined	Not Defined	Not Defined
Allow log on locally	Administrators, Backup Operators, Power Users, Users	Not Defined	Administrators	Not Defined
Allow log on through Terminal Services	Administrators and Remote Desktop Users	Not Defined	Administrators	Administrators
Change the system time	Administrators and Power Users	Not Defined	Administrators	Administrators
Debug programs	Administrators	Not Defined	No One	Not Defined
Deny access to this computer from the network	SUPPORT_388945a0	ANONYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts	ANONYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts	ANONYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts
Deny log on through Terminal Services	Not Defined	ANONYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts	ANONYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts	ANONYMOUS LOGON; Built-in Administrator, Guests; Support_388945a0; Guest; all NON-Operating System service accounts
Enable computer and user accounts to be trusted for delegation	Not defined	Not defined	No One	No One



<b>User Rights Assignments</b>	<b>Default</b>	<b>Member Server</b>	<b>High Security</b>	<b>Domain Controller</b>
Force shutdown from a remote system	Administrators	Not defined / Default	Not defined / Default	Not defined / Default
Generate security audits	NETWORK SERVICE, LOCAL SERVICE	Not defined / Default	Not defined / Default	Not defined / Default
Impersonate a client after authentication	SERVICE, Administrators	Not defined / Default	Local Service; Network Service	Not defined / Default
Increase scheduling priority	Administrators	Not defined / Default	Not defined / Default	Not defined / Default
Load and unload device drivers	Administrators	Not defined / Default	Not defined / Default	Not defined / Default
Lock pages in memory	Not defined	Not defined	Administrators	Not defined
Log on as a batch job	SUPPORT_388945a0, LOCAL SERVICE	Not defined	No One	Not defined
Manage auditing and security log	Administrators	Not defined / Default	Not defined / Default	Not defined / Default
Modify firmware environment values	Administrators	Not defined / Default	Not defined / Default	Not defined / Default
Perform volume maintenance tasks	Administrators	Not defined / Default	Not defined / Default	Not defined / Default
Profile single process	Administrators, Power Users	Not defined / Default	Administrators	Administrators
Profile system performance	Administrators	Not defined / Default	Not defined / Default	Not defined / Default
Remove computer from docking station	Administrators, Power Users	Not defined / Default	Administrators	Administrators
Replace a process level token	LOCAL SERVICE, NETWORK SERVICE	Not defined / Default	Not defined / Default	Not defined / Default
Restore files and directories	Administrators, Backup Operators	Not defined / Default	Administrators	Not defined / Default
Shut down the system	Backup Operators, Power Users, Administrators	Not defined / Default	Administrators	Not defined / Default
Synchronize directory service data	Not Defined	Not defined	No One	Not defined



User Rights Assignments	Default	Member Server	High Security	Domain Controller
Take ownership of files or other objects	Administrators	Not defined / Default	Not defined / Default	Not defined / Default

### Access this computer from the network

The **Access this computer from the network** user right determines which users and groups are allowed to connect to the computer over the network. This user right is required by a number of network protocols including server message block (SMB) – based protocols, network basic input/output system (NetBIOS), Common Internet File System (CIFS), Hypertext Transfer Protocol (HTTP), and Component Object Model Plus (COM+).

In Windows Server 2003 permissions granted to the **Everyone** security group no longer grant access to anonymous users, guest groups and accounts can still be granted access through the **Everyone** security group. For this reason, it is preferred to remove the **Everyone** security group from the **Access this computer from the network** user right in the High Security environment to further guard from attacks targeting guest access to the domain.

### Act as part of the operating system

The **Act as part of the operating system** user right allows a process to assume the identity of any user and thus gain access to the resources that the user is authorized to access. Typically, only low – level authentication services require this privilege.

### Add workstations to domain

The **Add workstations to domain** user right allows the user to add a computer to a specific domain. For the privilege to take effect, it must be assigned to the user as part of the Default Domain Controllers Policy for the domain.

### Adjust memory quotas for a process

The **Adjust memory quotas for a process** user right allows a user to adjust the maximum memory that is available to a process. This privilege is useful for system tuning, but it can be abused. In the wrong hands, this user right can be used to launch a DoS attack.

### Allow log on locally

The **Allow log on locally** user right determines which users can interactively log on to the specified computer. Logons initiated by pressing the CTRL+ALT+DEL key – combination on the keyboard require the user to have this logon right. Any account with this user right could be used to log on to the local console of the computer. Restricting this privilege to legitimate users who need to be able to log on to the system prevents unauthorized users from elevating their privileges or from introducing viruses into the computing environment.



## Allow log on through Terminal Services

The **Allow log on through Terminal Services** user right determines which users or groups have permission to log on as a Terminal Services client.

## Change the system time

The **Change the system time** user right determines which users and groups can change the time and date on the internal clock of the computer. Users with this user right can affect the appearance of event logs because event logs will reflect the new time, not the actual time that the events occurred. Limit the **Change the system time** privilege to users with a legitimate need to be able to change the time, such as members of the IT department. Discrepancies between the time on the local computer and on the domain controllers may cause problems for the Kerberos authentication protocol, which could make it impossible for users to log on to the domain or to get authorization for accessing domain resources after logging on.

## Debug programs

The **Debug programs** user right determines which users can attach a debugger to any process or to the kernel. This user right provides complete access to sensitive and critical operating system components. Program debugging should not take place in production environments except in extreme circumstances, such as troubleshooting a business – critical application that cannot be effectively assessed in the test environment.

## Deny access to this computer from the network

The **Deny access to this computer from the network** user right determines which users are prevented from accessing a computer over the network. This user right will deny a number of network protocols including SMB – based protocols, NetBIOS, CIFS, HTTP, and COM+. This policy setting supersedes the **Access this computer from the network** user right when a user account is subject to both policies. Configuring this logon right for other groups could limit the abilities of users assigned to specific administrative roles in your environment. Verify that delegated tasks will not be negatively impacted.

## Deny log on through Terminal Services

The **Deny log on through Terminal Services** user right determines which users and groups are prohibited from logging on as a Terminal Services client. After joining the baseline member server to a domain environment, there is no need to use local accounts to access the server from the network. Domain accounts can access the server for administration and end – user processing.

## Enable computer and user accounts to be trusted for delegation

The **Enable computer and user accounts to be trusted for delegation** privilege allows the user to change the **Trusted for Delegation** setting on a user or computer object in Active Directory. The user or computer that is granted this privilege must also have write access to the account control flags on the object. Misuse of this privilege could lead to unauthorized users impersonating other users on the network.



## Force shutdown from a remote system

The **Force shutdown from a remote system** user privilege allows a user to shut down a computer from a remote location on the network. Any user who can shut down a computer can cause a DoS condition; therefore, this privilege should be tightly restricted.

## Generate security audits

The **Generate security audits** user privilege allows a process to generate audit records in the security log. The security log can be used to trace unauthorized system access. Accounts that are able to write to the security log could be used by an attacker to fill that log with meaningless events. If the computer is configured to overwrite events as needed, the attacker could use this method to remove evidence of his or her unauthorized activities. If the computer is configured to shut down when it is unable to write to the security log, this method could be used to create a DoS condition.

## Impersonate a client after authentication

Assigning the **Impersonate a client after authentication** privilege allows applications running on behalf of that user to impersonate a client. Requiring this user right for this kind of impersonation prevents an unauthorized user from convincing a client to connect — for example, by remote procedure call (RPC) or named pipes — to a service that he or she has created and then impersonating that client, which can elevate the unauthorized user's permissions to administrative or system levels.

## Increase scheduling priority

The **Increase scheduling priority** privilege allows a user to increase the base priority class of a process. Increasing relative priority within a priority class is not a privileged operation. This privilege is not required by administrative tools supplied with the operating system but might be required by software development tools. A user with this privilege can increase the scheduling priority of a process to **Real – Time**, leaving little processing time for all other processes, which could lead to a DoS condition.

## Load and unload device drivers

The **Load and unload device drivers** privilege determines which users can dynamically load and unload device drivers. This privilege is not required if a signed driver for the new hardware already exists in the Driver.cab file on the computer. Device drivers run as highly privileged code. A user granted the **Load and unload device drivers** privilege can unintentionally install malicious code masquerading as a device driver. It is assumed that administrators will exercise greater care and install only drivers with verified digital signatures.

## Lock pages in memory

The **Lock pages in memory** user right allows a process to keep data in physical memory, which prevents the system from paging the data to virtual memory on disk. Enabling this user right can result in significant degradation of system performance. Users with this privilege can assign physical memory to several processes, leaving little or no random access memory (RAM) for other processes. This could lead to a DoS condition.



## Log on as a batch job

The **Log on as a batch job** user right allows a user to log on by using a batch – queue facility such as the Task Scheduler service. This is a low – risk vulnerability so the default settings for this user right are sufficient for most organizations.

## Manage auditing and security log

The **Manage auditing and security log** privilege allows a user to specify object access auditing options for individual resources such as files, Active Directory objects, and registry keys. The right to manage the security event log is a powerful user privilege that should be closely guarded. Anyone with this user right can clear the security log, possibly erasing important evidence of unauthorized activity.

## Modify firmware environment values

The **Modify firmware environment values** user right allows modification of system environment variables either by a process through an API, or by a user through **System Properties**. Anyone with this privilege could configure the settings of a hardware component to cause it to fail, which could lead to data corruption or a DoS condition.

## Perform volume maintenance tasks

The **Perform volume maintenance tasks** user right allows a non – administrative or remote user to manage volumes or disks. A user with this privilege could delete a volume, leading to the loss of data or a DoS condition.

## Profile single process

The **Profile single process** user right determines which users can use performance monitoring tools to monitor the performance of non – system processes. This is a moderate vulnerability; an attacker with this privilege could monitor a computer's performance to help identify critical processes that he or she might want to attack directly. The attacker may also be able to determine what processes are running on the system so that he or she could identify countermeasures to avoid — such as antivirus software, an intrusion – detection system, or other users logged onto a system.

## Profile system performance

The **Profile system performance** user right allows a user to monitor the performance of system processes. Not restricting this user right presents a moderate vulnerability; an attacker with this privilege could monitor a computer's performance to help identify critical processes that he or she might want to attack directly. The attacker could also determine what processes are running on the system to identify countermeasures to avoid, such as antivirus software or an intrusion – detection system.

## Remove computer from docking station

The **Remove computer from docking station** user right allows the user of a portable computer to undock the computer by clicking **Eject PC** on the **Start** menu. Anyone who has this user right can remove a portable computer that has been booted up from its docking station.



## Replace a process level token

The **Replace a process level token** user right allows a parent process to replace the access token that is associated with a child process.

## Restore files and directories

The **Restore files and directories** user right determines which users can bypass file, directory, registry, and other persistent objects permissions when restoring backed up files and directories. It also determines which users can set any valid security principal as the owner of an object.

## Shut down the system

The **Shut down the system** user right determines which locally logged on users can shut down the operating system using the **Shut Down** command. Misuse of this user right can result in a DoS attack. The ability to shut down domain controllers should be limited to a very small number of trusted administrators. Even though a system shutdown requires the ability to log on to the server, you should be very careful about the accounts and groups that you allow to shut down a domain controller.

## Synchronize directory service data

The **Synchronize directory service data** user right allows a process to read all objects and properties in the directory, regardless of the protection on the objects and properties. This privilege is required in order to use LDAP directory synchronization (Dirsync) services.

## Take ownership of files or other objects

The **Take ownership of files or other objects** user right allows a user to take ownership of any securable object in the system, including Active Directory objects, NTFS file system (NTFS) files, and folders, printers, registry keys, services, processes, and threads.

## Security Options

The Security Options section of Group Policy is used to configure security settings for computers, such as digital signing of data, administrator and guest account names, floppy disk drive and CD – ROM drive access, driver installation behavior, and logon prompts.

Security Options	Default	Member Server	High Security	Domain Controller
Accounts: Guest account status	Disabled	Disabled	Disabled	Disabled
Accounts: Limit local account use of blank passwords to console logon only	Enabled	Enabled	Enabled	Enabled
Audit: Audit the access of global system objects	Disabled	Disabled	Disabled	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled	Disabled	Disabled	Disabled



<b>Security Options</b>	<b>Default</b>	<b>Member Server</b>	<b>High Security</b>	<b>Domain Controller</b>
Audit: Shut down system immediately if unable to log security audits	Disabled	Disabled	Disabled	Disabled
Devices: Allow undock without having to log on	Enabled	Disabled	Disabled	Disabled
Devices: Allowed to format and eject removable media	Administrators	Administrators	Administrators	Administrators
Devices: Prevent users from installing printer drivers	Enabled	Enabled	Enabled	Enabled
Devices: Restrict CD – ROM access to locally logged – on user only	Disabled	Not Defined/ Default	Enabled	Enabled
Devices: Restrict floppy access to locally logged – on user only	Disabled	Not Defined/ Default	Enabled	Enabled
Devices: Unsigned driver installation behavior	Warn but allow installation	Warn but allow installation	Warn but allow installation	Warn but allow installation
Domain controller: Allow server operators to schedule tasks	Not Defined	Disabled	Disabled	Disabled
Domain controller: LDAP server signing requirements	Not Defined	Not Defined	Require signing if possible	Require signing if possible
Domain controller: Refuse machine account password changes	Not Defined	Disabled	Disabled	Disabled
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled	Disabled	Enabled if possible	Enabled if possible
Domain member: Digitally encrypt secure channel data (when possible)	Enabled	Enabled	Enabled	Enabled
Domain member: Digitally sign secure channel data (when possible)	Enabled	Enabled	Enabled	Enabled
Domain member: Disable machine account password changes security	Disabled	Disabled	Disabled	Disabled
Domain member: Maximum machine account password age	30 days	30 days	30 days	30 days
Domain member: Require strong (Windows 2000 or later) session key	Disabled	Enabled	Enabled	Enabled
Interactive logon: Do not display last user name	Disabled	Enabled	Enabled	Enabled
Interactive logon: Do not require CTRL+ALT+DEL	Disabled	Disabled	Disabled	Disabled



<b>Security Options</b>	<b>Default</b>	<b>Member Server</b>	<b>High Security</b>	<b>Domain Controller</b>
Interactive logon: Message text for users attempting to log on	Not Defined	Define – MnSCU Standard, “A log-on banner informing users as to authorizations, recourse, and privacy shall be presented on each log-on attempt.”	Define – MnSCU Standard, “A log-on banner informing users as to authorizations, recourse, and privacy shall be presented on each log-on attempt.”	Define – MnSCU Standard, “A log-on banner informing users as to authorizations, recourse, and privacy shall be presented on each log-on attempt.”
Interactive logon: Message title for users attempting to log on	Not Defined	Define – Text should be a warning	Define – Text should be a warning	Define – Text should be a warning
Interactive logon: Number of previous logons to cache (in case domain controller is not available)	10	1	0	0
Interactive logon: Prompt user to change password before expiration	14	≥ 14 days	≥ 14 days	≥ 14 days
Interactive logon: Require Domain Controller authentication to unlock workstation	Disabled	Disabled	Enabled	Enabled
Interactive logon: Smart card removal behavior	No Action	Not Defined (Unless smart cards are being used)	Not Defined (Unless smart cards are being used)	Not Defined (Unless smart cards are being used)
Microsoft network client: Digitally sign communications (always)	Disabled	Enabled if possible	Enabled if possible	Enabled if possible
Microsoft network client: Digitally sign communications (if server agrees)	Enabled	Enabled	Enabled	Enabled
Microsoft network client: Send unencrypted password to third – party SMB	Disabled	Disabled if possible	Disabled	Disabled
Microsoft network server: Amount of idle time required before suspending session	15 minutes	15 minutes	15 minutes	15 minutes
Microsoft network server: Digitally sign communications (always)	Disabled	Disabled	Enabled if possible	Enabled if possible



<b>Security Options</b>	<b>Default</b>	<b>Member Server</b>	<b>High Security</b>	<b>Domain Controller</b>
Microsoft network server: Digitally sign communications (if client agrees)	Enabled	Enabled	Enabled	Enabled
Microsoft network server: Disconnect clients when logon hours expire	Enabled	Enabled	Enabled	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts	Enabled	Enabled	Enabled	Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares	Disabled	Enabled	Enabled	Enabled
Network access: Do not allow storage of credentials or .NET Passports for network authentication	Disabled	Enabled	Enabled	Enabled
Network access: Let Everyone permissions apply to anonymous users	Disabled	Disabled	Disabled	Disabled
Network access: Named Pipes that can be accessed anonymously	Not Defined	None	None	None
Network access: Remotely accessible registry paths	System\ CurrentControlSet\ Control\ ProductOptions; System\ CurrentControlSet\ Control\ Server Applications; Software\ Microsoft\ Windows NT\ Current Version	Not Defined / Default	None	None



<b>Security Options</b>	<b>Default</b>	<b>Member Server</b>	<b>High Security</b>	<b>Domain Controller</b>
Network access: Remotely accessible registry paths and sub – paths	System\ CurrentControlSet\ Control\ Print\ Printers; System\ CurrentControlSet\ Services\ Eventlog; Software\ Microsoft\ OLAP Server; Software\ Microsoft\ Windows NT\ CurrentVersion\ Print; Software\ Microsoft\ Windows NT\ CurrentVersion\ Windows; System\ CurrentControlSet\ Control\ ContentIndex; System\ CurrentControlSet\ Control\ Terminal Server; System\ CurrentControlSet\ Control\ Terminal Server\ UserConfig; System\ CurrentControlSet\ Control\ Terminal Server\ DefaultUserConfiguration; Software\ Microsoft\ Windows NT\ CurrentVersion\ Perflib; System\ CurrentControlSet\ Services\ SysmonLog	Not Defined / Default	None	None
Network access: Restrict anonymous access to Named Pipes and Shares	Enabled	Enabled	Enabled	Enabled
Network access: Shares that can be accessed anonymously	COMCFG,DFS\$	None	None	None
Network access: Sharing and security model for local accounts	Classic – local users authenticate as themselves	Not Defined / Default	Not Defined / Default	Not Defined / Default
Network security: Do not store LAN Manager hash value on next password change	Disabled	Enabled	Enabled	Enabled
Network Security: Force Logoff when Logon Hours expire	Disabled	Enabled	Enabled	Enabled



<b>Security Options</b>	<b>Default</b>	<b>Member Server</b>	<b>High Security</b>	<b>Domain Controller</b>
Network security: LAN Manager authentication level	Send NTLM response only	Send NTLMv2 responses only	Send NTLMv2 response only\refuse LM & NTLM	If possible: Send NTLMv2 response only\refuse LM & NTLM
Network security: LDAP client signing requirements	Negotiate signing	Negotiate signing	Negotiate signing	Negotiate signing
Network security: Minimum session security for NTLM SSP based (including secure RPC) clients	No minimum	No minimum	Enabled all settings	Enabled all settings
Network security: Minimum session security for NTLM SSP based (including secure RPC) servers	No minimum	No minimum	Enabled all settings	Enabled all settings
Recovery console: Allow automatic administrative logon	Disabled	Disabled	Disabled	Disabled
Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	Enabled	Disabled	Disabled
Shutdown: Allow system to be shut down without having to log on	Disabled	Disabled	Disabled	Disabled
Shutdown: Clear virtual memory page file	Disabled	Disabled	Enabled	Disabled
System cryptography: Force strong key protection for user keys stored on the computer	Not Defined	User is prompted when the key is first used	If feasible: User must enter a password each time they use a key	User is prompted when the key is first used
System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing	Disabled	Disabled	Disabled	Disabled
System objects: Default owner for objects created by members of the Administrators group	Administrators group	Object creator	Object creator	Object creator
System objects: Require case insensitivity for non – Windows subsystems	Enabled	Enabled	Enabled	Enabled
System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)	Enabled	Enabled	Enabled	Enabled
System settings: Optional subsystems	POSIX	None	None	None



### **Accounts: Guest account status**

The **Accounts: Guest account status** security option setting determines whether the Guest account is enabled or disabled. This account allows unauthenticated network users to gain access to the system by logging in as **Guest**.

### **Accounts: Limit local account use of blank passwords to console logon only**

The **Accounts: Limit local account use of blank passwords to console logon only** security option setting determines whether local accounts that are not password protected can be used to log on from locations other than the physical computer console. Enabling this setting prevents a local account with a nonblank password from logging on to a network from a remote client, and local accounts that are not password protected will only be able to log on physically via the keyboard of the computer.

### **Audit: Audit the access of global system objects**

The **Audit: Audit the access of global system objects** security option setting audits the access of global system objects when it is in effect. If both the **Audit: Audit the access of global system objects** and the **Audit object access audit policy** settings are enabled, a large number of audit events will be generated.

### **Audit: Audit the use of Backup and Restore privilege**

The **Audit: Audit the use of Backup and Restore privilege** security option setting determines whether to audit the use of all user privileges, including **Backup and Restore**, when the **Audit privilege use** policy setting is in effect. Enabling this policy could generate a large number of security events, causing servers to respond slowly and forcing the security event log to record numerous events of little significance.

### **Audit: Shut down system immediately if unable to log security audits**

The **Audit: Shut down system immediately if unable to log security audits** security option setting determines whether the system shuts down immediately if it is unable to log security events.

### **Devices: Allow undock without having to log on**

The **Devices: Allow undock without having to log on** security option setting determines whether a portable computer can be undocked without the user having to log on to the system. Enabling this setting eliminates a logon requirement and allows using an external hardware eject button to undock the computer. Disabling this setting means a user must be granted the **Remove computer from docking station** user right (not defined in this guidance) in order to undock the computer without logging on to the system.

### **Devices: Allowed to format and eject removable media**

The **Devices: Allowed to format and eject removable media** security option setting determines who can format and eject removable media. Only administrators should be able to eject removable media on servers.



### **Devices: Prevent users from installing printer drivers**

For a computer to print to a network printer, it must have the driver for that network printer installed. Enabling the **Devices: Prevent users from installing printer drivers** security option setting allows only those in the **Administrators** or **Power Users** groups, or those with **Server Operator** privileges to install a printer driver as part of adding a network printer. Disabling this setting allows any user to install a printer driver as part of adding a network printer.

### **Devices: Restrict CD – ROM access to locally logged – on user only**

The **Devices: Restrict CD – ROM access to locally logged – on user only** security option setting determines whether a CD – ROM is accessible to both local and remote users simultaneously. Enabling this setting allows only the interactively logged – on user to access removable CD – ROM media. If this policy is enabled, and no one is logged on interactively, the CD – ROM is accessible over the network.

### **Devices: Restrict floppy access to locally logged – on user only**

The **Devices: Restrict floppy access to locally logged – on user only** security option setting determines whether removable floppy media are accessible to both local and remote users simultaneously. Enabling this setting allows only the interactively logged – on user to access removable floppy media. If this policy is enabled, and no one is logged on interactively, the floppy media is accessible over the network.

### **Devices: Unsigned driver installation behavior**

The **Devices: Unsigned driver installation behavior** security option setting determines what happens when an attempt is made to install a device driver (by means of Setup API) that has not been approved and signed by the Windows Hardware Quality Lab (WHQL). This option prevents the installation of unsigned drivers or warns the administrator that an unsigned driver is about to be installed. This can prevent installing drivers that have not been certified to run on Windows Server 2003. One potential problem with configuring this setting to the **Warn but allow installation** value is that unattended installation scripts will fail when installing unsigned drivers.

### **Domain controller: Allow server operators to schedule tasks**

The **Domain controller: Allow server operators to schedule tasks** security option setting determines whether Server Operators are allowed to submit jobs by means of the AT schedule facility. This setting is disabled in all three environments defined in this guide. The impact of disabling this setting should be small for most organizations. Users, including those in the **Server Operators** group, will still be able to create jobs via the Task Scheduler Wizard, but those jobs will run in the context of the account with which the user authenticates when they set up the job.

### **Domain controller: LDAP server signing requirements**

The **Domain controller: LDAP server signing requirements** security option setting determines whether the LDAP server requires signing to negotiate with LDAP clients. Network traffic that is neither signed nor encrypted is susceptible to man – in – the – middle attacks in which an intruder captures packets between the server and the client and modifies them before forwarding them to



the client. In the case of an LDAP server, this means that an attacker could cause a client to make decisions based on false records from the LDAP directory.

### **Domain controller: Refuse machine account password changes**

The **Domain controller: Refuse machine account password changes** security option setting determines whether domain controllers will refuse requests from member computers to change computer account passwords. Enabling this setting on all domain controllers in a domain prevents computer account passwords on domain members from changing, leaving them susceptible to attack.

### **Domain member: Digitally encrypt or sign secure channel data (always)**

The **Domain member: Digitally encrypt or sign secure channel data (always)** security option setting determines whether all secure channel traffic initiated by the domain member must be signed or encrypted. If a system is set to always encrypt or sign secure channel data, then it cannot establish a secure channel with a domain controller that is not capable of signing or encrypting all secure channel traffic, because all secure channel data is signed and encrypted.

### **Domain member: Digitally encrypt secure channel data (when possible)**

The **Domain member: Digitally encrypt secure channel data (when possible)** security option setting determines whether a domain member may attempt to negotiate encryption for all secure channel traffic that it initiates. Enabling this setting causes the domain member to request encryption of all secure channel traffic. Disabling this setting prevents the domain member from negotiating secure channel encryption.

### **Domain member: Digitally sign secure channel data (when possible)**

The **Domain member: Digitally sign secure channel data (when possible)** security option setting determines whether a domain member may attempt to negotiate signing for all secure channel traffic that it initiates. Signing protects the traffic from being modified by anyone who captures the data en route.

### **Domain member: Disable machine account password changes security**

The **Domain member: Disable machine account password changes security** option setting determines whether a domain member may periodically change its computer account password. Enabling this setting prevents the domain member from changing its computer account password. Disabling this setting allows the domain member to change its computer account password as specified by the **Domain Member: Maximum age for machine account password** setting, which by default is every 30days. Computers that are no longer able to automatically change their account passwords are in risk of an attacker determining the password for the system's domain account.



### **Domain member: Maximum machine account password age**

The **Domain member: Maximum machine account password age** security option setting determines the maximum allowable age for a computer account password. This setting also applies to computers running Windows 2000, but it is not available through the Security Configuration Manager tools on these computers. By default, the domain members automatically change their domain passwords every 30 days. Increasing this interval significantly, or setting it to 0 so that the computers no longer change their passwords, gives an attacker more time to undertake a brute force password guessing attack against one of the computer accounts.

### **Domain member: Require strong (Windows 2000 or later) session key**

The **Domain member: Require strong (Windows 2000 or later) session key** security option setting determines whether 128 – bit key strength is required for encrypted secure channel data. Enabling this setting prevents establishing a secure channel without 128 – bit encryption. Disabling this setting requires the domain member to negotiate key strength with the domain controller. Session keys used to establish secure channel communications between domain controllers and member computers are much stronger in Windows 2000 than they were in previous Microsoft operating systems.

### **Interactive logon: Do not display last user name**

The **Interactive logon: Do not display last user name** security option setting determines whether the name of the last user to log on to the computer is displayed in the Windows logon screen. Enabling this setting prevents displaying the last logged on user's name in the **Log On to Windows** dialog box.

### **Interactive logon: Do not require CTRL+ALT+DEL**

The **Interactive logon: Do not require CTRL+ALT+DEL** security option setting determines whether pressing CTRL+ALT+DEL is required before a user can log on. Disabling this setting requires all users to press CTRL+ALT+DEL before logging on to Windows (unless they are using a smart card for Windows logon).

### **Interactive logon: Message text for users attempting to log on**

The **Interactive logon: Message text for users attempting to log on** security option setting specifies a text message that is displayed to users when they log on. This text is often used for legal reasons, for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.

### **Interactive logon: Message title for users attempting to log on**

The **Interactive logon: Message title for users attempting to log on** security option setting allows a title to be specified in the title bar of the window that contains the Interactive logon users see when they log on to the system.



### **Interactive logon: Number of previous logons to cache (in case domain controller is not available)**

The **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** security option setting determines whether a user can log on to a Windows domain using cached account information. Logon information for domain accounts can be cached locally so that in the event that a domain controller cannot be contacted on subsequent logons, a user can still log on. This setting determines the number of unique users for whom logon information is cached locally. Configuring this value to **0** disables logon caching.

### **Interactive logon: Prompt user to change password before expiration**

The **Interactive logon: Prompt user to change password before expiration** security option setting determines how many days in advance users are warned that their passwords are about to expire. The Account Policies section of this guide recommends configuring user passwords to expire periodically. If users are not notified when their passwords are about to expire, they may not realize it until the passwords have already expired. This could lead to confusion for users accessing the network locally, or make it impossible for users who are accessing your organization's network via dial – up or virtual private networking (VPN) connections.

### **Interactive logon: Require Domain Controller authentication to unlock workstation**

For domain accounts, the **Interactive logon: Require Domain Controller authentication to unlock workstation** security option setting determines whether a domain controller must be contacted to unlock a computer. This setting addresses a vulnerability similar to the **Interactive logon: Number of previous logons to cache (in case domain controller is not available)** setting. A user could disconnect the network cable of the server and unlock the server using an old password without authenticating to unlock the server.

### **Interactive logon: Smart card removal behavior**

The **Interactive logon: Smart card removal behavior** security option setting determines what happens when the smart card for a logged – on user is removed from the smart card reader. Setting this option to **Lock Workstation** locks the workstation when the smart card is removed, allowing users to leave the area, take their smart cards with them, and automatically lock their workstations.

### **Microsoft network client: Digitally sign communications (always)**

The **Microsoft network client: Digitally sign communications (always)** security option setting determines whether packet signing is required by the SMB client component. Enabling this setting prevents the Microsoft network client from communicating with a Microsoft network server unless that server agrees to perform SMB packet signing. In mixed environments with legacy clients, set this option to **Disabled** as these clients will not be able to authenticate or gain access to domain controllers. However, you can use this setting in Windows 2000 or later environments.



### **Microsoft network client: Digitally sign communications (if server agrees)**

The **Microsoft network client: Digitally sign communications (if server agrees)** security option setting determines whether the SMB client will attempt to negotiate SMB packet signing. Implementing digital signing in Windows networks helps to prevent session hijacking. By enabling this setting, the Microsoft network client on member servers will request signing only if the servers with which it is communicating accept digitally signed communication.

### **Microsoft network client: Send unencrypted password to third – party SMB**

If the **Microsoft network client: Send unencrypted password to third – party SMB servers** security option setting is enabled, the SMB redirector is allowed to send plaintext passwords to non – Microsoft SMB servers that do not support password encryption during authentication.

### **Microsoft network server: Amount of idle time required before suspending session**

The **Microsoft network server: Amount of idle time required before suspending session** security option setting determines the amount of continuous idle time that must pass in an SMB session before the session is suspended due to inactivity. Administrators can use this policy to control when a computer suspends an inactive SMB session. If client activity resumes, the session is automatically reestablished.

### **Microsoft network server: Digitally sign communications (always)**

option setting determines whether packet signing is required by the SMB server component before further communication with an SMB client is permitted. Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, and Windows XP Professional include versions of SMB that support mutual authentication, which closes session hijacking attacks and supports message authentication (thus preventing man-in-the-middle attacks). SMB signing provides this authentication by placing a digital signature into each SMB packet, which is then verified by both the client and the server. When computers are configured to ignore all unsigned SMB communications, legacy applications and operating systems will be unable to connect. Completely disabling all SMB signing leaves the computers vulnerable to session hijacking attacks.

### **Microsoft network server: Digitally sign communications (if client agrees)**

The **Microsoft network server: Digitally sign communications (if client agrees)** security option setting determines whether the SMB server will negotiate SMB packet signing with clients that request it. Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, and Windows XP Professional include versions of SMB that support mutual authentication, which closes session hijacking attacks and supports message authentication (thus preventing man-in-the-middle attacks). SMB signing provides this authentication by placing a digital signature into each SMB packet, which is then verified by both the client and the server. When computers are configured to ignore all unsigned SMB communications, legacy applications and operating



systems will be unable to connect. Completely disabling all SMB signing leaves the computers vulnerable to session hijacking attacks.

### **Microsoft network server: Disconnect clients when logon hours expire**

The **Microsoft network server: Disconnect clients when logon hours expire** security option setting determines whether to disconnect users who are connected to a network computer outside of their user account's valid logon hours. This setting affects the SMB component. If your organization has configured logon hours for users, then it makes sense to enable this setting; otherwise, users should not be able to access network resources outside of their logon hours or they may be able to continue to use those resources with sessions established *during* allowed hours.

### **Network access: Do not allow anonymous enumeration of SAM accounts**

The **Network access: Do not allow anonymous enumeration of SAM accounts** security option setting determines what additional permissions will be granted for anonymous connections to the computer.

### **Network access: Do not allow anonymous enumeration of SAM accounts and shares**

The **Network access: Do not allow anonymous enumeration of SAM accounts and shares** security option setting determines whether anonymous enumeration of SAM accounts and shares is allowed.

### **Network access: Do not allow storage of credentials or .NET Passports for network authentication**

The **Network access: Do not allow storage of credentials or .NET Passports for network authentication** security option setting determines whether settings for **Stored User Names and Passwords** will save passwords, credentials, or Microsoft .NET Passports for later use after gaining domain authentication.

### **Network access: Let Everyone permissions apply to anonymous users**

The **Network access: Let Everyone permissions apply to anonymous users** security option setting determines what additional permissions are granted for anonymous connections to the computer. Enabling this setting allows anonymous Windows users to perform certain activities, such as enumerating the names of domain accounts and network shares. An unauthorized user could anonymously list account names and shared resources and use the information to guess passwords or perform social engineering attacks.



### **Network access: Named Pipes that can be accessed anonymously**

The **Network access: Named Pipes that can be accessed anonymously** security option setting determines which communication sessions (named pipes) will have attributes and permissions that allow anonymous access.

### **Network access: Remotely accessible registry paths**

The **Network access: Remotely accessible registry paths** security option setting determines which registry paths can be accessed over the network.

### **Network access: Remotely accessible registry paths and sub – paths**

The **Network access: Remotely accessible registry paths and sub – paths** security option setting determines which registry paths and sub – paths can be accessed over the network.

### **Network access: Restrict anonymous access to Named Pipes and Shares**

The **Network access: Restrict anonymous access to Named Pipes and Shares** security option setting restricts anonymous access to shares and named pipes when it is enabled to the settings for:

- **Network access: Named pipes that can be accessed anonymously**
- **Network access: Shares that can be accessed anonymously**

### **Network access: Shares that can be accessed anonymously**

The **Network access: Shares that can be accessed anonymously** security option setting determines which network shares can be accessed by anonymous users. The default for this setting has little impact as all users have to be authenticated before they can access shared resources on the server.

### **Network access: Sharing and security model for local accounts**

The **Network access: Sharing and security model for local accounts** security option setting determines how network logons using local accounts are authenticated. The **Classic** setting allows fine control over access to resources. Using the **Classic** setting allows you to grant different types of access to different users for the same resource. Using the **Guest only** setting allows you to treat all users equally. In this context, all users authenticate as **Guest only** to receive the same access level to a given resource.

### **Network security: Do not store LAN Manager hash value on next password change**

The **Network security: Do not store LAN Manager hash value on next password change** security option setting determines whether the LAN Manager (LM) hash value for the new password is stored when the password is changed. The LM hash is relatively weak and prone to attack, as compared with the cryptographically stronger Windows NT hash.



## Network Security: Force Logoff when Logon Hours expire

The **Network Security: Force Logoff when Logon Hours expire** setting determines whether to disconnect users who are connected to a local computer outside their user account's valid logon hours. This setting affects the SMB component.

Enabling this policy forcibly disconnects client sessions with the SMB server when the client's logon hours expire and the user will be unable to log on to the system until his or her next scheduled access time. Disabling this policy maintains an established client session after the client's logon hours expire. To affect domain accounts, this setting must be defined in the Default Domain Policy.

## Network security: LAN Manager authentication level

The **Network security: LAN Manager authentication level** security option setting determines which challenge/response authentication protocol is used for network logons. This choice affects the level of authentication protocol used by clients, the level of security negotiated, and the level of authentication accepted by servers as follows. The following numbers in parentheses below are the actual settings for the **LMCompatibilityLevel** registry value. This setting should be configured to the highest level that your environment allows according to the following guidelines:

In a pure Windows NT 4.0 SP4 or later environment — including Windows 2000 and Windows XP Professional — configure this setting to **Send NTLMv2 response only\refuse LM & NTLM** on all clients, and then to **Send NTLMv2 response only\refuse LM & NTLM** on all servers once all clients are configured. The exception to this recommendation is Windows 2003 Routing and Remote Access servers, which will not function properly if this setting is set higher than **Send NTLMv2 response only\refuse LM**.

The Enterprise Client environment contains Routing and Remote Access servers. For this reason, the setting for this environment is configured to **Send NTLMv2 response only\refuse LM**. The High Security environment does not contain Routing and Remote Access servers, so the setting for this environment is configured to **Send NTLMv2 response only\refuse LM & NTLM**.

If you have Windows 9x clients, and you can install the DSClient on all such clients, configure this setting to **Send NTLMv2 response only\refuse LM & NTLM** on computers running Windows NT (Windows NT, Windows 2000, and Windows XP Professional) Otherwise, you must leave this setting configured at no higher than **Send NTLMv2 responses only** on computers not running Windows 9x.

## Network security: LDAP client signing requirements

The **Network security: LDAP client signing requirements** security option setting determines the level of data signing that is requested on behalf of clients issuing LDAP BIND requests. Unsigned network traffic is susceptible to man – in – the – middle attacks. In the case of an LDAP server, this means that an attacker could cause a server to make decisions based on false queries from the LDAP client.



### **Network security: Minimum session security for NTLM SSP based (including secure RPC) clients**

The **Network security: Minimum session security for NTLM SSP based (including secure RPC) clients** security option setting allows a client to require the negotiation of message confidentiality (encryption), message signing, 128 – bit encryption, or NTLM version 2 (NTLMv2) session security.

### **Network security: Minimum session security for NTLM SSP based (including secure RPC) servers**

The **Network security: Minimum session security for NTLM SSP based (including secure RPC) servers** security option setting allows a server to require the negotiation of message confidentiality (encryption), message integrity, 128 – bit encryption, or NTLMv2 session security.

### **Recovery console: Allow automatic administrative logon**

The **Recovery console: Allow automatic administrative logon** security option setting determines whether the password for the **Administrator** account must be given before access to the system is granted. If this option is enabled, the Recovery Console does not require you to provide a password, and it automatically logs on to the system. The Recovery Console can be very useful when troubleshooting and repairing systems that cannot be restarted normally. However, enabling this setting can be detrimental because anyone can then walk up to the server, shut it down by disconnecting the power, restart it, select **Recover Console** from the **Restart** menu, and then assume full control of the server.

### **Recovery console: Allow floppy copy and access to all drives and all folders**

Enabling the **Recovery console: Allow floppy copy and access to all drives and all folders** security option setting makes the Recovery Console **SET** command available, which allows you to set the following Recovery Console environment variables:

- **AllowWildCards**: Enables wildcard support for some commands (such as the DEL command)
- **AllowAllPaths**: Allows access to all files and folders on the computer
- **AllowRemovableMedia**: Allows files to be copied to removable media, such as a floppy disk
- **NoCopyPrompt**: Does not prompt when overwriting an existing file

### **Shutdown: Allow system to be shut down without having to log on**

The **Shutdown: Allow system to be shut down without having to log on** security option setting determines whether a computer can be shut down without having to log on to the Windows operating system. Users who can access the console could shut the system down. An attacker or misguided user could connect to the server via Terminal Services and shut it down or restart it without having to identify him or herself.



## **Shutdown: Clear virtual memory page file**

The **Shutdown: Clear virtual memory page file** security option setting determines whether the virtual memory pagefile is cleared when the system is shut down. When this setting is enabled, it causes the system pagefile to be cleared each time that the system shuts down gracefully. If you enable this security setting, the hibernation file (hiberfil.sys) is also zeroed out when hibernation is disabled on a portable computer system. Shutting down and restarting the server will take longer and will be especially noticeable on servers with large paging files.

## **System cryptography: Force strong key protection for user keys stored on the computer**

The **System cryptography: Force strong key protection for user keys stored on the computer** security option setting determines whether users' private keys, such as their SMIME keys, require a password to be used. If this policy is configured so that users must provide a password — distinct from their domain password — every time that they use a key, then even if an attacker takes control of their computer and determines what their logon password is, accessing locally stored user keys will be more difficult.

## **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing**

The **System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing** security option setting determines whether the Transport Layer Security/Secure Sockets Layer (TL/SS) Security Provider supports only the TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA cipher suite. Although this setting increases security most public websites secured with TLS or SSL do not support these algorithms. Many client computers are also not configured to support these algorithms.

## **System objects: Default owner for objects created by members of the Administrators group**

The **System objects: Default owner for objects created by members of the Administrators group** security option setting determines whether the Administrators group or an object creator is the default owner of any system objects that are created. When system objects are created, the ownership will reflect which account created the object rather than the more generic Administrators group.

## **System objects: Require case insensitivity for non – Windows subsystems**

The **System objects: Require case insensitivity for non – Windows subsystems** security option setting determines whether case insensitivity is enforced for all subsystems. The Microsoft Win32® subsystem is case insensitive. However, the kernel supports case sensitivity for other subsystems, such as the Portable Operating System Interface for UNIX (POSIX). Since Windows is case insensitive (but the POSIX subsystem will support case sensitivity), not enforcing this setting makes it possible for a user of this subsystem to create a file with the same name as another file by using mixed case to label it. Doing this may block another user accessing these files with normal Win32 tools, because only one of the files will be available.



## System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)

The **System objects: Strengthen default permissions of internal system objects (e.g. Symbolic Links)** security option setting determines the strength of the default discretionary access control list (DACL) for objects. The setting helps secure objects that can be located and shared among processes. Ensuring that this setting is set to the default strengthens the DACL, allowing users who are not administrators to read shared objects but not to modify any that they did not create.

## System settings: Optional subsystems

The **System settings: Optional subsystems** security option setting determines which subsystems are used to support applications in your environment. The default value for this setting in Windows Server 2003 is **POSIX**.

## Event Log

The event logs records events on the system. The security log records audit events. The event log container of Group Policy is used to define attributes related to the application, security, and system event logs, such as maximum log size, access rights for each log, and retention settings and methods. The settings for the application, security, and system event logs are configured in the MSBP and applied to all member servers in the domain.

Log File Setting	Default	Member Server	High Security	Domain Controller
Maximum application log size	16,384 KB	≥16,384 KB	≥16,384 KB	≥16,384 KB
Maximum security log size	16,384 KB	≥100,000 KB	≥100,000 KB	≥100,000 KB
Maximum system log size	16,384 KB	≥16,384 KB	≥16,384 KB	≥16,384 KB
Prevent local guests group from accessing application log	Enabled	Enabled	Enabled	Enabled
Prevent local guests group from accessing security log	Enabled	Enabled	Enabled	Enabled
Prevent local guests group from accessing system log	Enabled	Enabled	Enabled	Enabled
Retention method for application log	As needed	As needed	As needed	As needed
Retention method for security log	As needed	As needed	As needed	As needed
Retention method for system log	As needed	As needed	As needed	As needed

## Maximum application log size

The **Maximum application log size** security setting specifies the maximum size of the application event log, which has a maximum capacity of 4 gigabytes (GB), although this is not recommended because of the risk of memory fragmentation leading to slow performance and



unreliable event logging. Requirements for the application log size vary depending on the function of the platform and the need for historical records of application related events.

### **Maximum security log size**

The **Maximum security log size** security setting specifies the maximum size of the security event log, which has a maximum capacity of 4 GB. Configuring the security log to at least 80 MB on domain controllers and stand – alone servers should adequately store enough information to conduct audits. Configuring this log for other systems to an adequate size is based on factors that include how frequently the log will be reviewed, available disk space, and so on.

### **Maximum system log size**

The **Maximum system log size** security setting specifies the maximum size of the application event log, which has a maximum capacity of 4 GB — although this is not recommended because of the risk of memory fragmentation leading to slow performance and unreliable event logging. Requirements for the application log size vary depending on the function of the platform and the need for historical records of application related events.

### **Prevent local guests group from accessing application log**

The **Prevent local guests group from accessing application log** security setting determines whether guests are prevented from accessing the application event log. By default in Windows Server 2003, guest access is prohibited on all systems.

### **Prevent local guests group from accessing security log**

The **Prevent local guests group from accessing security log** security setting determines whether guests are prevented from accessing the security event log. A user must possess the Manage auditing and security log user right that is not defined in this guidance to access the security log.

### **Prevent local guests group from accessing system log**

The **Prevent local guests group from accessing system log** security setting determines whether guests are prevented from accessing the system event log. By default in Windows Server 2003, guest access is prohibited on all systems.

### **Retention method for application log**

The **Retention method for application log** security setting determines the "wrapping" method for the application log. It is imperative that the application log is archived regularly if historical events are desirable for either forensics or troubleshooting purposes. Overwriting events as needed ensures that the log always stores the most recent events, although this could result in a loss of historical data.

### **Retention method for security log**

The **Retention method for security log** security setting determines the "wrapping" method for the security log. It is imperative that the security log is archived regularly if historical events are desirable for either forensics or troubleshooting purposes. Overwriting events as needed ensures



that the log always stores the most recent events, although this could result in a loss of historical data.

## Retention method for system log

The **Retention method for system log** security setting determines the "wrapping" method for the system log. It is imperative that the logs are archived regularly if historical events are desirable for either forensics or troubleshooting purposes. Overwriting events as needed ensures that the log always stores the most recent events, although this could result in a loss of historical data.

## System Services

When Windows Server 2003 is first installed, default system services are created and are configured to run when the system starts.

Service	Default	Member Server	High Security	Domain Controller
Alerter (Alerter)	Disabled	Disabled	Disabled	Disabled
Application Layer Gateway Service (ALG)	Manual	Disabled	Disabled	Disabled
Application Management (AppMgmt)	Manual	Disabled	Disabled	Disabled
ASP .NET State Service (aspnet_state)	Not Installed	Not Installed	Not Installed	Not Installed
Automatic Updates (wuauserv)	Automatic	Automatic – Depending on your configuration	Automatic – Depending on your configuration	Automatic – Depending on your configuration
Background Intelligent Transfer Service (BITS)	Manual	Manual	Manual	Manual
Certificate Services (CertSvc)	Not Installed	Not Installed	Not Installed	Not Installed
Client Service for Netware (NWCWorkstation)	Not Installed	Not Installed	Not Installed	Not Installed
ClipBook (ClipSrv)	Disabled	Disabled	Disabled	Disabled
Cluster Service (ClusSvc)	Not Installed	Not Installed	Not Installed	Not Installed
COM+ Event System (COMSysApp)	Manual	Manual	Manual	Manual
COM+ System Application (EventSystem)	Manual	Disabled	Disabled	Disabled
Computer Browser (Browser)	Automatic	Automatic	Automatic	Automatic
Cryptographic Services (CryptSvc)	Automatic	Automatic	Automatic	Automatic
DHCP Client (Dhcp)	Automatic	Automatic	Automatic	Automatic
DHCP Server (DHCPService)	Not Installed	Not Installed	Not Installed	Not Installed
Distributed File System (Dfs)	Automatic	Disabled	Disabled	Automatic
Distributed Link Tracking Client (TrkWks)	Automatic	Disabled	Disabled	Disabled
Distributed Link Tracking Server (TrkSvr)	Manual	Disabled	Disabled	Automatic
Distributed Transaction Coordinator (MSDTC)	Automatic	Disabled	Disabled	Disabled
DNS Client (Dnscache)	Automatic	Automatic	Automatic	Automatic
DNS Server (DNS)	Not Installed	Not Installed	Not Installed	Automatic
Error Reporting Service (ERSvc)	Automatic	Disabled	Disabled	Automatic



Service	Default	Member Server	High Security	Domain Controller
Event Log (EventLog)	Automatic	Automatic	Automatic	Automatic
Fax Service (Fax0)	Not Installed	Not Installed	Not Installed	Not Installed
File Replication Service (NtFrs)	Manual	Disabled	Disabled	Automatic
File Server for Macintosh (MacFile)	Not Installed	Not Installed	Not Installed	Not Installed
FTP Publishing Service (MSFtpsvc)	Not Installed	Not Installed unless server is a FTP server	Not Installed unless server is a FTP server	Not Installed
Help and Support (helpsvc)	Automatic	Disabled	Disabled	Disabled
HTTP SSL (HTTPFilter)	Manual	Disabled	Disabled	Disabled
Human Interface Device Access (HidServ)	Disabled	Disabled	Disabled	Disabled
IAS Jet Database Access (IASJet)	Not Installed	Not Installed	Not Installed	Not Installed
IIS Admin Service (IISADMIN)	Not Installed	Not Installed unless server is an IIS web server	Not Installed unless server is an IIS web server	Not Installed
IMAPI CD-Burning COM Service (ImapiService)	Disabled	Disabled	Disabled	Disabled
Indexing Service (cisvc)	Disabled	Disabled	Disabled	Disabled
Infrared Monitor (Irmon)	Not Installed	Not Installed	Not Installed	Not Installed
Internet Authentication Service (IAS)	Not Installed	Not Installed	Not Installed	Not Installed
Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)	Disabled	Disabled	Disabled	Disabled
Intersite Messaging (IsmServ)	Disabled	Disabled	Disabled	Automatic
IP Version 6 Helper Service (6to4)	Not Installed	Not Installed	Not Installed	Not Installed
IPSEC Services (PolicyAgent)	Automatic	Automatic	Automatic	Automatic
Kerberos Key Distribution Center (Kdc)	Automatic	Automatic	Automatic	Automatic
License Logging (LicenseService)	Disabled	Disabled	Disabled	Disabled
Logical Disk Manager (dmserver)	Automatic	Manual	Manual	Manual
Logical Disk Manager Administrative Service (dmadmin)	Manual	Manual	Manual	Manual
Message Queuing (msmq)	Not Installed	Not Installed	Not Installed	Not Installed
Message Queuing Down Level Clients (mqds)	Not Installed	Not Installed	Not Installed	Not Installed
Message Queuing Triggers (Mqtgsvc)	Not Installed	Not Installed	Not Installed	Not Installed
Messenger (Messenger)	Disabled	Disabled	Disabled	Disabled
Microsoft POP3 Service (POP3SVC)	Not Installed	Not Installed	Not Installed	Not Installed
MSSQL\$UDDI (MSSQL\$UDDI)	Not Installed	Not Installed	Not Installed	Not Installed
MSSQLServerADHelper (MSSQLServerADHelper)	Not Installed	Not Installed	Not Installed	Not Installed
MS Software Shadow Copy Provider (SwPrv)	Manual	Manual	Manual	Manual
.NET Framework Support Service (CORRTSvc)	Not Installed	Not Installed	Not Installed	Not Installed
Net Logon	Automatic	Automatic	Automatic	Automatic
NetMeeting Remote Desktop Sharing (mnmsrvc)	Disabled	Disabled	Disabled	Disabled



<b>Service</b>	<b>Default</b>	<b>Member Server</b>	<b>High Security</b>	<b>Domain Controller</b>
Network Connections (Netman)	Manual	Manual	Manual	Manual
Network DDE (NetDDE)	Disabled	Disabled	Disabled	Disabled
Network DDE DSDM (NetDDEdsdm)	Disabled	Disabled	Disabled	Disabled
Network Location Awareness (NLA)	Manual	Manual	Manual	Manual
Network News Transfer Protocol (NNTP)	Not Installed	Not Installed	Not Installed	Not Installed
NT LM Security Support Provider (NtLmSsp)	Not Installed	Automatic	Automatic	Automatic
Performance Logs and Alerts (SysmonLog)	Manual	Manual	Manual	Manual
Plug and Play (PlugPlay)	Automatic	Automatic	Automatic	Automatic
Portable Media Serial Number Service (WmdmPmSN)	Manual	Disabled unless the server is a print server	Disabled	Disabled
Print Server for Macintosh (MacPrint)	Not installed	Not installed	Not installed	Not installed
Print Spooler (Spooler)	Automatic	Disabled unless the server is a print server	Disabled	Disabled
Protected Storage (ProtectedStorage)	Automatic	Automatic	Automatic	Automatic
Remote Access Auto Connection Manager (RasAuto)	Manual	Disabled	Disabled	Disabled
Remote Access Connection Manager (RasMan)	Manual	Disabled	Disabled	Disabled
Remote Administration Service (SrvcSurg)	Not installed	Manual	Manual	Manual
Remote Desktop Help Session Manager (RDSessMgr)	Manual	Disabled	Disabled	Disabled
Remote Installation (BINLSVC)	Not Installed	Not installed	Not installed	Not installed
Remote Procedure Call (RpcSs)	Automatic	Automatic	Automatic	Automatic
Remote Procedure Call Locator (RPCLocator)	Manual	Disabled	Disabled	Automatic
Remote Registry Service (RemoteRegistry)	Automatic	Automatic	Automatic	Automatic
Remote Server Manager (AppMgr)	Not Installed	Not installed	Not installed	Not installed
Remote Server Monitor (Appmon)	Not installed	Not installed	Not installed	Not installed
Remote Storage Notification (Remote Storage User Link)	Not installed	Not installed	Not installed	Not installed
Remote Storage Server (Remote Storage Server)	Not installed	Not installed	Not installed	Not installed
Removable Storage (NtmsSvc)	Manual	Manual	Manual	Manual
Resultant Set of Policy Provider (RsoPProv)	Manual	Disabled	Disabled	Disabled
Routing and Remote Access (RemoteAccess)	Disabled	Disabled	Disabled	Disabled
SAP Agent (nwsapagent)	Not installed	Not installed	Not installed	Not installed



Service	Default	Member Server	High Security	Domain Controller
Secondary Logon (seclogon)	Automatic	Disabled	Disabled	Disabled
Security Accounts Manager (SamSs)	Automatic	Automatic	Automatic	Automatic
Server (lanmanserver)	Automatic	Automatic	Automatic	Automatic
Shell Hardware Detection (ShellHWDetection)	Automatic	Disabled	Disabled	Disabled
Simple Mail Transport Protocol (SMTPSVC)	Not Installed	Not installed	Not installed	Not installed
Simple TCP/IP Services (SimpTcp)	Not Installed	Not installed	Not installed	Not installed
Single Instance Storage Groveler (Groveler)	Not Installed	Not installed	Not installed	Not installed
Smart Card (ScardSvr)	Manual	Disabled	Disabled	Disabled
SNMP Service (SNMP)	Not Installed	Not installed	Not installed	Not installed
SNMP Trap Service (SNMPTRAP)	Not Installed	Not installed	Not installed	Not installed
Special Administration Console Helper (Sacsrv)	Manual	Disabled	Disabled	Disabled
SQLAgent\$* (UDDI or WebDB)	Not Installed	Not installed	Not installed	Not installed
System Event Notification (SENS)	Automatic	Automatic	Automatic	Automatic
Task Scheduler (Schedule)	Automatic	Disabled	Disabled	Disabled
TCP/IP NetBIOS Helper (LMHosts)	Automatic	Automatic	Automatic	Automatic
TCP/IP Print Server (LPDSVC)	Not Installed	Not installed	Not installed	Not installed
Telephony (TapiSrv)	Manual	Disabled	Disabled	Disabled
Telnet (TIntSvr)	Disabled	Disabled	Disabled	Disabled
Terminal Services (TermService)	Manual	Automatic	Consider either Manual or Disabled if you do not use this management protocol.	Consider either Manual or Disabled if you do not use this management protocol.
Terminal Services Licensing (TermServ Licensing)	Not Installed	Not Installed	Not Installed	Not Installed
Terminal Services Session Directory (Tssdis)	Disabled	Disabled	Disabled	Disabled
Themes (Themes)	Disabled	Disabled	Disabled	Disabled
Trivial FTP Daemon (ftpd)	Not Installed	Not Installed	Not Installed	Not Installed
Uninterruptible Power Supply (UPS)	Manual	Disabled – Depending on your configuration	Disabled – Depending on your configuration	Disabled – Depending on your configuration
Upload Manager (Uploadmgr)	Manual	Disabled	Disabled	Disabled
Virtual Disk Service (VDS)	Manual	Disabled	Disabled	Disabled
Volume Shadow Copy (VSS)	Manual	Disabled	Disabled	Disabled
WebClient (WebClient)	Disabled	Disabled	Disabled	Disabled
Web Element Manager (elementmgr)	Not Installed	Not Installed	Not Installed	Not Installed
Windows Audio (AudioSrv)	Disabled	Disabled	Disabled	Disabled
Windows Image Acquisition (WIA)	Disabled	Disabled	Disabled	Disabled
Windows Installer (MSIServer)	Manual	Manual	Manual	Manual



Service	Default	Member Server	High Security	Domain Controller
Windows Internet Name Service (WINS)	Not Installed	Not Installed	Not Installed	Automatic – Depending on your Configuration
Windows Management Instrumentation (winmgmt)	Automatic	Automatic	Automatic	Automatic
Windows Management Instrumentation Driver Extensions (Wmi)	Manual	Manual	Manual	Manual
Windows Media Services (WMServer)	Not Installed	Not Installed	Not Installed	Not Installed
Windows System Resource Manager (WindowsSystemResourceManager)	Not Installed	Not Installed	Not Installed	Not Installed
Windows Time (W32Time)	Automatic	Automatic	Automatic	Automatic
WinHTTP Web Proxy Auto-Discovery Service (WinHttpAutoProxySvc)	Manual	Disabled	Disabled	Disabled
Wireless Configuration (WZCSVC)	Automatic on Standard, Enterprise, and Datacenter Server. Manual on Web Server	Disabled	Disabled	Disabled
WMI Performance Adapter (WmiApSrv)	Manual	Manual	Manual	Manual
Workstation (lanmanworkstation)	Automatic	Automatic	Automatic	Automatic
World Wide Web Publishing Service (W3SVC)	Not Installed	Not Installed unless server is an IIS web server	Not Installed unless server is an IIS web server	Not Installed

### **Alerter (Alerter)**

The **Alerter** system service notifies selected users and computers of administrative alerts. Use the Alerter service to send alert messages to specified users that are connected on your network.

### **Application Layer Gateway Service (ALG)**

The **Application Layer Gateway Service** system service is a subcomponent of the Internet Connection Sharing (ICS) / Internet Connection Firewall (ICF) service that provides support protocol plug – ins that allow network protocols to pass through the firewall and work behind ICS.



### **Application Management (AppMgmt)**

The **Application Management** system service provides software installation services, such as Assign, Publish, and Remove. This service processes requests to enumerate, install, and remove programs deployed via a Microsoft network.

### **ASP .NET State Service (aspnet\_state)**

The **ASP .NET State Service** system service provides support for out – of – process session states for ASP.NET.

### **Automatic Updates (wuauserv)**

The **Automatic Updates** system service enables the download and installation of critical Windows updates.

### **Background Intelligent Transfer Service (BITS)**

The **Background Intelligent Transfer Service** (BITS) system service is a background file – transfer mechanism and queue manager. BITS is used to transfer files asynchronously between a client and an HTTP server.

### **Certificate Services (CertSvc)**

The **Certificate Services** system service is part of the core operating system that enables a business to act as its own certification authority (CA) and issue and manage digital certificates.

### **Client Service for Netware (NWCWorkstation)**

The **Client Service for Netware** system service provides access to file and print resources on NetWare networks to users interactively logged on to servers on which the service is installed. With Client Service for Netware, you can access file and print resources on Netware Servers that are running Novell Directory Services (NDS) or bindery security (NetWare versions 3.x or 4.x) from your computer.

### **ClipBook (ClipSrv)**

The **ClipBook** system service enables the Clipbook Viewer to create and share “pages” of data that may be viewed by remote computers. This service depends on the Network Dynamic Data Exchange (NetDDE) service to create the actual file shares that other computers can connect to, while the Clipbook application and service allow you to create the pages of data to share.

### **Cluster Service (ClusSvc)**

The **Cluster Service** system service controls server cluster operations and manages the cluster database. A cluster is a collection of independent computers that is as easy to use as a single computer, but it can be very difficult to manage. Managers see it as a single system, and programmers and users see it as a single system. The **Cluster Service** spreads data and computation among the nodes of the cluster. When a node fails, other nodes provide the services and data formerly provided by the missing node. When a node is added or repaired, the **Cluster Service** software migrates some data and computation to that node.



## **COM+ Event System (COMSysApp)**

The **COM+ Event System** service provides automatic distribution of events to subscribing COM components. The **COM+ Events** service extends the COM+ programming model to support late – bound events or method calls between the publisher or subscriber and the event system. Instead of repeatedly polling the server, the event system notifies you as information becomes available.

## **COM+ System Application (EventSystem)**

The **COM+ System Application** system service manages the configuration and tracking of components based on COM+.

## **Computer Browser (Browser)**

The **Computer Browser** system service maintains an up – to – date list of computers on your network and supplies the list to programs that request it. The **Computer Browser** service is used by Windows – based computers that need to view network domains and resources

## **Cryptographic Services (CryptSvc)**

The **Cryptographic Services** system service provides key management services for your computer.

## **DHCP Client (Dhcp)**

The **DHCP Client** system service manages network configuration by registering and updating IP addresses and updating Dynamic Domain Naming Service (DDNS) entries for your computer with DNS servers. You do not have to manually change the IP settings when a client, such as a roaming user, wanders throughout the network. The client is automatically given a new IP address regardless of the subnet it reconnects to—as long as a DHCP server is accessible from each of those subnets.

## **DHCP Server (DHCPServer)**

The **DHCP Server** system service allocates IP addresses and enables advanced configuration of network settings such as DNS servers and WINS servers to DHCP clients automatically.

## **Distributed File System (Dfs)**

The **Distributed File System** (DFS) service manages logical volumes distributed across a local or wide area network. DFS is a distributed service that integrates disparate file shares into a single logical namespace.

## **Distributed Link Tracking Client (TrkWks)**

The **Distributed Link Tracking Client** system service maintains links between the NTFS files within your computer or across computers in your network domain. The Distributed Link Tracking (DLT) Client service ensures that shortcuts and Object Linking and Embedding (OLE) links continue to work after the target file is renamed or moved.



## **Distributed Link Tracking Server (TrkSvr)**

The **Distributed Link Tracking Server** system service stores information so that files moved between volumes can be tracked for each volume in the domain. When enabled, the **Distributed Link Tracking Server** service runs on domain controllers.

## **Distributed Transaction Coordinator (MSDTC)**

The **Distributed Transaction Coordinator** system service is responsible for coordinating transactions that are distributed across multiple computer systems or resource managers, such as databases, message queues, file systems, or other transaction – protected resource managers.

## **DNS Client (Dnscache)**

The **DNS Client** system service resolves and caches DNS names for your computer. The DNS client service must be running on every computer that performs DNS name resolution. Resolving DNS names is essential for locating domain controllers in Active Directory domains. Running the DNS client service is also critical for locating devices identified using DNS name resolution.

## **DNS Server (DNS)**

The **DNS Client** system service resolves and caches DNS names for your computer. The DNS client service must be running on every computer that performs DNS name resolution. Resolving DNS names is essential for locating domain controllers in Active Directory domains. Running the DNS client service is also critical for locating devices identified using DNS name resolution.

## **Error Reporting Service (ERSvc)**

The **Error Reporting Service** system service collects, stores, and reports unexpected application closures to Microsoft and authorizes error reporting for services and applications running in non – standard environments. This service provides Microsoft product groups with efficient and effective information to debug driver and application faults. If the Display Error Notification service is enabled, users will still get a message indicating that a problem occurred, but they will not have the option to report this information to Microsoft or a local network error reporting server.

## **Event Log (EventLog)**

The **Event Log** system service enables event log messages issued by Windows – based programs and components to be viewed in Event Viewer. Event Log reports contain information that can be useful in diagnosing problems. If the **Event Log** is disabled, you will be unable to track events, which will significantly reduce the ability to successfully diagnose system problems.

## **Fax Service (Fax)**

The **Fax Service** system service, a Telephony API (TAPI) – compliant service, provides fax capabilities from your computer. The **Fax Service** allows users to send and receive faxes from their desktop applications by using either a local fax device or a shared network fax device.



### **File Replication Service (NtFrs)**

The **File Replication Service** (FRS) enables files to be automatically copied and maintained simultaneously on multiple servers. If the **File Replication Service** is disabled, file replication will not occur, and server data will not synchronize. In the case of a domain controller, stopping the FRS service might have a serious impact on the domain controller's ability to function.

### **File Server for Macintosh (MacFile)**

The **File Server for Macintosh** system service enables Macintosh users to store and access files on a local Windows server computer. This is not a requirement for a standard server environment.

### **FTP Publishing Service (MSFtpsvc)**

The **FTP Publishing Service** provides connectivity and administration through the IIS snap – in. The **FTP Publishing Service** is not a requirement for a standard server environment.

### **Help and Support (helpsvc)**

The **Help and Support** system service enables the Help and Support Center to run on your computer. The service supports the Help and Support Center application and enables communication between the client application and the help data. If this system service is disabled, the Help and Support Center will be unavailable.

### **HTTP SSL (HTTPFilter)**

The **HTTP SSL** system service enables IIS to perform SSL functions. HTTP SSL service enables secure electronic transactions; however, in order to reduce the attack surface, it is recommended to configure the service to Disabled.

### **Human Interface Device Access (HidServ)**

The **Human Interface Device Access** system service enables generic input access to Human Interface Devices (HID), which activate and maintain the use of predefined hot buttons on keyboards, remote controls, and other multimedia devices.

### **IAS Jet Database Access (IASJet)**

The **IAS Jet Database Access** system service is only available on 64-bit versions of Windows Server 2003. The service uses the Remote Authentication Dial – in User Service (RADIUS) protocol to provide authentication, authorization, and accounting services.

### **IIS Admin Service (IISADMIN)**

The **IIS Admin Service** allows administration of IIS components such as FTP, Applications Pools, Web sites, Web service extensions, and both Network News Transfer Protocol (NNTP) and Simple Mail Transfer Protocol (SMTP) virtual servers. If this service is disabled, you cannot run Web, FTP, NNTP, or SMTP sites.



### **IMAPI CD-Burning COM Service(ImapiService)**

The **IMAPI CD – Burning COM Service** manages CD burning through the Image Mastering Applications Programming Interface (IMAPI) COM interface and performs CD – R writes when requested by the user through Windows Explorer, Windows Media™ Player, (WMP) or third – party applications that use this API.

### **Indexing Service (cisvc)**

The **Indexing Service** indexes contents and properties of files on local and remote computers and provides rapid access to files through a flexible querying language. The **Indexing Service** also enables quick searching of documents on local and remote computers and a search index for content shared on the Web.

### **Infrared Monitor (Irmon)**

The **Infrared Monitor** system service enables file and image sharing using infrared. This service is installed by default only if an infrared device is detected during operating system installation of Windows Server 2003. This service is not available on Windows Server 2003 Web, Enterprise, or Datacenter Server. If this service is disabled, files and images cannot be shared using infrared.

### **Internet Authentication Service (IAS)**

The **Internet Authentication Service (IAS)** centrally manages network access authentication, authorization, auditing, and accounting. IAS is for virtual private network (VPN), dial – up, 802.1X wireless or Ethernet switch connection attempts sent by access servers that are compatible with the IETF RADIUS protocol.

### **Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)**

The **Internet Connection Firewall (ICF)/Internet Connection Sharing (ICS)** system service provides network address translation (NAT), addressing and name resolution, and intrusion prevention services for all computers in your home or small – office network through a dial – up or broadband connection.

### **Intersite Messaging (IsmServ)**

The **Intersite Messaging** system service enables messages to be exchanged between computers running Windows Server sites. This service is used for mail – based replication between sites. Active Directory includes support for replication between sites by using SMTP over IP transport. This service is, however, required on domain controllers.

### **IP Version 6 Helper Service (6to4)**

The **IP Version 6 Helper Service** system service offers IPv6 connectivity over an existing IPv4 network.



### **IPSEC Services (PolicyAgent)**

The **IPSEC Policy Agent** service provides end-to-end security between clients and servers on TCP/IP networks. It also manages IP security (IPSec) policy, starts the Internet Key Exchange (IKE), and coordinates IPSec policy settings with the IP security driver.

### **Kerberos Key Distribution Center (Kdc)**

The **Kerberos Key Distribution Center** system service enables users to log on to the network by using the Kerberos v5 authentication protocol.

### **License Logging (LicenseService)**

The **License Logging Service** monitors and records client access licensing for portions of the operating system. These include IIS, Terminal Server, and File/Print, as well as products that are not a part of the operating system, such as SQL Server and Microsoft Exchange Server.

### **Logical Disk Manager (dmserver)**

The **Logical Disk Manager** system service detects and monitors new hard disk drives and sends disk volume information to Logical Disk Manager Administrative Service for configuration. This service watches Plug and Play events for new drives that are detected and passes volume and disk information to the Logical Disk Manager Administrative Service to be configured.

### **Logical Disk Manager Administrative Service (dmadmin)**

The **Logical Disk Manager Administrative Service** performs administrative service for disk management requests and configures hard disk drives and volumes. The **Logical Disk Manager Administrative Service** is started only when you configure a drive or partition or a new drive is detected.

### **Message Queuing (msmq)**

The **Message Queuing** system service is a messaging infrastructure and development tool for creating distributed messaging applications for Windows. This service is not a requirement for the baseline server policy.

### **Message Queuing Down Level Clients (mqds)**

The **Message Queuing Down Level Clients** system service provides Active Directory access for Message Queuing clients (Windows 9x, Windows NT 4.0, and Windows 2000) on domain controllers

### **Message Queuing Triggers (Mqtgsvc)**

The **Message Queuing Triggers** system service provides rule – based monitoring of messages arriving in a Message Queuing queue and, when the conditions of a rule are satisfied, invokes a COM component or a stand – alone executable program to process the message.



### **Messenger (Messenger)**

The **Messenger** system service transmits and sends Alert service messages between clients and servers. This service is not related to Windows Messenger.

### **Microsoft POP3 Service (POP3SVC)**

The **Microsoft POP3 Service** provides e – mail transfer and retrieval services. Administrators can use the POP3 service to store and manage e – mail accounts on the mail server.

### **MSSQL\$UDDI (MSSQL\$UDDI)**

The **MSSQL\$UDDI** system service — Universal Description Discovery and Integration (UDDI) — is an industry specification for publishing and locating information about Web services. The Windows Server 2003 family includes UDDI Services, a Web service that provides UDDI capabilities for use within an enterprise or across organizations.

### **MSSQLServerADHelper (MSSQLServerADHelper)**

The **MSSQLServerADHelper** system service enables SQL Server and SQL Server Analysis Services to publish information in Active Directory when the services are not running under the LocalSystem account.

### **MS Software Shadow Copy Provider (SwPrv)**

The **MS Software Shadow Copy Provider** system service manages software for file shadow copies taken by the Volume Shadow Copy service. A shadow copy enables you to create a copy of a disk volume (or apparent copy) that represents a consistent read – only point in time, for that volume. This point in time then stays constant and allows an application, like Ntbackup, to copy data from the shadow copy to tape.

### **.NET Framework Support Service (CORRTSvc)**

The **.NET Framework Support Service** system service notifies a subscribing client when a specified process is initializing the Client Runtime Service. The **.NET Framework Support Service** provides a run – time environment called the Common Language Runtime, which manages the execution of code and provides services that make the development process easier.

### **Net Logon**

The **Netlogon** system service maintains a secure channel between your computer and the domain controller for authenticating users and services. If this service is disabled, computers on the system network may not authenticate users and services, and the domain controller will not register DNS records. Specifically, disabling this service could deny NTLM authentication requests, and, in case of domain controllers, they will not be discoverable by client computers.

### **NetMeeting Remote Desktop Sharing (mnmsrvc)**

The **NetMeeting Remote Desktop Sharing** system service enables an authorized user to access this computer remotely by using Microsoft NetMeeting® over a corporate intranet. The



service must be explicitly enabled by NetMeeting and can be disabled in NetMeeting or shut down via a Windows tray icon.

### **Network Connections (Netman)**

The **Network Connections** service manages objects in the Network Connections folder, in which you can view both network and remote connections. This service will start automatically when the start up type is **Manual** and the Network Connections interface is invoked.

### **Network DDE (NetDDE)**

The **Network DDE** system service provides network transport and security for Dynamic Data Exchange (DDE) for programs running on the same computer or on different computers.

### **Network DDE DSDM (NetDDEdsdm)**

The **Network DDE DSDM** system service manages DDE network shares. This service is used only by the Network DDE service to manage shared DDE conversations.

### **Network Location Awareness (NLA)**

The **Network Location Awareness (NLA)** system service collects and stores network configuration information such as IP address and domain name changes, as well as location change information, and then notifies programs when this information changes. Disabling this service prevents it from locating networks, and any services that explicitly depend on it will fail to start.

### **Network News Transfer Protocol (NNTP)**

The **Network News Transfer Protocol (NNTP)** system service allows computers running Windows Server 2003 to act as a news server.

### **NT LM Security Support Provider (NtLmSsp)**

The **NTLM Security Support Provider** system service provides security to RPC programs that use transports other than named pipes and enables users to log on to the network using the NTLM authentication protocol. The NTLM protocol authenticates clients that do not use Kerberos v5 authentication. If this service is disabled, users cannot log on to clients by using the NTLM authentication protocol or access network resources.

### **Performance Logs and Alerts (SysmonLog)**

The **Performance Logs and Alerts** system service collects performance data from local or remote computers based on preconfigured schedule parameters; it then writes the data to a log or triggers an alert.

### **Plug and Play (PlugPlay)**

The **Plug and Play** system service enables a computer to recognize and adapt to hardware changes with little or no user input. If this service is stopped by using the MSCONFIG



troubleshooting tool, the Device Manager interface will appear blank, and no hardware devices will be displayed.

### **Portable Media Serial Number Service (WmdmPmSN)**

The **Portable Media Serial Number** system service retrieves the serial number of any portable music player connected to your computer. These features are not required in the baseline server environment.

### **Print Server for Macintosh (MacPrint)**

The **Print Server for Macintosh** system service enables Macintosh clients to route printing to a print spooler located on a computer running Windows Server 2003 Enterprise Server.

### **Print Spooler (Spooler)**

The **Print Spooler** system service manages all local and network print queues and controls all print jobs.

### **Protected Storage (ProtectedStorage)**

The **Protected Storage** system service protects storage of sensitive information, such as private keys, and prevents access by unauthorized services, processes, or users. If this service is disabled, private keys will be inaccessible, certificate server will not operate, S/MIME and SSL will not work, and smart card logon will fail.

### **Remote Access Auto Connection Manager (RasAuto)**

The **Remote Access Auto Connection Manager** system service detects unsuccessful attempts to connect to a remote network or computer and then provides alternative methods for connection. The **Remote Access Auto Connection Manager** service offers to establish a dial – up or virtual private network (VPN) connection to a remote network whenever a program fails in an attempt to reference a remote DNS or NetBIOS name or address.

### **Remote Access Connection Manager (RasMan)**

The **Remote Access Connection Manager** system service manages dial – up and VPN connections from your computer to the Internet or other remote networks.

### **Remote Administration Service (SrvcSurg)**

The **Remote Administration Service** system service is responsible for running the following Remote Administration tasks when the server restarts:

- Increments the server boot count
- Raises an alert if the date and time has not been set on the server
- Raises an alert if the event e-mail notification functionality has not been configured



## **Remote Desktop Help Session Manager (RDSessMgr)**

The **Remote Desktop Help Session Manager** system service manages and controls the Remote Assistance feature in the Help and Support Center application (helpctr.exe).

## **Remote Installation (BINLSVC)**

The **Remote Installation Services (RIS)** system service is a Windows deployment feature included in members of the Windows Server family.

## **Remote Procedure Call (RpcSs)**

The **Remote Procedure Call (RPC)** system service is a secure inter-process communication (IPC) mechanism that enables data exchange and invocation of functionality residing in a different process. Different processes can take place on the same computer, the local area network (LAN), or across the Internet. This service should not be disabled. Disabling the **Remote Procedure Call (RPC)** service will result in the operating system not loading numerous services that are dependent on it.

## **Remote Procedure Call Locator (RPCLocator)**

The **Remote Procedure Call (RPC) Locator** system service enables RPC clients using the RpcNs\* family of APIs to locate RPC servers and manages the RPC name service database. This system service is required for domain controllers.

## **Remote Registry Service (RemoteRegistry)**

The **Remote Registry Service** system service enables remote users to modify registry settings on your computer — provided remote users have the required permissions. The service is primarily used by remote administrators and performance counters. If **Remote Registry Service** is disabled, modifying the registry will only be allowed on the local computer, and any services that explicitly depend on this service will fail to start.

## **Remote Server Manager (AppMgr)**

The **Remote Server Manager** acts as a Windows Management Instrumentation (WMI) instance provider for Remote Administration Alert Objects and a WMI method provider for Remote Administration Tasks.

## **Remote Server Monitor (Appmon)**

The **Remote Server Monitor** system service provides monitoring of critical system resources and manages optional watchdog timer hardware on remotely managed servers.

## **Remote Storage Notification**

The **Remote Storage Notification** system service notifies you when you read or write to files that are only available from a secondary storage media.



### **Remote Storage Server (Remote\_Storage\_Server)**

The **Remote Storage Server** system service stores infrequently used files in secondary storage media. This service allows Remote Storage Notification to notify the user when an offline file has been accessed.

### **Removable Storage (NtmsSvc)**

The **Removable Storage** system service manages and catalogs removable media and operates automated removable media devices. This service maintains a catalog of identifying information for removable media used by your computer, including tapes and CDs.

### **Resultant Set of Policy Provider (RsoPProv)**

The **Resultant Set of Policy Provider** system service enables you to connect to a Windows Server 2003 domain controller, access the WMI database for that computer, and simulate Resultant Set of Policy (RSoP) for Group Policy settings that would be applied to a user or computer located in Active Directory on a Windows 2000 or later domain. This is commonly referred to as planning mode.

### **Routing and Remote Access (RemoteAccess)**

The **Routing and Remote Access** system service provides multi – protocol LAN – to – LAN, LAN – to – WAN, VPN, and NAT routing services. In addition, this service also provides dial – up and VPN remote access services.

### **SAP Agent (nwsapagent)**

The **SAP Agent** system service advertises network services on an IPX network by using the IPX Service Advertising Protocol (IPX SAP) protocol.

### **Secondary Logon (seclogon)**

The **Secondary Logon** system service allows the user to create processes in the context of different security principals. Restricted users commonly use this service to log on as a user with elevated privileges for temporarily running administrative programs. This service enables users to start processes under alternate credentials.

### **Security Accounts Manager (SamSs)**

The **Security Accounts Manager (SAM)** system service is a protected subsystem that manages user and group account information. In Windows 2000 and the Windows Server 2003 family, the SAM in the local computer registry stores workstation security accounts and domain controller accounts are stored in Active Directory.

### **Server (lanmanserver)**

The **Server** system service provides RPC support, file, print, and named pipe sharing over the network.



## **Shell Hardware Detection (ShellHWDetection)**

The **Shell Hardware Detection** system service monitors and provides notification for AutoPlay hardware events. This service is not a requirement for the baseline server policy.

## **Simple Mail Transport Protocol (SMTPSVC)**

The **Simple Mail Transport Protocol (SMTP)** system service transports electronic mail across the network.

## **Simple TCP/IP Services (SimpTcp)**

The **Simple TCP/IP Services** system service supports the following TCP/IP protocols:

- Echo (port 7, RFC 862)
- Discard (port 9, RFC 863)
- Character Generator (port 19, RFC 864)
- Daytime (port 13, RFC 867)
- Quote of the Day (port 17, RFC 865)

## **Single Instance Storage Groveler (Groveler)**

The **Single Instance Storage Groveler (SIS)** system service is an integral component of the Remote Installation Service (RIS) that reduces the overall storage required on the RIS volume.

## **Smart Card (ScardSvr)**

The **Smart Card** system service manages and controls access to a smart card inserted into a smart card reader attached to your computer. If this service is disabled, computers in your environment will be unable to read smart cards. Also, any services that explicitly depend on it will fail to start.

## **SNMP Service (SNMP)**

The **SNMP Service** allows incoming SNMP requests to be serviced by the local computer. The **SNMP Service** includes agents that monitor activity in network devices and report to the network console workstation. There are no requirements or dependencies in the three environments for the **SNMP Server**.

## **SNMP Trap Service (SNMPTRAP)**

The **SNMP Trap Service** receives trap messages generated by local or remote SNMP agents and forwards the messages to SNMP management programs running on your computer.

## **Special Administration Console Helper (Sacsrv)**

The **Special Administration Console Helper** system service (SAC) performs remote management tasks if any of the Windows Server 2003 family of operating systems stops functioning due to a Stop error message.



### **SQLAgent\$\* (UDDI or WebDB)**

**SQLAgent\$\* (\* UDDI or WebDB)** is a job scheduler and monitoring service. It also moves information between computers running SQL Server and is used heavily for backups and replication. If the **SQLAgent\$\* (\* UDDI or WebDB)** service is stopped, SQL replication will not occur. In addition, there will be a disruption of all scheduled jobs and alert/event monitoring and auto restart of the SQL Server service. If this service is disabled, any services that explicitly depend on this service will fail to start.

### **System Event Notification (SENS)**

The **System Event Notification** system service monitors and tracks system events such as Windows logon network and power events and then notifies COM+ Event System subscribers of these events.

### **Task Scheduler (Schedule)**

The **Task Scheduler** system service enables you to configure and schedule automated tasks on your computer. The Task Scheduler service monitors whatever criteria you choose and carries out the task when the criteria have been met.

### **TCP/IP NetBIOS Helper (LMHosts)**

The **TCP/IP NetBIOS Helper Service** system service provides support for NetBIOS over the TCP/IP (NetBT) service and NetBIOS name resolution for clients on your network, thus enabling users to share files, print, and log on to the network.

### **TCP/IP Print Server (LPDSVC)**

The **TCP/IP Print Server** system service enables TCP/IP – based printing using the Line Printer Daemon protocol.

### **Telephony (TapiSrv)**

The **Telephony** service provides API (TAPI) support for programs that control telephony devices, as well as IP-based voice connections on the local computer and through the LANs on servers also running the service.

### **Telnet (TlntSvr)**

The **Telnet** system service for Windows provides ASCII terminal sessions to Telnet clients. This service supports two types of authentication and four types of terminals: ANSI, VT – 100, VT – 52, and VTNT.

### **Terminal Services (TermService)**

The **Terminal Services** system service provides a multi – session environment that allows client devices to access a virtual Windows desktop session and Windows – based programs running on the server. **Terminal Services** allows multiple users to be connected interactively to a computer and to display desktops and applications on remote computers.



## **Terminal Services Licensing (TermServ Licensing)**

The **Terminal Services Licensing** system service installs a licensed server and provides registered client licenses when connecting to a Terminal Server.

## **Terminal Services Session Directory (Tssdis)**

The **Terminal Services Session Directory** system service provides a multi – session environment that allows client devices to access a virtual Windows desktop session and Windows – based programs running on Windows Server 2003.

## **Themes (Themes)**

The **Themes** system service provides user experience theme management services. The **Themes** service provides rendering support for the new Windows XP Professional graphic user interface (GUI).

## **Trivial FTP Daemon (tftpd)**

The **Trivial FTP Daemon** (TFTP) system service does not require a user name or password and is an integral part of RIS. The **Trivial FTP Daemon** service implements support for the TFTP protocol defined by the following RFCs:

- RFC 1350 - TFTP
- RFC 2347 - Option extension
- RFC 2348 - Block size option
- RFC 2349 - Timeout interval and transfer size options

Client computers requesting RIS from this server will fail to install if this service is disabled.

## **Uninterruptible Power Supply (UPS)**

The **Uninterruptible Power Supply** system service manages an uninterruptible power supply (UPS) connected to your computer by a serial port.

## **Upload Manager (Uploadmgr)**

The **Upload Manager** system service manages the synchronous and asynchronous file transfers between clients and servers on the network. Driver data is anonymously uploaded from customer computers to Microsoft and then used to help users find the drivers required for their systems.

## **Virtual Disk Service (VDS)**

The **Virtual Disk Service** (VDS) system service provides a single interface for managing block storage virtualization whether done in operating system software, redundant array of independent disks (RAID) storage hardware subsystems, or other virtualization engines.

## **Volume Shadow Copy (VSS)**

The **Volume Shadow Copy** system service manages and implements Volume Shadow copies used for backup and other purposes. This service is a core requirement for the baseline server policy.



### **WebClient (WebClient)**

The **WebClient** system service allows Win32 applications to access documents on the Internet.

### **Web Element Manager (elementmgr)**

The **Web Element Manager** system service is responsible for serving Web user interface elements for the Administration Web site at port 8098.

### **Windows Audio (AudioSrv)**

The **Windows Audio** system service provides support for sound and related Windows Audio event functions.

### **Windows Image Acquisition (WIA)**

The **Windows Image Acquisition (WIA)** system service provides image acquisition services for scanners and cameras.

### **Windows Installer (MSIServer)**

The **Windows Installer** system service manages the installation and removal of applications by applying a set of centrally – defined setup rules during the installation process.

### **Windows Internet Name Service (WINS)**

The **Windows Internet Name Service (WINS)** system service enables NetBIOS name resolution. Presence of the WINS server(s) is crucial for locating the network resources identified by using NetBIOS names. WINS servers are required unless all domains have been upgraded to Active Directory and all computers on the network are running Windows Server 2003.

### **Windows Management Instrumentation (winmgmt)**

The **Windows Management Instrumentation** system service provides a common interface and object model to access management information about operating systems, devices, applications, and services. WMI is an infrastructure for building management applications and instrumentation shipped as part of the current generation of Microsoft operating systems. If this service is disabled, most Windows – based software will not function properly, and any services that explicitly depend on it will fail to start.

### **Windows Management Instrumentation Driver Extensions (Wmi)**

The **Windows Management Instrumentation Driver Extensions** system service monitors all drivers and event trace providers that are configured to publish WMI or event trace information.

### **Windows Media Services (WMServer)**

The **Windows Media Services** system service provides streaming media services over IP – based networks. This service replaces the four separate services that comprised Windows Media Services versions 4.0 and 4.1: Windows Media Monitor Service, Windows Media Program Service, Windows Media Station Service, and Windows Media Unicast Service.



## **Windows System Resource Manager**

The **Windows System Resource Manager (WSRM)** system service is a tool to help customers deploy applications into consolidation scenarios.

## **Windows Time (W32Time)**

The **Windows Time** system service maintains date and time synchronization on all computers running on a Windows network. It uses the Network Time Protocol (NTP) to synchronize computer clocks so that an accurate clock value, or timestamp, can be assigned to network validation and resource access requests. It is a core requirement for reliable Kerberos authentication in Active Directory domains

## **WinHTTP Web Proxy Auto-Discovery Service (WinHttpAutoProxySvc)**

The **WinHTTP Web Proxy Auto – Discovery Service** system service implements the Web Proxy Auto – Discovery (WPAD) protocol for Windows HTTP Services (WinHTTP). WPAD is a protocol to enable an HTTP client to automatically discover a proxy configuration.

## **Wireless Configuration (WZCSVC)**

The **Wireless Zero Configuration** system service enables automatic configuration for IEEE 802.11 wireless adapters for wireless communications.

## **WMI Performance Adapter (WmiApSrv)**

The **WMI Performance Adapter** system service provides performance library information from WMI HiPerf providers. The service is a manual service and is not running by default. It runs on demand when a performance client (for example, Sysmon) uses Performance Data Helper (PDH) to query performance data. Once the client disconnects, the service stops. If this service is disabled, WMI performance counters will be unavailable.

## **Workstation (lanmanworkstation)**

The **Workstation** system resource creates and maintains client network connections and communications. If this service is disabled, you cannot establish connections to remote servers and access files through named pipes.

## **World Wide Web Publishing Service (W3SVC)**

The **World Wide Web Publishing Service** system service provides Web connectivity and administration through the Internet Information Service snap – in.

## ***Administrative Templates***

### **Disable Automatic Install of Internet Explorer components**

Enabling the **Disable Automatic Install of Internet Explorer components** setting prevents Internet Explorer from downloading components when users browse to Web sites that require these components to fully function. Disabling or not configuring this setting prompts users to



download and install components each time they visit Web sites that use them. This policy is intended to help the administrator control which components the user may install.

Group Policy Value	Default	Setting
Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\ Disable Automatic Install of Internet Explorer components	Not Configured	Enabled

### Terminal Services: Always prompt client for a password on connection

The **Always prompt client for a password on connection** setting specifies whether Terminal Services always prompts the client for a password upon connection. You can use this setting to enforce a password prompt for users logging on to **Terminal Services**, even if they already provided the password in the Remote Desktop Connection client. By default, **Terminal Services** allows users to automatically log on by entering a password in the Remote Desktop Connection client.

Enabling this setting prevents users from automatically logging on to **Terminal Services** by supplying their passwords in the Remote Desktop Connection client. They are prompted for a password to log on. Disabling this setting always allows users to log on to **Terminal Services** automatically by supplying their passwords in the Remote Desktop Connection client.

Group Policy Value	Default	Setting
Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security\ Always prompt client for a password on connection	Not Configured	Enabled

### Terminal Services: Encryption Levels

Specifies whether to enforce an encryption level for all data sent between the client and the remote computer during a Terminal Services session.

Group Policy Value	Default	Setting	Encryption Level
Computer Configuration\Administrative Templates\Windows Components\Terminal Services\Encryption and Security\ Encryption Levels	Not Configured	Enabled	High (128 Bit)

### System: Turn off Autoplay

**Autoplay** starts reading from a drive as soon as you insert media in the drive, causing the setup file for programs or audio media to start immediately. An attacker could use this feature to launch a program to damage a client or data on the computer. Enabling the **Turn off Autoplay** setting turns off the **Autoplay** feature. **Autoplay** is disabled by default on some removable drive types, such as floppy disk and network drives; but this is not the case on CD – ROM drives.

Group Policy Value	Default	Setting
Computer Configuration\Administrative Templates\System\Turn off Autoplay	Not Configured	Enabled

### Screen Saver: Password protect the screen saver

The **Password protect the screen saver** setting determines whether screen savers used on the computer are password – protected.



Enabling this setting makes all screen savers password protected. Disabling this setting prevents password protection from being set on any screen saver. This setting configuration also disables the **Password protected** check box on the **Screen Saver** tab of the **Display in Control Panel** dialog box, which offers another way of preventing users from changing the password protection setting.

Group Policy Value	Default	Setting
User Configuration\Administrative Templates\Control Panel\Display>Password protect the screen saver	Not Configured	Enabled

## Registry Settings

### Security Considerations for Network Attacks

To help prevent denial of service (DoS) attacks, you should keep your computer updated with the latest security fixes and harden the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol stack on your Windows Server 2003 computers that are exposed to potential attackers. The default TCP/IP stack configuration is tuned to handle standard Intranet traffic. If you connect a computer directly to the Internet, Microsoft recommends that you harden the TCP/IP stack to protect against DoS attacks.

DoS attacks directed at the TCP/IP stack tend to be of two classes: attacks that use an excessive number of system resources, for example, by opening numerous TCP connections; or attacks that send specially crafted packets that cause the network stack or the entire operating system to fail. These registry settings help to protect against the attacks directed at the TCP/IP stack. DoS attacks include those that flood a Web server with communication to keep it busy, and others that flood a remote network with an enormous amount of packets. Routers and servers become overloaded by attempting to route or handle each packet. DoS attacks can be difficult to defend against. To help prevent them, the TCP/IP protocol stack can be hardened.

The following registry value entries should be taken into consideration when hardening your server: **HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\**

Subkey Registry Value Entry	Format	Default	Recommended Value (Decimal)
EnableCMPRedirect	DWORD	1	0
SynAttackProtect	DWORD	0	1
EnableDeadGWDetect	DWORD	0	0
EnablePMTUDiscovery	DWORD	1	0
KeepAliveTime	DWORD	7,200,000	300,000
DisableIPSourceRouting	DWORD	0	2
TcpMaxConnectResponseRetransmissions	DWORD	2	2
TcpMaxDataRetransmissions	DWORD	5	3
PerformRouterDiscovery	DWORD	0	0
TCPMaxPortsExhausted	DWORD	5	5



**EnableICMPRedirect: Allow ICMP redirects to override OSPF generated routes**

Internet Control Message Protocol (ICMP) redirects cause the stack to plumb host routes. These routes override the Open Shortest Path First (OSPF) – generated routes.

**SynAttackProtect: Syn attack protection level**

This registry value causes TCP to adjust retransmission of SYN – ACKs. When you configure this value, the connection responses time – out more quickly in the event of a connect request (SYN) attack.

**EnableDeadGWDetect: Allow automatic detection of dead network gateways**

When dead – gateway detection is enabled, TCP may ask the IP to change to a backup gateway if a number of connections are experiencing difficulty.

**EnablePMTUDiscovery: Allow automatic detection of MTU size**

When this value is enabled, the default setting, the TCP stack tries to automatically determine either the maximum transmission unit (MTU) or the largest packet size over the path to a remote host.

**KeepAliveTime: How often keep – alive packets are sent in milliseconds**

This value controls how often TCP attempts to verify that an idle connection is still intact by sending a keep – alive packet. If the remote computer is still reachable, it acknowledges the keep – alive packet.

**DisableIPSourceRouting: IP source routing protection level**

IP source routing is a mechanism allowing the sender to determine the IP route that a datagram should take through the network.

**TcpMaxConnectResponseRetransmissions: SYN – ACK retransmissions when a connection request is not acknowledged**

This parameter determines the number of times that TCP retransmits a SYN before aborting the attempt. The retransmission time – out is doubled with each successive retransmission in a given connect attempt. The initial time – out value is three seconds.

**TcpMaxDataRetransmissions: How many times unacknowledged data is retransmitted**

This parameter controls the number of times that TCP retransmits an individual data segment (non – connect segment) before aborting the connection. The retransmission time – out is doubled with each successive retransmission on a connection. It is reset when responses resume. The base time – out value is dynamically determined by the measured round – trip time on the connection.

**PerformRouterDiscovery: Allow IRDP to detect and configure Default Gateway addresses**

This setting is used to enable or disabled the Internet Router Discovery Protocol (IRDP). IRDP allows the system to detect and configure Default Gateway addresses automatically.



---

**TCpMaxPortsExhausted: How many dropped connect requests to initiate SYN attack protection**

This parameter controls the point at which SYN – ATTACK protection starts to operate. SYN – ATTACK protection begins to operate when **TcpMaxPortsExhausted** connect requests have been refused by the system because the available backlog for connections is set at 0.

**AFD.SYS settings**

Windows Sockets applications such as File Transfer Protocol (FTP) servers and Web servers have their connection attempts handled by Afd.sys. Afd.sys has been modified to support large numbers of connections in the half – open state without denying access to legitimate clients. This is accomplished by allowing the administrator to configure a dynamic backlog. The version of Afd.sys included with Windows Server 2003 supports four registry parameters that can be used to control the dynamic backlog behavior.

**HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\AFD\Parameters\** registry key

Subkey Registry Value Entry	Format	Default	Recommended Value (Decimal)
DynamicBacklogGrowthDelta	DWORD	0	10
EnableDynamicBacklog	DWORD	0	1
MinimumDynamicBacklog	DWORD	0	20
MaximumDynamicBacklog	DWORD	0	20000

**DynamicBacklogGrowthDelta: Number of connections to create when additional connections are necessary for Winsock applications**

This setting controls the number of free connections to create when additional connections are necessary. Be careful with this value, as a large value could lead to explosive free connection allocations.

**EnableDynamicBacklog: Enable dynamic backlog for Winsock applications**

This is a global switch to enable or disable dynamic backlog. It defaults to 0 (off), setting it to 1 enables the new dynamic backlog feature.

**MinimumDynamicBacklog: Minimum number of free connections for Winsock applications**

This setting controls the minimum number of free connections allowed on a listening endpoint. If the number of free connections drops below this value, then a thread is queued to create additional free connections. This value should not be too large, as the dynamic backlog code engages whenever the number of free connections falls below this value. Too large a value may lead to a performance reduction.

**MaximumDynamicBacklog: Maximum number of 'quasi – free' connections for Winsock applications**

This setting controls the maximum number of "quasi – free" connections allowed on a listening endpoint. Quasi – free connections include the number of free connections plus those connections in a half – connected (SYN\_RECEIVED) state. No attempt is made to create additional free connections if doing so would exceed this value.



## Configure NetBIOS Name Release Security: (NoNameReleaseOnDemand) Allow the computer to ignore NetBIOS name release requests except from WINS servers

Network basic input/output system (NetBIOS) over TCP/IP is a networking protocol that, among other things, provides a means of easily resolving NetBIOS names registered on Windows – based systems to the IP addresses configured on those systems. This value determines whether the computer releases its NetBIOS name when it receives a name – release request.

**HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Netbt\Parameters\** registry key.

Subkey Registry Value Entry	Format	Default	Recommended Value (Decimal)
NoNameReleaseOnDemand	DWORD	1	1

## Disable Auto Generation of 8.3 File Names: Enable the computer to stop generating 8.3 style filenames

Windows Server 2003 supports 8.3 file name formats for backward compatibility with 16 – bit applications. The 8.3 file name convention is a naming format that allows file names that are up to eight characters in length.

The following registry value entry has been added to the template in the **HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\FileSystem\** registry key.

Subkey Registry Value Entry	Format	Default	Recommended Value (Decimal)
NtfsDisable8dot3NameCreation	DWORD	0	1

## Disable Autorun: Disable Autorun for all drives

Autorun begins reading from a drive on your computer as soon as media is inserted in it. As a result, the setup file of programs and the sound on audio media starts immediately.

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer\** registry key.

Subkey Registry Value Entry	Format	Default	Recommended Value (Decimal)
NoDriveTypeAutoRun	DWORD	0	0xFF

## Make Screensaver Password Protection Immediate: The time in seconds before the screen saver grace period expires

Windows includes a grace period between when the screen saver is launched, and when the console is actually locked automatically if screen saver locking is enabled.

**HKEY\_LOCAL\_MACHINE\SYSTEM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\** registry key.



Subkey Registry Value Entry	Format	Default	Recommended Value (Decimal)
ScreenSaverGracePeriod	String	5	0

## Enable Safe DLL Search Order: Enable Safe DLL search mode

The dynamic – link library (DLL) search order can be configured to search for DLLs requested by running processes in one of two ways:

- Search folders specified in the system path first, and then search the current working folder.
- Search current working folder first, and then search the folders specified in the system path.
- 

The registry value is set to 1. With a setting of 1, the system first searches the folders that are specified in the system path, and then searches the current working folder. With a setting of 0, the system first searches the current working folder, and then searches the folders that are specified in the system path.

**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\** registry key.

Subkey Registry Value Entry	Format	Default	Recommended Value (Decimal)
SafeDllSearchMode	DWORD	0	0

## NTFS

NTFS partitions support ACLs at the file and folder levels. This support is not available with the file allocation table (FAT), FAT32, or file systems. FAT32 is a version of the FAT file system that has been updated to permit significantly smaller default cluster sizes and to support hard disks up to two terabytes in size. FAT32 is included in Windows 2000 and Windows 2003

Format all partitions on every server using NTFS. Use the **convert utility** to carefully convert FAT partitions to NTFS, but keep in mind that the convert utility will set the ACLs for the converted drive to **Everyone: Full Control**.

## Configure SNMP Community Name

The Simple Network Management Protocol (SNMP) is a network management standard widely used with Transmission Control Protocol/Internet Protocol (TCP/IP) networks. SNMP provides a method of managing network nodes — servers, workstations, routers, bridges, and hubs — from a centrally located host. SNMP performs its management services by using a distributed architecture of management systems and agents. Systems running network management software are referred to as SNMP management systems or SNMP managers. Managed network nodes are referred to as SNMP agents.

The SNMP service provides a rudimentary form of security using community names and authentication traps. You can restrict SNMP communications for the agent and allow it to communicate with only a set list of SNMP management systems. Community names can be used to authenticate SNMP messages, and thus provide a rudimentary security scheme for the SNMP



service. Although a host can belong to several communities at the same time, an SNMP agent does not accept requests from a management system in a community that is not on its list of acceptable community names. There is no relationship between community names and domain names or workgroup names. A community name can be thought of as a password shared by SNMP management consoles and managed computers. It is your responsibility as a system administrator to set hard – to – guess community names when you install the SNMP service.

## ***IIS Configuration***

### **URLScan**

UrlScan is a free security tool from Microsoft that restricts the types of HTTP requests that Internet Information Services (IIS) will process. By blocking specific HTTP requests, the UrlScan security tool helps prevent potentially harmful requests from reaching the server.

URLScan can be downloaded from:

<http://www.microsoft.com/downloads/details.aspx?familyid=23d18937-dd7e-4613-9928-7f94ef1c902a&displaylang=en>

The following table details the capabilities of URLScan version 2.5 and native IIS6.0 capabilities.

<b>UrlScan 2.5 Feature</b>	<b>IIS 6.0 Built-in Capability</b>	<b>Recommendation</b>
<b>DenyExtensions:</b> This feature was implemented in UrlScan to limit the attack surface of the server by preventing, based on file name extensions, specific requests from running ISAPI or CGI code on the server.	IIS 6.0 limits the attack surface of the server by allowing administrators to specify the ISAPI and CGI code that can run on the server. Because IIS 6.0 specifies the code directly, it is not necessary to know which file extensions in the URL are capable of invoking the code.	Consider deny the following extensions: .cer, .cdx, .asa, .exe, .bat, .cmd, .com, .htw, .ida, .idq, .htr, .idc, .stm, .printer, .ini, .log, .pol, .dat
<b>DenyVerbs:</b> WebDAV code can be invoked on a Web server based on the use of particular HTTP verbs. This feature was implemented in UrlScan to limit the attack surface of the server by preventing requests that would invoke WebDAV.	IIS 6.0 allows administrators to explicitly enable or disable WebDAV. Since this action affects the WebDAV executable code directly, it is not necessary to inspect the HTTP verb that is associated with each request.	At a minimum, deny the following verbs: TRACE/TRACK, DELETE, OPTIONS, PROPFIND
<b>DenyHeaders:</b> WebDAV code can be invoked on a Web server based on the presence of particular HTTP headers. This feature was implemented in UrlScan to limit the attack surface of the server by preventing requests that would invoke WebDAV.	IIS 6.0 allows administrators to explicitly enable or disable WebDAV. Since this action affects the WebDAV executable code directly, it is not necessary to inspect the HTTP header that is associated with each request.	If WebDAV is not required it should be disabled.



UrlScan 2.5 Feature	IIS 6.0 Built-in Capability	Recommendation
<p><b>NormalizeUriBeforeScan:</b> This feature allows administrators to specify whether IIS will process the raw URL that is sent by the client or the canonicalized URL that is processed on the server.</p> <p><b>Note:</b> It is not practical to set this value to 0 on a production server. When this value is set to 0, all file name extensions and other URL checks in the UrlScan.ini file must specify all possible encodings of each character. The number of resulting permutations would be virtually impossible to manage on a production server.</p>	<p>The lockdown mechanism that is built into IIS 6.0 is based on the executable code that is permitted to run ? it is not based on the URL that the client requested. For this reason, <b>NormalizeUriBeforeScan</b> is not necessary on IIS 6.0.</p>	
<p><b>VerifyNormalization:</b> UrlScan was designed to run on many versions of IIS. The code that handles URL canonicalization has been improved with later releases and service packs of IIS. This feature allows UrlScan to detect potential issues with URL canonicalization on unpatched systems.</p>	<p>The HTTP.SYS component used by IIS 6.0 has improved canonicalization code that has been specifically written to help protect against URL canonicalization attacks.</p>	
<p><b>DenyUriSequences:</b> This feature was implemented in UrlScan to allow UrlScan to detect sequences that are used in URL?based attacks on a Web server.</p>	<p>It is not necessary for IIS 6.0 to deny URL sequences. By design, IIS 6.0 is not susceptible to URLbased attacks that use any of the character sequences listed in the default <b>DenyUriSequences</b> section of the UrlScan.ini file provided by Microsoft.</p>	<p>Consider disabling the following Url Sequences: ..., :, ./, \, %, &amp;</p>
<p><b>AllowDotInPath:</b> The UrlScan lockdown mechanism depends on a filter notification that occurs very early in the processing of a request. At this time, UrlScan cannot know for sure how IIS will parse the URL for PATH_INFO. It is possible that PATH_INFO will affect the file name extension on the URL. Setting <b>AllowDotInPath</b> to 0 will cause UrlScan to reject any request where the file extension is ambiguous due to a dot-in-path condition.</p>	<p>The <b>AllowDotInPath</b> feature is not necessary in IIS 6.0 because IIS 6.0 does not depend on filter notifications for its lockdown mechanism.</p>	



UrlScan 2.5 Feature	IIS 6.0 Built-in Capability	Recommendation
<p><b>RemoveServerHeader:</b> This feature allows UrlScan to remove or alter the identity of the server from the "Server" response header in the response to the client.</p>	<p>IIS 6.0 does not include the <b>RemoveServerHeader</b> feature because this feature offers no real security benefit. Most server attacks are not operating system?specific. Also, it is possible to detect the identity of a server and information about the operating system by mechanisms that do not depend on the server header.</p>	
<p><b>EnableLogging, PerProcessLogging, and PerDayLogging:</b> UrlScan is not part of the core IIS server. Rather, UrlScan is an add-on utility that produces its own log files. These settings control aspects of how UrlScan produces and names its log files.</p>	<p>IIS 6.0 logs all of its lockdown activity in the W3SVC logs. Requests that are rejected due to lockdown or executable code are identified by 404 errors with sub-error 2 (404.2) in the logs. Requests for static files that are rejected due to an unknown type are identified by 404 with sub-error 3 (404.3) in the logs.</p>	
<p><b>AllowLateScanning:</b> This feature allows administrators to specify whether UrlScan examines URLs before or after other filters. There are a number of filters that modify URLs, and it might be desirable for UrlScan to examine the URL after it has been modified. The FrontPage Server Extensions filter is an example of such a filter.</p>	<p>The <b>AllowLateScanning</b> feature is not necessary in IIS 6.0 because IIS 6.0 does not depend on filter notifications for its lockdown mechanism. The lockdown mechanism built into IIS 6.0 is based on the executable code that is allowed to run ? not on the URL that the client requested.</p>	
<p><b>RejectResponseUrl:</b> This feature works in conjunction with <b>UseFastPathReject</b>. If <b>UseFastPathReject</b> is set to 0, then any rejected requests will be remapped to the URL specified by <b>RejectResponseUrl</b>. If the specified URL does not exist, the client will receive a normal 404 response just as if the client had requested a non-existent page. If the specified URL does exist, the server can customize the response that is sent to the client.</p>	<p>In IIS 6.0, a request that is rejected due to a lockdown of executable code will generate a 404.2 custom error. A static file that is rejected due to an unknown MIME type will generate a 404.3 custom error. Administrators can use the IIS custom error mechanism to control these responses.</p>	



UrlScan 2.5 Feature	IIS 6.0 Built-in Capability	Recommendation
<p><b>UseFastPathReject:</b> The UrlScan lockdown mechanism depends on a filter notification that that occurs very early in the processing of a request. As a result, if UrlScan rejects the request directly from this notification, the normal 404 response cannot be generated. Rather, the client will receive a terse 404 response instead of the rich custom error that normally occurs. If <b>UseFastPathReject</b> is set to 0, UrlScan will remap the request to the URL specified by <b>RejectResponseUrl</b>.</p>	<p>IIS 6.0 does not depend on filter notifications for its lockdown mechanism. In IIS 6.0, a request that is rejected due to lockdown of executable code will generate a 404.2 custom error. A static file that is rejected due to an unknown file type will generate a 404.3 custom error. Administrators can use the IIS custom error mechanism to control these responses.</p>	
<p><b>AllowHighBitCharacters:</b> This feature allows UrlScan to detect non-ASCII characters in URLs.</p>	<p>The character range that is allowed is handled by HTTP.SYS. This value can be changed by modifying the following registry key: HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Services\ HTTP\ Parameters\ EnableNonUTF8 <b>Caution:</b> Incorrectly editing the registry could severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.</p>	
<p><b>MaxAllowedContentLength:</b> This feature allows UrlScan to place limits on the size of requests that are posted to the server.</p>	<p>IIS 6.0 has the built-in capability to limit the size of requests, which is configurable by the <b>MaxRequestEntityAllowed</b> and <b>ASPMaxRequestEntityAllowed</b> metabase properties.</p>	



UrlScan 2.5 Feature	IIS 6.0 Built-in Capability	Recommendation
<p><b>MaxUrl, MaxQueryString, and MaxHeader:</b> These settings allow UrlScan to place limits on the sizes of URLs, query strings, and specific headers that are sent to the server.</p>	<p>The HTTP.SYS component used by IIS 6.0 allows size limits to be set on various parts of the request. The values can be changed by modifying <b>AllowRestrictedChars, MaxFieldLength, UriSegmentMaxLength, and UriSegmentMaxCount</b> in the registry under the following registry keys:</p> <ul style="list-style-type: none"><li>• HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Services\ HTTP\ Parameters\ AllowRestrictedChars</li><li>• HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Services\ HTTP\ Parameters\ MaxFieldLength</li><li>• HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Services\ HTTP\ Parameters\ UriSegmentMaxLength</li><li>• HKEY_LOCAL_MACHINE\ System\ CurrentControlSet\ Services\ HTTP\ Parameters\ UriSegmentMaxCount</li></ul> <p><b>Caution:</b> Incorrectly editing the registry could severely damage your system. Before making changes to the registry, you should back up any valued data on the computer.</p>	

## IISLockdown utility

The freely available IIS Lockdown Wizard functions by turning off unnecessary features, thereby reducing attack surface available to attackers. Running this tool implements several best practices:

- Removes IISHelp, IISAdmin, Scripts and other virtual directories installed by default
- Secures unused script mappings
- Disables anonymous Web users' write capability to Web content
- Disables execute permissions on administrative tools
- Backs up the metabase

This tool can be downloaded from: <http://www.microsoft.com/technet/security/tools/locktool.mspx>